AMERICAN EXPRESS

Business and Operational Policies

October 2022, Version 2

GLOBAL NETWORK SERVICES

Confidential and Trade Secret Materials

This document contains sensitive, confidential, and trade secret information and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

To the maximum extent permitted by law, American Express does not make and hereby disclaims any and all representations, warranties, and liabilities, whether express or implied, or arising by law or from a course of dealing or usage of trade, including implied warranties of merchantability or fitness for a particular purpose or any warranty of title or non-infringement. Each Participant must comply with laws and regulations applicable to the subject matter of this document. These laws and regulations can differ from country to country, and each Participant is solely responsible for being aware and adhering to them in all countries where applicable.

The policies, procedures, and rules in this manual are subject to change from time to time by American Express Global Network Services.

© 2022 American Express Travel Related Services Company, Inc.

All Rights Reserved

Summary of Changes for this Edition

October 2022, Version 2

This Summary of Changes section describes revisions that are included in this edition of the *Business and Operational Policies* manual. All revisions in the manual are identified by a change bar in the margin.

Please contact your American Express Global Network Services (AEGNS) representative with any questions.

How Change Bars Are Used in this Manual

All changes to the *Business and Operational Policies* manual are indicated with a change bar. A change bar is a vertical line (usually in the left margin) that visually identifies new or revised text. **Only** substantial changes are listed in the Summary of Changes table below. Substantial changes are those changes having potential impact to Participants' operational procedures.

Sections of this manual that are deleted are referenced in the Summary of Changes using the section numbering from the previous publication. This will avoid confusion from any auto-numbering changes that may occur in this publication.

Summary of Changes

Subject	Revision
Created Version 2	The *Business and Operational Policies* manual was republished on Friday, November 18 to correct inconsistencies in the Table of Contents and bookmarks. No content changes were made. This update was originally announced in the November 2022 *Network Participant Updates* Information Digest article *Formatting Correction for Bi-Annual Publications*.
Payment Aggregator Term Update	The term "Payment Aggregator" was modified to "Payment Facilitator" throughout the *Business and Operational Policies* manual.
Section 1.6.4, "BIN Blocking Services," on page 7	This section was modified to remove references to the BIN Blocking Fee. This update was originally announced in the May 2022 *Network Participant Updates* article *BIN Blocking Fee Elimination and BIN Rental Fee Addition*.
Section 1.7, "The Transaction Life Cycle," on page 10	Figure 1-1, "Transaction Life Cycle," on page 10 was modified to include Good Faith and update "Presentment" to "First Presentment". This update was originally announced in the August 2022 *Network Participant Updates* article *Network Disputes Policy Updates*.
Section 2.2.7.2, "Participant Training," on page 15	The section was added to create awareness of online training prior to gaining access to certain AEGNS tools and services. This update was originally announced in the August 2022 *Network Participant Updates* article *Participant Training*.
Section 2.2.17, "Audit Rights," on page 26 Section 2.2.17.1, "Network Assessment Program," on page 27	These sections were modified to remove the reference to "onsite" assessments. This update was originally announced in the May 2022 *Network Participant Updates* article *Network Assessment Program Update*.
Section 2.4, "Participant Data Security Policy," on page 38	This section was modified to include Point of Interaction (POI) in the Payment Card Industry PIN Transaction Security (PCI PTS) reference and to add Payment Card Industry Point-to-Point Encryption (PCI P2PE). This update was originally announced in the August 2022 *Network Participant Updates* article *PCI Standards Update*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Summary of Changes (continued)

Subject	Revision
Section 2.4.2, "Acquirer Data Security Compliance Requirements," on page 40	This section was modified to include POI in the PCI PTS reference and to add Payment PCI P2PE. This update was originally announced in the August 2022 *Network Participant Updates* article *PCI Standards Update*.
Section 2.4.2.1, "Acquirers' S/Es and Service Providers Data Security Compliance Requirements," on page 41	This section was modified to include POI in the PCI PTS reference and to add Payment PCI P2PE. This update was originally announced in the August 2022 *Network Participant Updates* article *PCI Standards Update*.
Section 2.4.4, "Issuer Data Security Compliance Requirements," on page 42	This section was modified to include POI in the PCI PTS reference. This update was originally announced in the August 2022 *Network Participant Updates* article *PCI Standards Update*.
Table 2-7, "Digital Capabilities AEGNS Optional On-Behalf-Of Services," on page 53 Table 2-8, "Digital Wallet Program On-Behalf-Of Services," on page 62	These tables were modified to replace the term Limited Use Payment Credential (LUPC) with Limited Use Key (LUK). This update was originally announced in the January 2022 *Network Participant Updates* article *Digital Wallet Program On-Behalf-Of Service -Transaction Keys in HCE Mobile Wallets*.
Section 2.5.4.1, "General Requirements for Digital Wallet Programs," on page 58	This section was modified to clarify that an FLS exception does not apply to Digital Wallet Application-initiated Transactions that are person-to-person payments. This update was originally announced in the September 2022 *Network Participant Updates* article *Digital Wallet Application-Initiated Fraud Dispute Rights*.
Section 2.5.4.7.2, "S/E Acceptance Procedures for CPQR Transactions," on page 66	This section was modified to allow airlines, cruise lines, and lodging S/Es to submit multiple ROCs with single Authorization. This update was originally announced in the September 2022 *Network Participant Updates* article *Multiple ROC Transactions with Single Authorization*.
Section 2.5.5.1.1, "ID&V Management," on page 67	This section was modified to add the term Limited Use Payment Credential (LUPC) to the policy. This update was originally announced in the January 2022 *Network Participant Updates* article *Digital Wallet Program On-Behalf-Of Service -Transaction Keys in HCE Mobile Wallets*.
Section 2.5.5.1.3, "Cryptogram Management and Tokenization," on page 68	This section was modified to add the acronym LUPC to the policy, and clarify credential access. This update was originally announced in the January 2022 *Network Participant Updates* article *Digital Wallet Program On-Behalf-Of Service -Transaction Keys in HCE Mobile Wallets*.
Section 2.5.5.1.4, "Expresspay Mobile HCE Application Life Cycle Management ," on page 68	This section was modified to add the acronym LUPC to the policy. This update was originally announced in the January 2022 *Network Participant Updates* article *Digital Wallet Program On-Behalf-Of Service -Transaction Keys in HCE Mobile Wallets*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Summary of Changes (continued)

Subject	Revision
Section 2.6, "Indirect Acceptors," on page 74 Section 2.6.1, "Acquirer Requirements for Indirect Acceptors," on page 75 Section 2.6.1.1, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 75 Section 2.6.1.2, "Right to Request Information," on page 76 Section 2.6.1.3, "Data Element Requirements," on page 76 Section 2.6.1.4, "Additional Requirements for Bill Payment Providers," on page 76 Section 2.6.1.5, "Additional Requirements for Installment Payment Providers," on page 78 Section 2.6.1.6, "Additional Requirements for Marketplaces," on page 78	This section and all subsections were created to describe the obligations that Participants must follow for Indirect Acceptors. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with modifications made in the April 2022 *Network Participant Updates*.
Section 2.9.3.5, "Payment Facilitator," on page 89	This section was modified to clarify the definition of Payment Facilitators and to expressly allow Payment Facilitators to contract with Marketplaces. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with updates announced in the April 2022 *Network Participant Updates*.
Section 2.9.3.5.2, "General Requirements for Acquirers, Payment Facilitators, and Sponsored Merchants," on page 90	This section was modified to expressly allow Payment Facilitators to contract with Marketplaces. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with updates announced in the April 2022 *Network Participant Updates*.
Section 2.9.4.2, "Restricted Industries," on page 95	This section was modified to add Indirect Acceptor and Peer-to-Peer Payment as a restricted industry. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with updates announced in the April 2022 *Network Participant Updates*.
Section 2.9.14, "Stored Value Digital Facility Acquirer Requirements," on page 103	This section was modified to clarify that a Stored Value Digital Facility (SVDF) may be an Indirect Acceptor. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with updates announced in the April 2022 *Network Participant Updates*.
Section 2.9.18, "American Express SafeKey Acquirer Requirements," on page 107	This section was modified to remove outdated information and reorganize existing requirements. This update was originally announced in the August 2022 *Network Participant Updates* article *SafeKey Language Updates*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Summary of Changes (continued)

Subject	Revision
Section 2.10.1, "Certification of Card Issuing Programs," on page 110	This section was modified to replace "embossed" with a general phrase to accommodate both embossed and flat-printed Cards, and remove the out-dated footnote. This update was originally announced in the August 2022 *Network Participant Updates* article *Brand Design Updates*.
Section 2.10.13, "American Express SafeKey Issuer Requirements," on page 119	This section was modified to remove outdated information and reorganize existing requirements. This update was originally announced in the August 2022 *Network Participant Updates* article *SafeKey Language Updates*.
Section 2.13.6, "Exceptions," on page 124	This section was added to provide guidance and clarification about the existing process to request Exceptions. This update was originally announced in the July 2022 *Network Participant Updates* article *Exception Process*.
Section 3.2.5.1, "Types of Prepaid Cards," on page 130	This section was modified to remove an outdated description. This update was originally announced in the August 2022 *Network Participant Updates* article *Brand Design Updates*.
Section 3.9.1.5, "Card Production," on page 207	This section was modified to remove an outdated term and footnote. This update was originally announced in the August 2022 *Network Participant Updates* article *Brand Design Updates*.
Section 3.9.2.3, "Additional Optional ATM Services," on page 211	This new section explains that Issuers can provide ATM PIN Management at their discretion.This section also describes ATM PIN Management services, and explains that Issuers must obtain Certification to provide ATM optional services, and that these services are provided at the discretion of the ATM Provider. This update was originally announced in the April 2022 *Network Participant Updates* article *ATM Optional Transactions Policy*.
Table 4-1, "Expresspay at TAT - Operational Parameters," on page 219	This table was modified to add Hong Kong (Special Administrative Region of China). This update was originally announced in the August 2022 *Network Participant Updates* article *Expresspay at Transit Access Terminals - Hong Kong Transit*.
Table 4-1, "Expresspay at TAT - Operational Parameters," on page 219 Table 4-2, "Expresspay at TAT - Declined Authorizations," on page 220	These tables were modified to add Singapore. This update was originally announced in the March 2022 *Network Participant Updates* article *Expresspay at Transit Access Terminals - Singapore Transit*.
Section 4.2.2, "Multiple ROC Transactions with Single Authorization," on page 214	This section was added to allow airlines, cruise lines, and lodging S/Es to submit multiple ROCs with single Authorization. This update was originally announced in the September 2022 *Network Participant Updates* article *Multiple ROC Transactions with Single Authorization*.
Section 4.2.3, "Card Acceptance Restrictions," on page 214 Section 4.2.7, "In-Person Charges," on page 216	These sections were modified to allow airlines, cruise lines, and lodging S/Es to submit multiple ROCs with single Authorization. This update was originally announced in the September 2022 *Network Participant Updates* article *Multiple ROC Transactions with Single Authorization*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Summary of Changes (continued)

Subject	Revision
Section 4.2.7, "In-Person Charges," on page 216	This section was modified to accommodate use of flat-printed Cards. This update was originally announced in the August 2022 *Network Participant Updates* article *Brand Design Updates*.
Section 4.6.1.3.3, "ATM Security Pictures," on page 243	This section was added to allow Issuers the option to request ATM security pictures. This update was originally announced in the July 2022 *Network Participant Updates* article *ATM Security Pictures Request.*
Section 5.3.8, "Authorizations Support," on page 250	This section was modified to remove references to the BIN Blocking Fee. This update was originally announced in the May 2022 *Network Participant Updates* article *BIN Blocking Fee Elimination and BIN Rental Fee Addition*.
Chapter 6	No substantive changes were made to this chapter.
Section 7.3.2.3, "Fulfillment," on page 282 Section 7.3.2.14, "Documentation Delivery," on page 285 Section 7.4.1, "Fulfillment Notification Reason Codes," on page 293 Section 7.8, "Process Timeframes," on page 303	These sections were modified to clarify Disputes policy. This update was originally announced in the August 2022 *Network Participant Updates* article *Network Disputes Policy Updates*.
"ISO 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented" on page 309 "ISO 4512 - Multiple Processing" on page 311 "ISO 4513 - Credit Not Presented" on page 312 "ISO 4516 - Request for Support Not Fulfilled" on page 317	These ISO codes were modified to clarify Disputes policy. This update was originally announced in the August 2022 *Network Participant Updates* article *Network Disputes Policy Updates*.
"ISO 4512 - Multiple Processing" on page 311	This section was modified to exclude cruise lines and lodging S/Es. This update was originally announced in the September 2022 *Network Participant Updates* article *Multiple ROC Transactions with Single Authorization*.
"ISO 4513 - Credit Not Presented" on page 312 "ISO 4515 - Paid Through Other Means" on page 316	These ISO codes were modified for Installment Payment Provider and Bill Payment Provider Transactions. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with updates announced in the April 2022 *Network Participant Updates*.
"ISO 4527 - Missing Imprint" on page 326	The following Excluded Transaction item was added to the end of the existing list: Transactions using a flat-printed Card. This update was originally announced in the August 2022 *Network Participant Updates* article *Brand Design Updates*.
"ISO 4544 - Cancellation of Recurring Goods/Services" on page 332	The following content was added to the end of the existing Excluded Transactions list: Installment Payment Provider Transactions. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with updates announced in the April 2022 *Network Participant Updates*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Summary of Changes (continued)

Subject	Revision
"ISO 4553 - Not as Described or Defective Merchandise" on page 334 "ISO 4554 - Goods and Services Not Received" on page 337	These ISO codes were modified for Installment Payment Provider and Bill Payment Provider Transactions. This update was originally announced in the September 2021 *Network Participant Updates* article *Indirect Acceptors*, with updates announced in the April 2022 *Network Participant Updates*.
"ISO 4763 - Fraud Full Recourse" on page 348	This ISO code was modified to remove item two (2) from the Excluded Transactions list and to add item seven (7) to the Conditions list. This update was originally announced in the October 2021 *Network Participant Updates* and updated in the August 2022 *Network Participant Updates* article *HRSE Industry & Performance Criteria Refresh*.
"ISO 4798 - Fraud Liability Shift - Counterfeit" on page 350	This ISO code was modified to include additional countries in scope. This update was originally announced in the October 2021 *Network Participant Updates* article *AEIPS Fraud Liability Shift - Counterfeit Expansion*.
Table 7-23, "Allowable Codes for Digital Wallet Payments Transactions," on page 358	This table was updated to include ISO 4540 (Card not Present) as an allowable fraud Chargeback reason. This update was originally announced in the September 2022 *Network Participant Updates* article *Digital Wallet Application-Initiated Fraud Dispute Rights*.
Section 7.10.8.1, "AEIPS Fraud Liability Shift (FLS)," on page 359 Section 7.10.8.1.1, "Types of AEIPS FLS," on page 360 Section 7.10.8.1.2, "PIN Capable and Enabled POS Devices," on page 360	These sections were modified to expand AEIPS Counterfeit Fraud Liability Shift Participation requirements to additional countries. This update was originally announced in the October 2021 *Network Participant Updates* article *AEIPS Fraud Liability Shift - Counterfeit Expansion*.
Table 7-24, "AEIPS Counterfeit FLS Participation"	This table was deleted. This update was originally announced in the October 2021 *Network Participant Updates* article *AEIPS Fraud Liability Shift - Counterfeit Expansion*.
Table 7-24, "AEGNS Assignment of Liability Detail," on page 359	Table 7-25 was reordered and renumbered and now displays as Table 7-24. This update was originally announced in the October 2021 *Network Participant Updates* article *AEIPS Fraud Liability Shift - Counterfeit Expansion*.
Section 7.10.8.3, "American Express SafeKey Fraud Liability Shift," on page 361	This section was modified to remove outdated information and reorganize existing requirements. This update was originally announced in the August 2022 *Network Participant Updates* article *SafeKey Language Updates*.
Table 7-26, "Allowable Codes for SafeKey," on page 362	This table was modified to remove 4763 as an allowable code for SafeKey. This update was originally announced in the October 2021 *Network Participant Updates* and updated in the August 2022 *Network Participant Updates* article *HRSE Industry & Performance Criteria Refresh*.
Section 8.2.2, "Sensitive Materials," on page 376	This section was modified to replace "embossed" and "unembossed" with "personalized." This update was originally announced in the August 2022 *Network Participant Updates* article *Brand Design Updates*.
Section 8.5.1, "Security Office," on page 379	This section was modified to replace "embossing" with "personalization." This update was originally announced in the August 2022 *Network Participant Updates* article *Brand Design Updates*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Summary of Changes (continued)

Subject	Revision
Section 8.9.1.1, "Removing an S/E from the High Risk S/E List," on page 384	This section was modified to remove High Risk S/Es from the HRSE Program based on Fraud to Gross (FTG) performance and to specify that gross fraud per month must be below $25,000. A new table was created to define Low Tier and High Tier FTG calculations. This update was originally announced in the October 2021 *Network Participant Updates* article *HRSE Industry & Performance Criteria Refresh*, with modifications made in the August 2022 *Network Participant Updates*.
Section 8.9.2, "High Risk S/E Criteria," on page 385	This section was modified to add details about Low Tier and High Tier FTG calculations. This update was originally announced in the October 2021 *Network Participant Updates* and updated in the August 2022 *Network Participant Updates* article *HRSE Industry & Performance Criteria Refresh*.
Section 8.9.2.3, "Fraud to Gross Sales Volume Ratio," on page 386	This section was modified to remove previous FTG Sales Volume ratio, to add Low Tier and High Tier calculations and thresholds, and to clarify that the S/E no longer qualifies for SafeKey FLS based on performance criteria and to refer to Section 7.10.8.3, "American Express SafeKey Fraud Liability Shift," on page 361 for more information. This update was originally announced in the October 2021 *Network Participant Updates* and updated in the August 2022 *Network Participant Updates* article *HRSE Industry & Performance Criteria Refresh*.
Section 8.9.2.4, "High Risk S/E Industries," on page 386	This section was modified to update High Risk S/E industries. This update was originally announced in the October 2021 *Network Participant Updates* and updated in the August 2022 *Network Participant Updates* article *HRSE Industry & Performance Criteria Refresh*.
Section 8.9.6.1, "American Express SafeKey Fraud Liability Shift Qualification S/E Fraud Thresholds," on page 391	This section was modified to show the new monthly Fraud to Gross Sales Volume Ratio of 0.9% and to include a reference to Section 8.9.2.3, "Fraud to Gross Sales Volume Ratio," on page 386 for more information. This update was originally announced in the October 2021 *Network Participant Updates* and updated in the August 2022 *Network Participant Updates* article *HRSE Industry & Performance Criteria Refresh*.
Section 8.10.1, "Card Security," on page 391	This section was modified to reflect the global expansion of AEIPS Counterfeit Fraud Liability Shift participation. This update was originally announced in the October 2021 *Network Participant Updates* and updated in the August 2022 *Network Participant Updates* article *AEIPS Fraud Liability Shift - Counterfeit Expansion*.
Chapter 9	No substantive changes were made to this chapter.
Section 10.5.5, "BIN Blocking Fees' Table 10-11, "BIN Blocking Fees"	The headings for this section and table were renamed, as described in the next line.
Section 10.5.5, "Active BIN Rental Fee," on page 407 Table 10-11, "Active BIN Rental Fees," on page 407	This section and table were modified to remove BIN Blocking Fees and replace with Active BIN Rental Fee. This update was originally announced in the May 2022 *Network Participant Updates* article *BIN Blocking Fee Elimination and BIN Rental Fee Addition*.
Table 10-26, "Operational Support Fee Schedule," on page 414	This table was modified to remove the reference to "onsite" assessments. This update was originally announced in the May 2022 *Network Participant Updates* article *Network Assessment Program Update*.
Chapter 11	No substantive changes were made to this chapter.
Chapter 12	No substantive changes were made to this chapter.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Summary of Changes (continued)

Subject	Revision
Chapter 13, "Abbreviations and Acronyms," beginning on page 490	The following terms were added: • LUK - Limited Use Key • P2P - Peer-to-Peer Payment The following term was deleted: • UDK - Unique Derived Key
Chapter 14, "Definitions," beginning on page 495	The following terms were added: • American Express Verification Value (AEVV) • Bill Payment Provider • End Beneficiary • Exception • Indirect Acceptor • Installment Payment Provider • Marketplace • Peer-to-Peer Payment (P2P) • Staged Digital Wallet The following term was modified: • Payment Facilitator (previously referred to as Payment Aggregator or Payment Service Provider)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table of Contents

Summary of Changes for this Edition iii
Table of Contents xi
List of Tables xxxv
List of Figures xxxvii

1 Introduction 1
1.1 Introduction to this Manual 1
1.1.1 AEGNS Relationship with American Express Company 1
1.1.2 How the Business and Operational Policies Manual is Organized 1
1.1.3 Conventions Used in this Manual 1
1.1.3.1 Grammar and Usage 1
1.1.3.2 Style and Symbols 1
1.2 English Language 2
1.3 Procedures for Revisions 2
1.3.1 Distribution of Materials 2
1.4 Related AEGNS Manuals, Guidelines, and Resources 3
1.5 Network Participation 5
1.5.1 Authorized Activities - Overview 5
1.5.2 Merchant Acquiring - General 5
1.5.2.1 Conduct of Merchant Acquiring Business 5
1.5.3 Card Issuing - General 5
1.5.3.1 Conduct of Card Issuing Business 6
1.6 Network Services 6
1.6.1 Access to the Amex Shared ATM Network 6
1.6.2 ATM Transaction Routing 6
1.6.3 Authorization Transaction Routing 7
1.6.4 BIN Blocking Services 7
1.6.5 Chargeback Routing and Processing 7
1.6.6 Clearing 7
1.6.7 Currency Conversion 7
1.6.8 Debit Card BIN File 8
1.6.8.1 Debit Card BIN File Usage 8
1.6.9 Exception File 8
1.6.10 Fraud Prevention Assistance 9
1.6.11 Management Information System 9
1.6.12 Policy and Technical Manuals 9
1.6.13 Recurring Billing Cancellation Service 9
1.6.14 Service Establishment Network Acceptance 9
1.6.15 Settlement and Funds Exchange 9
1.6.16 Stand-In Authorization 9
1.7 The Transaction Life Cycle 10

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2 Business Policies and Rules 11
2.1 Introduction 11
2.2 General Requirements for AEGN Participants 11
2.2.1 Initial Eligibility Requirements for Participants 11
2.2.2 Ongoing Eligibility Requirements for Participants 12
2.2.3 Financial Safety and Soundness of Participants 13
2.2.3.1 Participant Selection and Monitoring of Settlement Bank 13
2.2.4 Participant Books of Account 13
2.2.5 Security Requirements for Participants 13
2.2.6 Network Infrastructure Access and Certification 14
2.2.7 Systems Development and Maintenance 14
2.2.7.1 AEGNS Assistance Prior to Launch 14
2.2.7.2 Participant Training 15
2.2.8 Data Quality 15
2.2.9 Program Progress Reports 16
2.2.9.1 Annual Attestation of Accuracy 16
2.2.10 Marketing, Advertising, and Public Relations 16
2.2.10.1 General Advertising Policies 16
2.2.10.1.1 Use of the Registration Mark (®) 16
2.2.10.1.2 Use of Amex Licensed Marks 17
2.2.10.1.3 Use of the Words “Card” and “Cardmember” 17
2.2.10.1.4 Communication Standards 17
2.2.10.1.5 Accuracy and Truth in Advertising 17
2.2.10.1.6 Disclosure Requirements - Prohibited Countries 17
2.2.10.1.7 Material Facts 18
2.2.10.1.8 Use of Exaggerated Claims 18
2.2.10.2 Advertising and Marketing Review Requirements 18
2.2.10.2.1 Creative Brief and Pre-Production Material Submission 18
2.2.10.2.2 Approval of Advertising Campaigns 19
2.2.10.2.3 Additional Policies for Blue Box Line Card and Prepaid Card Issuers 19
2.2.10.3 Production Costs and Talent Rights 20
2.2.10.3.1 Translation Costs 20
2.2.10.3.2 Talent Rights 20
2.2.10.4 Changes to AEGNS-Approved Advertising and Marketing Materials 20
2.2.10.5 Post Review of Advertising and Marketing Materials 20
2.2.10.6 AEGNS Internet Marketing Communications Policies and Guidelines 20
2.2.10.6.1 Paid Search Policies and Guidelines 21
2.2.10.7 Failure to Comply With AEGNS Advertising and Marketing Policies 21
2.2.10.8 Compliance to Local Regulatory Requirements 22
2.2.10.9 Participant Eligible Marketing Region 22
2.2.10.10 Right to Request Removal of Unapproved Communications 22
2.2.11 Press Releases/Publicity 22
2.2.12 Participants’ Key Contacts 22
2.2.13 Social Media 22
2.2.14 Privacy Policies 23

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.15 Transaction Data Use 24
2.2.16 Alternative Dispute Resolution 24
2.2.17 Audit Rights 26
2.2.17.1 Network Assessment Program 27
2.2.18 Taxes on Fees and Assessments 28
2.2.19 Global Disputes Monitoring Program 29
2.2.19.1 Retrieval Request Threshold Standard 29
2.2.19.2 First Chargeback Threshold Standard 29
2.2.19.3 Participant GDMP Status 30
2.2.20 Crisis Preparedness and Service Continuity Program 30
2.3 Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements 30
2.3.1 General Requirements 31
2.3.1.1 AML/ATF Transaction Monitoring 32
2.3.2 Customer Screening Program 32
2.3.2.1 Certifications and Ongoing Due Diligence 33
2.3.2.2 Non-Compliance 33
2.3.3 Additional Anti-Money Laundering (AML) Requirements for Cash Disbursements 33
2.3.3.1 Activation for Cash Disbursement Transactions 34
2.3.3.2 Other Cash Disbursement Requirements 34
2.3.4 AML/ATF Requirements for All Prepaid Cards 34
2.3.4.1 AML/ATF Requirements for Non-Reloadable Prepaid Cards 35
2.3.4.2 AML/ATF Requirements for Reloadable Prepaid Cards 35
2.3.5 Non-Compliance 35
2.3.6 Prohibited and Restricted Countries and Persons 36
2.3.6.1 Prohibited Countries and Regions 36
2.3.6.2 Other Prohibited Countries 36
2.3.6.3 Restricted Countries 37
2.3.6.4 Additional Prohibited Persons, Entities, and Governments 37
2.3.7 Foreign Corrupt Practices Act and Anti-Bribery Requirements 37
2.4 Participant Data Security Policy 38
2.4.1 PCI Assessment and Reporting Relief for S/Es 39
2.4.1.1 PCI Assessment and Reporting Relief Program 39
2.4.2 Acquirer Data Security Compliance Requirements 40
2.4.2.1 Acquirers' S/Es and Service Providers Data Security Compliance Requirements 41
2.4.3 Acquirer Data Security Compliance Validation Requirements 41
2.4.3.1 Acquirers' S/Es and Service Providers Data Security Compliance Validation Requirements 41
2.4.4 Issuer Data Security Compliance Requirements 42
2.4.4.1 Issuers' Service Provider Data Security Compliance Requirements 43
2.4.5 Issuer Data Security Compliance Validation Requirements 43
2.4.5.1 Issuers' Service Provider Data Security Compliance Validation Requirements 43
2.4.6 Participant Data Security Compliance Validation Documentation 43
2.4.6.1 Annual PCI Data Security Assessment 43
2.4.7 Participant Data Security Non-Compliance 43

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.8 Encryption Data Security Requirements 44
2.4.8.1 Online PIN Encryption Requirements 45
2.4.8.2 Issuer Compliance Requirements 45
2.4.8.3 Acquirer Compliance Requirements 45
2.4.8.4 Third-Party Compliance Requirements 46
2.4.8.5 Use of Alternate Encryption 46
2.4.8.6 Key Management Program Compliance Requirements 46
2.4.8.7 Participant Responsibilities Following Data Compromise 46
2.4.8.8 Encryption Security Policy Validation Requirements 46
2.4.9 Requirements for Notification of Data Compromise 47
2.4.10 Participant Responsibilities Following Discovery of Data Compromise 48
2.4.11 Notification of Data Compromise from AEGNS to Potentially Impacted Issuers 49
2.4.12 Cardholder Data Compromise Recovery Process (CDCRP) 49
2.4.12.1 Data Compromise Event Criteria 49
2.4.12.2 CDCRP Financial Liability Relief for S/Es 50
2.4.12.2.1 CDCRP Financial Liability Relief Program 50
2.4.12.3 Issuer Responsibilities under the CDCRP 51
2.4.12.4 AEGNS Responsibilities to Acquirers under the CDCRP 51
2.4.12.5 AEGNS Responsibilities to Issuers under the CDCRP 51
2.4.12.6 CDCRP Liability Calculations 52
2.5 Digital Capabilities 52
2.5.1 Digital Capabilities Enablement 52
2.5.1.1 Digital Capabilities Enablement Issuer Guidelines 52
2.5.1.2 Digital Capabilities Enablement AEGNS Optional On-Behalf-Of Services 53
2.5.2 Tokenization 53
2.5.2.1 Token Request and Token Requestor 54
2.5.2.2 Token Service Provider 54
2.5.2.3 Token Process Management 54
2.5.2.3.1 Token Types 54
2.5.2.3.2 Token Generation 55
2.5.2.3.3 Token Assurance ID&V 55
2.5.2.3.4 Token Mapping 55
2.5.2.3.5 De-Tokenization 56
2.5.2.4 Token BIN Management Strategy 56
2.5.2.4.1 Token BIN and BIN Management 56
2.5.2.5 Token Domain Management 56
2.5.2.5.1 Token Domain and Domain Restriction Controls 56
2.5.2.6 Token Life Cycle Management 57
2.5.3 Card-on-File Tokenization 57
2.5.4 Digital Wallet Programs 57
2.5.4.1 General Requirements for Digital Wallet Programs 58
2.5.4.2 Digital Wallet Program Participant Terms 59
2.5.4.3 Digital Wallet Program Services 60
2.5.4.3.1 Provisioning and Mapping Services 61
2.5.4.3.2 Authorization Services 61

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.4.4 Acquirer Certification Requirements for Digital Wallet Programs 62
2.5.4.5 Digital Wallet Payments 63
2.5.4.5.1 S/E Acceptance Procedures for Digital Wallet Contactless-Initiated Transactions 63
2.5.4.5.2 S/E Acceptance Procedures for Digital Wallet Application-Initiated Transactions 63
2.5.4.5.3 S/E Acceptance Procedures for Digital Wallet MST Transactions 63
2.5.4.5.4 Recurring Billing for Digital Wallet Payments 64
2.5.4.5.5 Chargeback Policies for Digital Wallet Payments 64
2.5.4.5.6 Credit ROCs for Digital Wallet Program Transactions 64
2.5.4.6 Expresspay Mobile 64
2.5.4.7 Consumer-Presented Quick Response 65
2.5.4.7.1 Issuer Requirements for Consumer-Presented Quick Response 65
2.5.4.7.2 S/E Acceptance Procedures for CPQR Transactions 66
2.5.5 Expresspay Mobile Host Card Emulation 66
2.5.5.1 Expresspay Mobile HCE Ecosystem 67
2.5.5.1.1 ID&V Management 67
2.5.5.1.2 Expresspay Mobile HCE Application Security 68
2.5.5.1.3 Cryptogram Management and Tokenization 68
2.5.5.1.4 Expresspay Mobile HCE Application Life Cycle Management 68
2.5.5.1.5 Certification of Expresspay Mobile HCE Products 69
2.5.6 Payment Account Reference 70
2.5.6.1 Payment Account Reference - Acquirer Requirements 70
2.5.7 Secure Remote Commerce 70
2.5.7.1 SRC Ecosystem....70
2.5.7.1.1 SRC System 70
2.5.7.1.2 SRC Initiator 70
2.5.7.1.3 Digital Card Facilitator....70
2.5.7.1.4 Digital Payment Application 70
2.5.7.2 General SRC Requirements 71
2.5.7.3 Issuer SRC Requirements 71
2.5.7.4 Acquirer SRC Requirements 71
2.5.7.5 S/E SRC Requirements 71
2.5.7.6 SRC Chargeback Policies 71
2.5.8 Issuer Originated Payments.... 72
2.5.8.1 General Requirements for Issuer Originated Payments....72
2.5.8.2 Merchant-Presented Quick Response....72
2.5.8.2.1 Authorization Processing for MPQR....73
2.5.8.2.2 Acquirer Requirements for MPQR....73
2.5.8.2.3 S/E Acceptance Procedures for MPQR....73
2.5.8.2.4 Issuer Requirements for MPQR....74
2.5.8.2.5 Chargeback Policies for MPQR....74
2.6 Indirect Acceptors 74
2.6.1 Acquirer Requirements for Indirect Acceptors 75
2.6.1.1 Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements ...75
2.6.1.2 Right to Request Information 76
2.6.1.3 Data Element Requirements....76
2.6.1.4 Additional Requirements for Bill Payment Providers....76

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.6.1.5 Additional Requirements for Installment Payment Providers 78
2.6.1.6 Additional Requirements for Marketplaces 78
2.7 Service Provider 78
2.7.1 General Requirements 79
2.7.1.1 Service Provider Categories and Service Types 79
2.7.1.2 Non-Compliance 80
2.8 Authorized Processors 80
2.8.1 Use of Authorized Processors 81
2.8.2 Processor's Confidentiality Obligations 82
2.8.3 Compliance 82
2.9 Requirements for Conducting Merchant Acquiring Business 83
2.9.1 Acquirer-Related Certification 83
2.9.1.1 POS Certification Requirements 84
2.9.2 Reporting to AEGNS 85
2.9.2.1 Annual Plan Disclosure 85
2.9.2.2 Acquirer File Submission Requirements 85
2.9.2.2.1 S/E Demographics Detail Data (9640) Message Submission Requirements 85
2.9.2.2.2 On-Us POS and ATM (1340) Message Submission Requirements 85
2.9.2.3 Acquirer Data Collection File Submission Requirements 85
2.9.3 S/E Qualifications and Agreement Requirements 86
2.9.3.1 S/E Application Elements 86
2.9.3.2 S/E Acquisition Verification Process 86
2.9.3.3 Compliant S/E Agreement Design 87
2.9.3.3.1 Multinational Accounts (MNAs) 88
2.9.3.4 Acquirer Eligible Marketing Region 89
2.9.3.5 Payment Facilitator 89
2.9.3.5.1 Payment Facilitator Qualifications 90
2.9.3.5.2 General Requirements for Acquirers, Payment Facilitators, and Sponsored Merchants 90
2.9.3.5.3 Reporting Requirements for Payment Facilitators 91
2.9.3.5.4 Payment Facilitator Agreement Requirements 92
2.9.3.5.5 Sponsored Merchant Agreement Requirements 92
2.9.3.5.6 Sponsored Merchant Reporting Requirements 93
2.9.3.5.7 Data Elements Requirements 93
2.9.3.5.8 Data Quality 93
2.9.3.6 Terms Applicable to the European Union/European Economic Area and United Kingdom Only 94
2.9.4 Prohibited and Restricted Industry Requirements 94
2.9.4.1 Prohibited Industries 94
2.9.4.2 Restricted Industries 95
2.9.4.3 General Requirements for Acquirers, Lotteries, and Gambling S/Es 96
2.9.5 Brand Protection 97
2.9.5.1 Illegal or Brand Damaging Activity 97
2.9.5.2 Reporting Violations 98
2.9.5.3 Investigations 99
2.9.5.4 Correcting Violations 99
2.9.5.5 Verification of Compliance 99

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.5.6 Brand Protection Assessment 99
2.9.5.7 Data Quality 100
2.9.6 Unique S/E Number 101
2.9.7 S/E Website Information Display Guidelines 101
2.9.8 S/E Monitoring 102
2.9.9 S/E Floor Limits 102
2.9.10 S/E Classifications 102
2.9.11 S/E Card Acceptance Process 102
2.9.12 Acquirer Transaction Processing Requirements 102
2.9.13 Requirements for Acquirers of Cash Disbursements 103
2.9.13.1 Point of Sale Device Requirement for Cash Disbursement 103
2.9.14 Stored Value Digital Facility Acquirer Requirements 103
2.9.15 Internet Transaction Descriptor Information 103
2.9.16 Record of Charge Archival Storage 103
2.9.17 Chip Card Requirements 104
2.9.17.1 Certification Authority Public Key (CAPK) Management for Acquirers 104
2.9.17.2 AEIPS Terminal Requirements for the EU/EEA & UK 105
2.9.17.3 PIN Bypass Requirements for Acquirers 105
2.9.17.4 Expresspay-Enabled POS Devices 105
2.9.17.5 AEIPS and Expresspay Enablement Program for Acquirers 106
2.9.18 American Express SafeKey Acquirer Requirements 107
2.9.18.1 Reuse of SafeKey Authentication Data 108
2.9.19 Marketing, Advertising, and Public Relations 108
2.9.20 Transfer of S/E Portfolio 108
2.9.21 No Factoring 109
2.9.22 Cancelled S/E Policy 109
2.10 Requirements for Conducting Card Issuing Business 109
2.10.1 Certification of Card Issuing Programs 110
2.10.1.1 Advanced Payment Product Certification Requirements 110
2.10.1.2 Beta Test of Cards and Expresspay Mobile 111
2.10.1.3 Launch Date 111
2.10.1.4 Card Security Requirements 111
2.10.1.4.1 Card Security Encoding Requirements 111
2.10.1.4.2 Card Security Code (CSC) Validation 111
2.10.1.5 Issuer Liability for Licensed BINs 112
2.10.2 Reporting to AEGNS 112
2.10.2.1 Annual Plan Disclosure 112
2.10.2.2 Fraud Data 112
2.10.3 Cardmember Information - Data Requirements 113
2.10.3.1 Issuers in the United States 113
2.10.3.2 Local Network Card Issuers Outside of the United States 113
2.10.3.3 Non-Local Network Card Issuers Outside of the United States 113
2.10.4 Use of Cardmember Information 113
2.10.4.1 Issuers in the United States and Non-Local Network Card Issuers Outside of the United States 113

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.4.2 Issuers Outside of the United States 113
2.10.4.3 Issuer Obligations 114
2.10.4.4 Third-Party Obligations 114
2.10.5 Cash Disbursement Issuer Requirements 114
2.10.6 Stored Value Digital Facility Issuer Requirements 114
2.10.7 Chip and Contactless Card Requirements 115
2.10.7.1 AEIPS Chip and PIN-Enabled Cards for EU/EEA & UK 115
2.10.7.2 Transaction Requirements for the EU/EEA & UK 115
2.10.7.3 Certification Authority Public Key Management for Issuers 115
2.10.7.4 PIN Bypass Requirements for Issuers 116
2.10.7.5 AEIPS and Expresspay Enablement Program for Issuers 116
2.10.8 Additional Marketing and Advertising Requirements for Issuers 117
2.10.8.1 Brand Advertising 117
2.10.8.2 Incentive Programs 117
2.10.8.3 Issuer Eligible Marketing Region 117
2.10.9 Recurring Billing Cancellation Service Requirements 117
2.10.10 Conversion Rates 118
2.10.11 Transfer or Conversion of Card Portfolio 118
2.10.12 Participation in Securitization Programs 118
2.10.13 American Express SafeKey Issuer Requirements 119
2.10.14 Network Processing Requirements for U.S. and Canadian Issuing Participants 120
2.10.14.1 Automated Address Verification (AAV) 120
2.10.14.2 Name and Address Verification (NAV) Program 120
2.10.14.3 ZIP Code Verification (ZCV) Program 120
2.11 AEGNS' Right to Terminate or Suspend Participant Agreement and/or Authorized Activities 120
2.11.1 Conditions for Immediate Termination or Suspension 120
2.11.2 Conditions for Termination or Suspension Upon Thirty (30) Days' Notification 121
2.12 Expiration or Termination of the Participant Agreement 121
2.12.1 Expiration/Termination of Acquirer Participant Agreement 121
2.12.1.1 Acquirer's Continuing Obligations 121
2.12.1.2 AEGNS' Continuing Obligations 122
2.12.2 Expiration/Termination of Issuer Participant Agreement 122
2.12.2.1 Issuer's Continuing Obligations 122
2.12.2.2 S/E Payables 123
2.12.2.3 AEGNS Rights Upon Termination/Expiration 123
2.12.2.4 AEGNS' Continuing Obligations 123
2.13 Operating Policy Compliance and Enforcement 123
2.13.1 Non-Compliance Fees 123
2.13.2 Determination of Violation 124
2.13.3 Notification of Violation Process 124
2.13.4 Request for Information 124
2.13.5 Action Plans 124
2.13.6 Exceptions 124

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3 Product Features and Specifications 125
3.1 Introduction 125
3.2 Overview of Products Supported by the AEGN 125
3.2.1 Consumer Cards 125
3.2.1.1 American Express Enterprise Line Consumer Cards 126
3.2.1.2 Blue Box Line Consumer Cards 126
3.2.2 Commercial Products 126
3.2.2.1 American Express Enterprise Line Commercial Products 127
3.2.2.2 Blue Box Line Commercial Products 128
3.2.3 Account Card 128
3.2.3.1 Minimum Product Requirements for Account Card 128
3.2.4 Dual Card Account 129
3.2.5 Prepaid Cards 129
3.2.5.1 Types of Prepaid Cards 130
3.2.5.2 U.S. Multi-Network Prepaid Cards 130
3.2.5.3 General Requirements for Issuers of Prepaid Cards 130
3.2.5.4 Prepaid Card Functionality 131
3.2.6 Debit Cards 131
3.2.6.1 U.S. Multi-Network Debit Cards 131
3.2.6.2 General Acceptance Requirements of Debit Cards 131
3.2.7 Chip Cards 131
3.2.7.1 AEIPS-Based Payments 132
3.2.7.2 Contactless Cards (Expresspay) 132
3.3 American Express Enterprise Line Consumer Cards 133
3.3.1 American Express Card (green) 140
3.3.2 American Express Gold Card 141
3.3.3 The Platinum Card 142
3.3.4 The Centurion Card 145
3.3.5 Blue from American Express 148
3.3.6 American Express Credit Card (green) 149
3.3.7 American Express Gold Credit Card 150
3.3.8 American Express Platinum Credit Card 151
3.3.9 American Express Debit Card 151
3.4 American Express Enterprise Line Commercial Products 152
3.4.1 American Express Enterprise Line Small Business Products 152
3.4.1.1 The American Express Business Card 157
3.4.1.2 The American Express Business Gold Card 157
3.4.1.3 The American Express Business Platinum Card 158
3.4.1.4 The Business Centurion Card 159
3.4.1.5 American Express Travel Agency Account 160
3.4.1.6 American Express Business Debit Card 161
3.4.2 American Express Enterprise Line Corporate Products 161
3.4.2.1 American Express Corporate Card 166
3.4.2.2 American Express Corporate Gold Card 166
3.4.2.3 American Express Corporate Platinum Card 167

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.4.2.4 American Express Corporate Purchasing Card 168
3.4.2.5 American Express Corporate Meeting Card 168
3.4.2.6 American Express Business Travel Account 169
3.4.3 Enhanced Functionality Requirements for American Express Enterprise Line Corporate Products 169
3.5 Blue Box Line Consumer Cards 170
3.5.1 Product Tier: Member 173
3.5.2 Product Tier: Select 173
3.5.3 Product Tier: Max 174
3.5.4 Product Tier: Icon 175
3.5.5 Product Tier: Debit 176
3.6 Blue Box Line Commercial Products 176
3.6.1 Blue Box Line Small Business Products 176
3.6.1.1 [Issuer Name] Member Business American Express Card 182
3.6.1.2 [Issuer Name] Select Business American Express Card 182
3.6.1.3 [Issuer Name] Max Business American Express Card 183
3.6.1.4 [Issuer Name] Icon Business American Express Card 183
3.6.1.5 [Issuer Name] American Express Business Purchasing Card 184
3.6.1.6 [Issuer Name] American Express Travel Agency Account 185
3.6.1.7 [Issuer Name] American Express Business Debit Card 185
3.6.2 Blue Box Line Corporate Products 185
3.6.2.1 [Issuer Name] Corporate American Express Card 189
3.6.2.2 [Issuer Name] Gold Corporate American Express Card 189
3.6.2.3 [Issuer Name] Platinum American Express Corporate Card 190
3.6.2.4 [Issuer Name] American Express Business Travel Account 190
3.7 Descriptions of Product Features and Benefits 191
3.7.1 Air Addenda 191
3.7.2 Airport Lounge Access Program 191
3.7.3 Business Travel Accident Insurance 191
3.7.4 Car Rental Insurance 191
3.7.5 Cardless Account 192
3.7.6 Cardmember Communication 192
3.7.7 Cardmember Customer Service 192
3.7.8 Cardmember Employee ID and Cost Center 192
3.7.9 Cardmember Loyalty Programs 192
3.7.10 Cardmember Online Account Access Services 192
3.7.11 Travel Servicing 192
3.7.12 Choice of Billing Frequency 193
3.7.13 Choice of Cycle Cut Dates 193
3.7.14 Company Savings/Loyalty Program 193
3.7.15 Concierge Service 193
3.7.16 Corporate Account Hierarchy 193
3.7.17 Corporate Account Management 194

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.18 Corporate Billing Options 194
3.7.18.1 Corporate Products 194
3.7.18.2 Small Business Products 194
3.7.19 Company Liability Options 194
3.7.20 Dedicated Operations Unit (for Company-Level Service) 194
3.7.21 Descriptive Travel/Customer Reference Data (Matched and Merged with Charge Data) 195
3.7.22 Dining Program/Offers 195
3.7.23 Direct Debit of Monthly Balance or Minimum Payment 195
3.7.24 Electronic Remittance File 195
3.7.25 Emergency Assistance 196
3.7.26 Emergency Card Replacement 196
3.7.27 English Language Support 196
3.7.28 Enhanced Global Management Information System (eGMIS) 196
3.7.29 Field Sales Force 196
3.7.30 Flight Delay and Cancellation Insurance 197
3.7.31 Global Limits 197
3.7.32 Global Rebates 197
3.7.33 Issuer-Generated Data Files 197
3.7.34 Limited Liability for Lost/Stolen Cards 198
3.7.35 Line Item Detail 198
3.7.36 Luggage Delay Protection 198
3.7.37 Luggage Loss Protection 198
3.7.38 Management Information System (MIS) Standard Reporting 198
3.7.39 Merchant Category Restrictions 199
3.7.40 MIS Customized Reporting 199
3.7.41 Online Card Application Form 199
3.7.42 Online Fraud Protection Guarantee 199
3.7.43 Online Program Management 199
3.7.44 Online Reconciliation/Expense Reporting Tool 199
3.7.45 Open Item Billing 200
3.7.46 Option to Extend Payment Terms 200
3.7.47 Premium Product Platform (PPP) 200
3.7.48 Pre-Set Spending Limits 200
3.7.49 Proactive Data Quality Processes 200
3.7.50 Product-Designated Website Pages 201
3.7.51 Promotional Program Capability 201
3.7.52 Publishing Magazine Title 201
3.7.53 Insurance Programs 201
3.7.53.1 Warranty Protection 201
3.7.53.2 Theft and Damage Protection 201
3.7.53.3 Return Protection 202
3.7.54 Insurance Programs 202
3.7.55 Tax Invoice Capture/Presentment 202

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.56 Travel Accident Insurance 202
3.7.57 Travel Accident Insurance - Group Coverage 202
3.7.58 Travel Related Offer Program 202
3.7.59 VAT/GST Information 202
3.7.60 Year-end Summary of Charges 203
3.8 Co-Brand and Affinity Card Agreements 203
3.8.1 Co-Brand and Affinity Card Program 203
3.8.1.1 Blue Box Line Co-Brand and Affinity Card Program 203
3.8.1.2 American Express Enterprise Line Co-Brand Program 203
3.8.2 Ownership and Control of the Co-Brand and Affinity Card Program 203
3.8.3 Approval of Co-Brand and Affinity Partners 204
3.8.4 Approval of Co-Brand or Affinity Programs 204
3.8.5 Advertising Standards and Card Design - Co-Brand and Affinity Partners 205
3.8.6 Co-Brand and Affinity Card - Acceptance Requirements 205
3.9 Issuer-Provided Services 205
3.9.1 Issuer-Provided Card Account Services 206
3.9.1.1 Account Setup and Plastic Issuance 206
3.9.1.1.1 Consumer Account Setup and Plastic Issuance 206
3.9.1.1.2 Corporate Card Program Account Setup and Plastic Issuance 206
3.9.1.2 Billing and Collections 206
3.9.1.3 Card Pricing 207
3.9.1.4 Card Validity Period 207
3.9.1.5 Card Production 207
3.9.1.6 Cardmember Agreement/Solicitation Materials 207
3.9.1.6.1 Disclosure of Foreign Currency Factor 207
3.9.1.6.2 Notice Regarding Cardmember Information 208
3.9.1.6.3 Other Requirements 208
3.9.1.7 Additional Information for Prepaid Card Cardmember Agreement/Solicitation and/or Fulfillment Materials 208
3.9.1.8 Legal Compliance 209
3.9.1.9 Risk Assessment 209
3.9.2 Issuer-Provided Core Card Services 209
3.9.2.1 Cardmember Customer Service 209
3.9.2.2 Cash Access 210
3.9.2.2.1 Cash Advances 210
3.9.2.2.2 Cash Disbursements 210
3.9.2.2.3 Cash Withdrawal 210
3.9.2.2.4 Access to Participant's ATM Network 210
3.9.2.2.5 Access to Participant's Shared ATM Network 210
3.9.2.2.6 Access to the Amex Shared ATM Network 210
3.9.2.2.7 Cash Access at Issuer's Branch Locations 210
3.9.2.2.8 PIN Issuance 210
3.9.2.3 Additional Optional ATM Services 211
3.9.3 Additional Services for Prepaid Cards 211
3.9.3.1 Funding of Prepaid Cards 211

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.9.3.2 Return of Prepaid Card Funds on Card Cancellation or Card Expiry 212
3.9.4 Additional Features 212
3.9.4.1 Guidelines for Additional Features 212
3.9.4.2 Approval Process for Additional Features 213
3.10 Issuer Access to American Express Sourced Benefits 213

4 S/E and ATM Standards 214
4.1 Introduction 214
4.2 S/E Card Acceptance Procedures 214
4.2.1 Split Shipment Transactions 214
4.2.2 Multiple ROC Transactions with Single Authorization 214
4.2.3 Card Acceptance Restrictions 214
4.2.4 Discounts on Purchases 215
4.2.5 Discriminatory Treatment 215
4.2.5.1 Co-Brand and Affinity Partners 215
4.2.6 Printed Card Security Code (PCSC) Validation 215
4.2.7 In-Person Charges 216
4.2.7.1 Obtaining Signature for In-Person Charges 217
4.2.7.2 Service Code Interrogation Requirements 217
4.2.8 Expresspay Acceptance 217
4.2.9 Expresspay Transactions at Transit Access Terminals (TATs) 218
4.2.9.1 TAT S/E Requirements 218
4.2.9.1.1 Card Acceptance Requirements for Expresspay Transactions at TATs 218
4.2.9.1.2 Authorization Requirements for Expresspay Transactions at TATs 219
4.2.9.1.3 Submission Requirements for Expresspay Transactions at TATs 219
4.2.9.1.4 Charge ROC Requirements for Expresspay Transactions at TATs 220
4.2.9.2 S/E-Initiated Transit Debt Recovery 220
4.2.9.3 S/E Management of the Deny List 221
4.2.9.4 Expresspay Card or Expresspay Mobile for Pay-In-Advance Transit Fares 221
4.2.10 Card Not Present Charges 221
4.2.10.1 Internet S/E Card Acceptance Requirements 222
4.2.10.2 American Express SafeKey Card Acceptance Requirements 222
4.2.10.3 Online Order/In-Store Pick-up Transaction Processing 222
4.2.11 Credentials-on-File 223
4.2.12 Merchant-Initiated Transactions 223
4.2.13 Aggregated Transactions 224
4.2.13.1 General Requirements 224
4.2.13.2 Submission Requirements 224
4.2.14 Customer Activated Terminals 224
4.2.15 Recurring Billing 225
4.2.15.1 Introductory Offers 225
4.2.16 Installment Sales 226
4.2.17 Acceptable Forms of ID 226
4.2.18 Non-Real Time (Delayed) Authorizations 226

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.19 Estimated Charge Amounts 227
4.2.19.1 Lodging 227
4.2.19.2 Cruise Lines 227
4.2.19.3 Car Rental 227
4.2.19.3.1 Capital Damages to Rental Vehicles - Charge Submission Requirements 228
4.2.19.3.2 Capital Damages to Rental Vehicles - Documentation 228
4.2.19.4 Restaurants and Bars 228
4.2.19.5 Taxicabs/Limousines 229
4.2.19.6 Card Not Present Grocery and Retail 229
4.2.20 Special Programs 229
4.2.20.1 No Show Reservations Program 229
4.2.20.1.1 Lodging Reservation 229
4.2.20.1.2 Lodging Cancellation 229
4.2.20.1.3 Alternate Lodging Accommodations 230
4.2.20.2 No Show Reservation Requirements for Other Industries 230
4.2.20.2.1 Rental Reservation 230
4.2.20.2.2 Rental Cancellation 230
4.2.20.2.3 Alternative Rental Services 231
4.2.20.3 Advance Deposit or Payment Program 231
4.2.20.3.1 Reservation Policy Disclosure 231
4.2.20.3.2 Cancellation Policy Disclosure 231
4.2.20.3.3 Alternate Accommodations 231
4.2.20.4 No Signature/No PIN Program 232
4.2.20.5 ZIP Code Verification (ZCV) Program 233
4.2.20.6 Name and Address Verification (NAV) Program 233
4.2.20.7 Promotional Program Capability 233
4.2.20.8 POS Online PIN Certification and Enablement Program 234
4.2.21 Charge ROCs 236
4.2.21.1 Completing Charge ROCs 237
4.2.22 Credit ROCs 237
4.2.22.1 Completing Credit ROCs 237
4.2.22.2 Credit ROC Restrictions 238
4.2.23 Delayed Delivery 238
4.3 Code 10 238
4.3.1 Suspect Cards 238
4.3.2 Suspect Cardmember 239
4.3.3 Card Capture 239
4.4 Card Recovery 239
4.4.1 Card Recovery Criteria, Procedures and Cash Awards 239
4.4.2 Recovered Card Reporting and Cash Award - Acquirer Responsibilities 240
4.4.3 Recovered Card Reporting and Cash Award - Issuer Responsibilities 240
4.4.4 Payment of the Cash Award 240
4.5 Cash Disbursements 240
4.5.1 Card Acceptance Requirements for Cash Disbursement Providers 240
4.6 ATM Requirements 241

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.6.1 ATM Access - Acquirers 242
4.6.1.1 Terminal Requirements 242
4.6.1.2 ATM Transaction Processing 242
4.6.1.3 ATM Card Acceptance 243
4.6.1.3.1 Service Delivery 243
4.6.1.3.2 Transaction Log Archival Storage 243
4.6.1.3.3 ATM Security Pictures 243
4.6.2 ATM Access - Issuers 243
4.6.3 ATM Card Capture 243
4.6.4 ATM Locations 244

5 Authorizations 245
5.1 Introduction 245
5.2 Authorization Processing 245
5.2.1 Online Authorization Processing 245
5.2.1.1 Online Authorization Request 245
5.2.1.2 Online Authorization Response 245
5.2.1.3 Online Authorization Process 245
5.2.2 Chip Card (Offline) Authorizations 246
5.2.2.1 Chip Card (Offline) Authorization Process 246
5.2.2.2 Chip Card Fallback 246
5.3 AEGNS Authorization Services 247
5.3.1 ATM and POS Authorization Message Routing 247
5.3.2 Activity Logging 247
5.3.2.1 Authorization Log Records 247
5.3.3 Prepaid Card Authorization Processing 248
5.3.4 Authorization Reversals 248
5.3.5 Authorization on Credit 249
5.3.6 Authorization Adjustments 249
5.3.7 Address Verification 250
5.3.8 Authorizations Support 250
5.3.9 BIN Blocking 250
5.3.10 Currency Conversion 250
5.3.11 Deferred Payment Plan (DPP) 250
5.3.12 Fraud and Risk Scoring Service 250
5.3.13 Cash Disbursements 251
5.3.14 Participant Reporting 251
5.3.15 Stand-In Authorization Service 251
5.3.16 System Outage Resolution 251
5.4 Issuer Authorization Requirements 251
5.4.1 Hours of Operation 252
5.4.2 Notification of Scheduled Outages 252
5.4.3 Notification of Unscheduled Outages 252
5.4.4 Issuer Authorization Response Standards 252

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.5 Acquirer Authorization Requirements 253
5.5.1 Hours of Operation 253
5.5.2 Authorization Systems for S/Es 253
5.5.3 Cancelled S/E Policy 253
5.5.4 System Outage Notification 253
5.6 POS Authorization Requests 253
5.6.1 Card Present Authorization Requests 254
5.6.1.1 Magnetic Stripe Authorization 254
5.6.1.2 Key-Entered Authorization 254
5.6.1.3 AEIPS Authorization 254
5.6.1.4 Expresspay Authorization 254
5.6.2 Card Not Present Authorization Requests 254
5.6.2.1 Key-Entered Authorization 254
5.6.2.2 Card Not Present Recurring Billing Authorizations 254
5.6.3 Voice Authorization 255
5.7 Authorization Responses 255
5.7.1 POS Online Response Messages 255
5.8 Stand-In Processes 256
5.8.1 Host Stand-In 257
5.8.1.1 Types of Host Stand-In Tables 257
5.8.1.2 Unsupported Functions and Features 257
5.8.1.3 Mandatory Host Stand-In 5-Digit Card Security Code (5CSC) Requirements 258
5.8.1.4 Optional Host Stand-In Features 258
5.8.2 Remote Stand-In 258
5.8.2.1 Types of Remote Stand-In Tables 258
5.8.2.2 Unsupported Functions and Features 259
5.8.3 Scheduled Stand-In 259
5.8.4 Unscheduled Stand-In 259
5.8.5 Stand-In Authorization Parameters 259
5.8.6 Stand-In Table 260
5.8.7 Exception File 260
5.8.8 Network Authorization Decision Making Process During Issuer Stand-In 260
5.8.9 Store and Forward Process 261
5.8.10 Stand-In Processing Legal Disclaimer 261
5.9 Network Floor Limits 261
5.9.1 Chip Fallback Floor Limits 261
5.10 Authorization Features 261
5.10.1 Address Verification 261
5.10.1.1 Automated Address Verification 262
5.10.1.2 Name and Address Verification (NAV) Program 262
5.10.1.2.1 S/E Requirements 262
5.10.1.2.2 Issuer Requirements 262
5.10.2 Cardholder Verification Methods 263
5.10.3 Deferred Payment Plan (DPP) 263
5.10.3.1 Issuer-Based Deferred Payment Plan 263

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.10.3.2 Acquirer-Based Deferred Payment Plan 263
5.10.4 CSC Feature 264
5.10.4.1 5CSC 264
5.10.4.2 4DBC and 4CSC 265
5.10.4.3 3CSC 265
5.10.4.4 iCSC 266
5.10.4.5 One-Time Password (OTP) 266
5.11 ATM Authorizations 266
5.11.1 ATM Authorization Process - End to End 266
5.11.2 ATM Acquirer Authorization Standards 267
5.11.2.1 Hours of Operation 267
5.11.2.2 Authorization Systems 267
5.11.2.3 Authorization Message Content 267
5.11.2.4 System Outage Notification 267
5.11.3 ATM Authorization Requests 268
5.11.3.1 ATM Location Requirements 268
5.11.3.2 Personal Identification Number (PIN) 268
5.11.4 ATM Authorization Responses 268

6 Clearing and Settlement 269
6.1 Introduction 269
6.2 Overview 269
6.2.1 The Transaction Life Cycle 269
6.2.2 Time Usage in the Business and Operational Policies Manual 269
6.3 Clearing Procedures 269
6.3.1 Presentment and Acceptance of Transaction 270
6.3.2 Submission Process 270
6.3.2.1 Message Type 270
6.3.2.2 Message Order 270
6.3.2.3 Message Outclearing 271
6.3.2.4 Cancelled S/E Submissions 271
6.3.2.5 Message Inclearing 271
6.3.3 Settlement Schedule 271
6.3.4 Scheduled Outages 271
6.3.5 Clearing and Settlement Financial Life Cycle and Processing Times 272
6.3.6 Bank Holidays - Clearing 272
6.4 Settlement and Funds Exchange 272
6.4.1 Settlement Process 272
6.4.1.1 Daily Activity Process 273
6.4.1.2 Settlement Advisement 273
6.4.2 Funds Exchange 273
6.4.2.1 Automated Funds Exchange 273
6.4.2.2 Manual Funds Exchange 274
6.4.2.3 Foreign Exchange Conversion Rate Establishment 274
6.4.2.3.1 Foreign Exchange on Chargebacks 274

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.4.3 Settlement Exceptions 274
6.4.3.1 Bank Holidays - Settlement 275
6.4.3.2 Participant Failure to Settle on a Timely Basis 275
6.4.3.3 AEGNS Failure to Settle on a Timely Basis 275
6.4.3.4 Participant Liability for Net Settlement 276
6.4.3.5 Delay in Daily Settlement Advisement 276
6.4.3.6 Unjust Enrichment and Compensation Computation 277
6.4.3.6.1 Compensation to the Participant 277
6.4.3.6.2 Compensation from the Participant 277
6.4.3.7 Funds Exchange Dispute Process 277
6.4.3.8 Delays 277
6.4.3.9 Currency Restrictions and Exchange Controls 278
6.4.3.10 Suspension of Settlement 279
6.5 Double Byte Character (DBC) Support 279

7 Chargeback Policies 280
7.1 Introduction 280
7.2 Chargeback Policies Overview 280
7.2.1 Handling of Disputed Transactions 281
7.3 The Transaction Life Cycle 281
7.3.1 Authorization Processing 281
7.3.1.1 Authorization Request 281
7.3.1.2 Authorization Response 282
7.3.2 Clearing and Settlement Processing 282
7.3.2.1 Presentment 282
7.3.2.2 Retrieval Request 282
7.3.2.3 Fulfillment 282
7.3.2.4 First Chargeback 283
7.3.2.5 Second Presentment 283
7.3.2.6 Final Chargeback 284
7.3.2.7 Dispute Transaction Fees 284
7.3.2.8 Dispute Message Reject Fee 285
7.3.2.9 Good Faith 285
7.3.2.10 Pre-Arbitration 285
7.3.2.11 Arbitration Filing 285
7.3.2.12 Pre-Compliance Requirement 285
7.3.2.13 Compliance Filing 285
7.3.2.14 Documentation Delivery 285
7.3.3 Disputes Process Transaction Life Cycle 286
7.4 Retrieval Request and Fulfillment 288
7.4.1 Fulfillment Notification Reason Codes 293
7.4.2 Itemized Documentation Codes 294
7.5 Fulfillment Data Requirements 294
7.5.1 Fulfillment Data Requirement Tables 295
7.6 Second Presentment Data Requirements 300

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.7 Compelling Evidence 301
7.8 Process Timeframes 303
7.9 Chargeback Policy Rules 304
7.9.1 Retrieval Chargeback Types 304
7.9.2 Authorization Chargeback Types 304
7.9.3 Processing Error Chargeback Types 304
7.9.4 Cardmember Dispute Chargeback Types 305
7.9.5 Fraud Chargeback Types 305
7.9.5.1 Fraud Data Entry Requirement 305
7.9.5.2 Counterfeit Card Chargeback Restriction 305
7.9.6 Chargeback Reasons "At A Glance" 306
7.9.7 Description of the Chargeback Format 307
ISO Code - A 4-Digit Message Reason Code for the Chargeback 307
ISO 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented 309
ISO 4512 - Multiple Processing 311
ISO 4513 - Credit Not Presented 312
ISO 4515 - Paid Through Other Means 316
ISO 4516 - Request for Support Not Fulfilled 317
ISO 4517 - Request for Support Illegible/Incomplete 319
ISO 4521 - Invalid Authorization 321
ISO 4523 - Unassigned Cardmember Account Number 325
ISO 4527 - Missing Imprint 326
ISO 4530 - Currency Discrepancy 327
ISO 4534 - Multiple ROCs 328
ISO 4536 - Late Presentment 329
ISO 4540 - Card Not Present 330
ISO 4544 - Cancellation of Recurring Goods/Services 332
ISO 4553 - Not as Described or Defective Merchandise 334
ISO 4554 - Goods and Services Not Received 337
ISO 4750 - Car Rental Charge Non-Qualified or Unsubstantiated 341
ISO 4752 - Credit/Debit Presentment Error 343
ISO 4754 - Local Regulatory/Legal Dispute 344
ISO 4755 - No Valid Authorization 345
ISO 4763 - Fraud Full Recourse 348
ISO 4798 - Fraud Liability Shift - Counterfeit 350
ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-Received 352
7.10 Chargeback Policy Requiring Special Handling 354
7.10.1 AEGNS Network Disputes Manager-Processed Transactions 354
7.10.2 Chip Card Special Handling 354
7.10.3 ATM Chargebacks 354
7.10.4 Cash Disbursement 355
7.10.5 Special Programs 356
7.10.5.1 No Signature/No PIN Program 356
7.10.5.2 ZIP Code Verification (ZCV) Program 356
7.10.6 Expresspay 357

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.7 Digital Wallet Program 358
7.10.8 Fraud Liability Shift 359
7.10.8.1 AEIPS Fraud Liability Shift (FLS) 359
7.10.8.1.1 Types of AEIPS FLS 360
7.10.8.1.2 PIN Capable and Enabled POS Devices 360
7.10.8.2 Fallback 360
7.10.8.3 American Express SafeKey Fraud Liability Shift 361
7.10.9 Promotional Program Transactions 362
7.10.10 Merchant-Presented Quick Response 363
7.11 Good Faith 364
7.11.1 Good Faith Request 364
7.11.2 Good Faith Filing Procedures 364
7.11.2.1 Automated Good Faith Submission 365
7.11.2.2 Manual Good Faith Submission 365
7.11.3 Good Faith Processing Timeframes 365
7.11.4 Good Faith Fees 365
7.11.5 Good Faith Submission Address 366
7.11.6 Good Faith Corrections and Reversals 366
7.11.7 Good Faith Arbitration Withdrawal Procedure 366
7.12 Arbitration and Compliance 366
7.12.1 Arbitration 366
7.12.1.1 Arbitration Filing Procedures 367
7.12.1.2 Arbitration Submission Timeframe 368
7.12.1.3 Arbitration Fees 368
7.12.1.4 Arbitration Withdrawal Procedures 369
7.12.2 Compliance 369
7.12.2.1 Compliance Filing Procedures 370
7.12.2.2 Compliance Submission Timeframe 371
7.12.2.3 Compliance Fees 371
7.12.2.4 Compliance Withdrawal Procedures 372
7.12.3 AEGNS Arbitration and Compliance Filing Review Process 372
7.12.3.1 Review Process for Accepted Filings 373
7.12.3.1.1 Filing Review Process Timeframe 374

8 Security and Fraud 375
8.1 Introduction 375
8.2 Card Production 375
8.2.1 Certification Requirements for Card Production 375
8.2.2 Sensitive Materials 376
8.2.3 Access Control 376
8.2.4 Notification in Case of Loss or Theft During Card Production 377
8.2.5 Reporting in Case of Loss or Theft During Card Production 377
8.2.6 Card Production Audit Controls 378
8.3 Shipments from Card Manufacturer to Card Personalization Site 378
8.4 Delivery of Personalized Cards to Cardmembers 378

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.4.1 Preparation for Delivery 378
8.4.2 Precautions Against Mail Theft 378
8.4.3 Return of Undeliverable Cards 379
8.4.4 Card Activation 379
8.5 Participant Security Management 379
8.5.1 Security Office 379
8.5.1.1 Security Contact Information 380
8.5.2 Investigations 380
8.5.2.1 Investigative Responsibilities 380
8.5.2.2 Fraud Recoveries 380
8.5.3 AEGNS Fraud and Security Investigation Services 381
8.6 FraudNet 381
8.6.1 FraudNet Registration 382
8.6.2 FraudNet Training 382
8.7 Issuer Fraud Reporting 382
8.7.1 Issuer Fraud Data Entry 383
8.8 AEGNS Fraud Reports 383
8.9 AEGNS Acquirer and S/E Risk Management 383
8.9.1 High Risk S/E List 383
8.9.1.1 Removing an S/E from the High Risk S/E List 384
8.9.2 High Risk S/E Criteria 385
8.9.2.1 Fictitious and/or Collusive S/E 385
8.9.2.2 Illegal or Prohibited Industry 385
8.9.2.3 Fraud to Gross Sales Volume Ratio 386
8.9.2.4 High Risk S/E Industries 386
8.9.2.5 Cancelled S/Es (Derogatory) 387
8.9.3 S/E Risk Management 388
8.9.3.1 Acquirer UIR 388
8.9.3.2 Acquirer Participant Communication Platform (PCP) 389
8.9.4 S/E Actioning System (SEAS) 389
8.9.4.1 High Risk Listing Recommendations 389
8.9.4.2 Manual Review Recommendations 390
8.9.4.3 SEAS Compliance Monitoring 390
8.9.5 AEGNS Investigation of S/Es 390
8.9.6 S/E Monitoring for Fraud Liability Shift Eligibility 391
8.9.6.1 American Express SafeKey Fraud Liability Shift Qualification S/E Fraud Thresholds 391
8.10 AEGNS Issuer and Cardmember Risk Management 391
8.10.1 Card Security 391
8.10.2 5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program 392
8.10.3 Cardmember Risk Management 392
8.10.3.1 Dynamic Fraud Management 393
8.10.3.1.1 Issuer Override Request and Fraud Liability 394
8.10.3.1.2 Dynamic Fraud Management Network Services 394

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.10.3.1.3 Dynamic Fraud Management Network Services Use 394
8.10.3.2 Issuer UIR 395
8.10.3.3 Recurrent Cardmember Fraud 395
8.10.3.4 Issuer Participant Communication Platform (PCP) 396
8.10.4 Issuer Fraud Rate 396
8.10.5 Fraud Risk Services 396
8.10.5.1 SafeKey On-Behalf-Of Services 397
8.10.5.2 AEIPS and Expresspay On-Behalf-Of Services 397
8.11 Fraud Mitigation Practices 397

9 AEGNS Service Performance Program 400
9.1 Internal Service Metrics 400
9.2 AEGNS Servicing Action Plan 400

10 Network Fees 401
10.1 Introduction 401
10.2 Disputes Fees 401
10.2.1 Network Disputes Manager License Fees 401
10.2.2 Pre-Arbitration and Pre-Compliance Processing Fees 401
10.2.3 Arbitration Fees 402
10.2.4 Good Faith Fees 402
10.2.5 Compliance Fees 402
10.2.6 Dispute Transaction Fees 402
10.2.7 Dispute Message Reject Fee 403
10.3 Fraud Fees 403
10.3.1 Fraud Non-Compliance Fee Schedule A 403
10.3.2 Violations Subject to Fraud Non-Compliance Fee Schedule A 404
10.3.3 5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program Non-Compliance Fees 405
10.3.4 Security and Fraud Investigation Service Fees 405
10.3.5 FraudNet License Fees 405
10.3.6 Urgent Investigation Request (UIR) Fees 406
10.4 Network Connectivity Fees 406
10.4.1 GLOBE Fees 406
10.4.2 GLOBE Relocation Fees 406
10.4.3 Internet Virtual Private Network Fees 406
10.5 Service Fees 406
10.5.1 Remittance Fees 407
10.5.2 Product Enhancement Service Fees 407
10.5.3 Fees for Additional Cardmember Benefits and Services 407
10.5.4 ATM Service Fees 407
10.5.5 Active BIN Rental Fee 407
10.5.6 Network Test Simulator Fees 407
10.5.7 Manual Funds Exchange Processing Fee 408
10.5.8 Settlement Advisement Fee 408

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.5.9 Late Settlement Fee 408
10.5.10 Funds Exchange Reissue Fee 408
10.5.11 Premium Product Platform (PPP) Fees 409
10.5.12 Issuer Personalization Certification Testing 409
10.5.12.1 Online Personalization Validation Tool Fees 410
10.5.12.2 AEGNS-Led Issuer Personalization Certification Testing Fees 410
10.6 Data Security Fees 411
10.6.1 Data Security Policy (DSP) Non-Compliance Fees 411
10.6.2 Notification of Data Compromise Non-Compliance Fees 411
10.7 Miscellaneous 411
10.7.1 General Non-Compliance Fees 411
10.7.2 Brand Protection Fees 412
10.7.2.1 Brand Protection Assessment Fees 412
10.7.2.2 Brand Protection Non-Compliance Fees 412
10.7.3 Reporting Fees 413
10.7.3.1 Portfolio Reporting Fee 413
10.7.4 Network Assessment Program Reports and Fees 414

11 AEGNS Systems Access and Interface Requirements 415
11.1 Introduction 415
11.2 AEGNS Systems User Access Policy 415
11.2.1 Requesting Access to AEGNS Systems 415
11.2.2 Access Control Policy 416
11.2.3 User Level Policy 416
11.2.4 Information Security Awareness Training 417
11.2.5 Timely Notification of Changes in User Access 417
11.2.6 User Re-Certification 418
11.2.7 Confidentiality 418
11.2.8 Security Policy Violations 418
11.3 AEGNS Email Policy 418
11.3.1 Transport Layer Security Configuration Implementation 419
11.3.2 Domain Name System Requirements 419
11.4 Security 419
11.4.1 Connectivity Security 419
11.4.2 Information Security 419
11.5 Participant Connectivity to the Network 419
11.5.1 The GLOBE 420
11.5.1.1 Additional Requirements 420
11.5.1.1.1 Terms and Conditions 420
11.5.1.1.2 Risk of Loss 421
11.5.1.1.3 Insurance 421
11.5.1.1.4 GLOBE Relocation 422
11.5.1.1.5 GLOBE Returns 422
11.5.1.2 General 422
11.5.2 Internet Virtual Private Network Connections 423

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.5.2.1 Additional Requirements 423
11.6 Terminal Access 423
11.7 Network Test Simulator 424
11.7.1 Network Test Simulator Definitions 424
11.7.2 Requirements 425
11.7.2.1 Access to Service and Use 425
11.7.2.2 Fee 425
11.7.3 General 425
11.7.4 Termination and Return of Materials 426

12 Exhibits 427
Exhibit 1. AEGNS Internet Marketing Communications Policies and Guidelines (IO/JV) 427
Exhibit 2. AEGNS Internet Marketing Communications Policies and Guidelines (NCL) 438
Exhibit 3. Confidentiality Letter 447
Exhibit 4. Guaranty Agreement 448
Exhibit 5. Secure Remote Commerce Terms and Conditions 451
Exhibit 6. No Signature/No PIN Program Thresholds 453
Exhibit 7. European Economic Area Data Protection Model Contracts 454
Exhibit 8. Single Charge and VIP Stand-In Parameter Table 464
Exhibit 9. Velocity-Based Stand-In Parameter Table 467
Exhibit 10. Benefit Participation Terms and Conditions 472
Exhibit 11. AEGNS ATM Exception/First Presentment (DR) and Reversal (CR) 475
Exhibit 12. AEGNS Card Recovery Award Form 478
Exhibit 13. Reserved 480
Exhibit 14. AEGNS CDCRP Issuer Claim Form 481
Exhibit 15. Dynamic Fraud Management Network Services Terms and Conditions 482
Exhibit 16. Reserved 484
Exhibit 17. Floor Limit Table 485
Exhibit 18. AEGNS Good Faith Form 486
Exhibit 19. Neutrality Principles for Conducting Merchant Acquiring Business 489

13 Abbreviations and Acronyms 490
13.1 Abbreviations and Acronyms 490

14 Definitions 495
14.1 Definitions 495

Index 523

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

List of Tables

Table 1-1. Services Provided by AEGNS 6
Table 2-1. Regional Retrieval Request Threshold 29
Table 2-2. Regional First Chargeback Threshold 29
Table 2-3. Participant GDMP Status 30
Table 2-4. S/E and Service Provider Compliance Validation Requirements 42
Table 2-5. CDCRP Financial Liability Relief 50
Table 2-6. Digital Capabilities Enablement Issuer Guidelines 52
Table 2-7. Digital Capabilities AEGNS Optional On-Behalf-Of Services 53
Table 2-8. Digital Wallet Program On-Behalf-Of Services 62
Table 2-9. Indirect Acceptor Merchant Category Code Requirements 76
Table 2-10. Allowed Industries for Bill Payment Providers Facilitating Consumer Payments 77
Table 2-11. Restricted Industries Requirements 95
Table 2-12. Investigation Time Periods 99
Table 2-13. CAPK Management Life Cycle 104
Table 2-14. AEIPS and Expresspay Enablement Program - Acquirer Countries 106
Table 2-15. Acquirer SafeKey Support Requirements 107
Table 2-16. CAPK Management Life Cycle 116
Table 2-17. AEIPS and Expresspay Enablement Program - Issuer Requirements 116
Table 2-18. Issuer SafeKey Support Requirements 119
Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards 133
Table 3-2 Features and Benefits for American Express Enterprise Line Small Business Commercial Products 152
Table 3-3 Features and Benefits for American Express Enterprise Line Commercial Corporate Products 161
Table 3-4 Features and Benefits for Blue Box Line Consumer Cards 170
Table 3-5 Features and Benefits for Blue Box Line Small Business Commercial Products 177
Table 3-6 Features and Benefits for Blue Box Line Corporate Commercial Products 185
Table 4-1. Expresspay at TAT - Operational Parameters 219
Table 4-2. Expresspay at TAT - Declined Authorizations 220
Table 4-3. Ineligible Merchant Category Codes for the No PIN Program 232
Table 4-4. Promotional Program Markets 233
Table 4-5. POS Online PIN Certification and Enablement Program Participation 235
Table 5-1 Designated Acquirer Countries to Support Prepaid Card Authorization-Related Services 248
Table 5-2 POS Online Response Messages 256
Table 5-3 Cardholder Verification Methods 263
Table 6-1. Settlement Exception Processes 275
Table 7-1 Disputes Process Transaction Life Cycle Steps 287
Table 7-2 Retrieval Request - Description for Use 288
Table 7-3 Retrieval Request Notification Reasons 289
Table 7-4. Fulfillment Notification Reason Codes 293
Table 7-5. Itemized Documentation Codes 294
Table 7-6 Data Required on all Fulfillments, Regardless of Industry 295
Table 7-7 Data Required for Airline Industry 296
Table 7-8 Additional Data Required for Car Rental Industry 296
Table 7-9 Additional Data Required for Lodging Industry 297
Table 7-10 Additional Data Required for Restaurant Industry 298
Table 7-11 Additional Data Required for Communication Industry 298
Table 7-12 Additional Data Required for ATM Transactions 299
Table 7-13 Additional Data Required for Mail Order/Telephone Order/Internet Order 299
Table 7-14 Second Presentment Message Reason Codes 300

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-15 Compelling Evidence as a Second Presentment Responsibility 301
Table 7-16 Process Timeframes 303
Table 7-17 Chargeback Reasons 306
Table 7-18. Allowable Codes for ATM Dispute-Related Messages 355
Table 7-19. Allowable Codes for Cash Disbursement Messages 356
Table 7-20. Allowable Codes for No Signature/No PIN Program 357
Table 7-21. Allowable Codes for ZCV Program 357
Table 7-22. Allowable Codes for Expresspay Transactions 358
Table 7-23. Allowable Codes for Digital Wallet Payments Transactions 359
Table 7-24. AEGNS Assignment of Liability Detail 360
Table 7-25. AEIPS Lost/Stolen/Non-Received FLS Participation 361
Table 7-26. Allowable Codes for SafeKey 363
Table 7-27. Allowable Codes for Merchant-Presented Quick Response 364
Table 8-1. Derogatory Status Reason Codes (Cancellation) 388
Table 8-2 Fraud Mitigation Practices 398
Table 10-1. Network Disputes Manager Fees 402
Table 10-2. Arbitration Fees 403
Table 10-3. Compliance Fees 403
Table 10-4 Dispute Transaction Fees 403
Table 10-5 Dispute Message Reject Fee 404
Table 10-6. Fraud Non-Compliance Fee Schedule A 404
Table 10-7 Violations Subject to Fraud Non-Compliance Fee Schedule A 405
Table 10-8. 5CSC and iCSC Program Non-Compliance Fees 406
Table 10-9. FraudNet Reporting Fees 406
Table 10-10. FraudNet Reporting Fees 407
Table 10-11. Active BIN Rental Fees 408
Table 10-12. Network Test Simulator Fees 408
Table 10-13. Manual Funds Exchange Processing Fees 409
Table 10-14. Settlement Advisement Fee 409
Table 10-15. Late Settlement Fee 409
Table 10-16. Funds Exchange Reissue Fee 409
Table 10-17. Premium Product Platform (PPP) Fees 410
Table 10-18. Online Personalization Validation Tool Fees 411
Table 10-19. AEGNS-Led Issuer Personalization Certification Testing Fees 411
Table 10-20. Data Security Policy (DSP) Non-Compliance Fees 412
Table 10-21. General Non-Compliance Fees 412
Table 10-22. Brand Protection Assessment Fees 413
Table 10-23. Brand Protection Non-Compliance Fees 413
Table 10-24. Portfolio Reporting Fees 414
Table 10-25. Report Availability and Fees 415
Table 10-26. Operational Support Fee Schedule 415
Table 11-1. GLOBE Relocation Requirements 423
Table 11-2. Network Test Simulator Definitions 425
Table 12-1 ATM Exception First Presentment and Reversal Form Field Definitions 478
Table 12-2 Card Recovery Award Claim/Recovery Advice Form Field Definitions 480
Table 12-3 Floor Limits–Alphabetical Order by Country (All Countries) 486
Table 12-4 Network Good Faith Form Definitions 488
Table 13-1. Abbreviations and Acronyms 491
Table 14-1. Definitions 496

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

List of Figures

Figure 1-1 Transaction Life Cycle 10
Figure 5-1 5CSC Location on Cards 264
Figure 5-2 4CSC/4DBC Location on Cards 265
Figure 5-3 3CSC Location on Cards 265
Figure 5-4 iCSC Location on Cards 266
Figure 7-1 Disputes Process Transaction Life Cycle Flow 286

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1 Introduction

1.1 Introduction to this Manual

The *Business and Operational Policies manual* is intended to give American Express Global Network (AEGN) Acquirers and Issuers the information necessary to participate in the AEGN as required by their Agreements. The policies in this edition replace previous versions of the *Business and Operational Policies manual* and supersede all other American Express published policies on the same subject.

All policy in this manual is effective at the date of publication, unless otherwise stated.

1.1.1 AEGNS Relationship with American Express Company

American Express Global Network Services (AEGNS) is a business unit within American Express Travel Related Services Company, Inc., which is a subsidiary of American Express Company. AEGNS has responsibility for the operations of the AEGN including such areas as brand management, marketing, operations, settlement, Management Information Services (MIS), telecommunications, and systems.

1.1.2 How the *Business and Operational Policies* Manual is Organized

American Express Global Network Services (AEGNS) is responsible for establishing policies and maintaining them via published manuals which are updated regularly. Participants are provided with a set of AEGN manuals upon signing an Agreement with an American Express Entity.

The *Business and Operational Policies manual is one of such manuals and* is divided into chapters referencing the policies of specific categories in the AEGN. Each chapter begins with a brief introduction of that chapter.

1.1.3 Conventions Used in this Manual

The *Business and Operational Policies manual* utilizes the following conventions throughout.

1.1.3.1 Grammar and Usage

All reference to "time" is stated in Eastern Time (ET in the United States). The use of "day" or "days" refers to calendar days.

A plural usage of a term also includes the singular. Additionally, the singular includes the plural. For example, the use of "a Participant" would include "all Participants." The reverse is also true; "all Participants" applies to individual Participants.

1.1.3.2 Style and Symbols

Words that are capitalized in this manual have specific meaning in the context of the *Business and Operational Policies manual*. See the "Definitions" chapter beginning on page 495 for any word or term in question.

References to this manual and other manuals are printed in *Italics*[1]. The use of **Bold** is for visual emphasis.

All changes to the *Business and Operational Policies* manual will be indicated with a change bar. A change bar is a vertical line in the left margin that visually identifies new or revised text. **Only** substantive changes will be listed in the Summary of Changes for this Edition table. Substantial changes are defined as those changes having potential impact to Participants' operational procedures. Sections of this manual that are deleted will be referenced using the section numbering from the previous publication. This will avoid confusion from any auto-numbering changes that may occur in this publication.

1. References to specific Network Specifications manuals will appear in italics. General references to the set of Network Specifications manuals will not appear in italics. Content-specific Network Specifications manual titles are included in Section 1.4, "Related AEGNS Manuals, Guidelines, and Resources," on page 3.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.



A trash can icon has been placed in the margin next to any significant deletion of text, including sections, tables, paragraphs, notes, and bullet points. An example of this icon appears in the margin next to this paragraph. If text has been deleted and changed, a change bar will appear next to the trash can icon.

Note: A "Note" indicates supplemental information regarding a section in the manual. This paragraph is an example of a Note.

1.2 English Language

The official version of the *Business and Operational Policies* manual is in English, which language shall be controlling in all respects. All AEGN Agreements, forms, reports, and other documents that are furnished by either a Participant or AEGNS to the other, including any changes made by the recipient, shall be in the English Language. Cardmember and Service Establishment (S/E) agreements and related materials used by a Participant in a language other than English must be submitted to AEGNS in English and in such other language(s).

Participants may translate, at their sole expense, any part or all of the AEGNS manuals, agreements, forms, and other documents furnished by AEGNS only with prior written approval by AEGNS and only in accordance with such terms and conditions as AEGNS may prescribe. All translations, regardless of the participation of a Participant or its employees, agents or consultants in their development, shall be the sole and exclusive property of AEGNS. Participants agree to execute all necessary agreements, and to procure all necessary agreements from other parties, to vest the exclusive, perpetual, and worldwide rights of AEGNS to any such translations. In the event of a conflict between the translation and the English version of any such AEGNS manuals, agreements, forms or other documents, the English version thereof shall govern for all purposes.

1.3 Procedures for Revisions

The *Business and Operational Policies manual* will be published twice each year, in April and October. The *Network Participant Updates (NPU)* will be published on the second Friday of the second full business week of each month, and can include announcements of policy changes as well as new product or service announcements and their associated changes.

The dates for implementation of changes announced by AEGNS will vary by the type of change:

- Policy change (P) - All policy in this manual is effective at the date of publication, unless otherwise stated. In the event that a Participant is unable to implement one (or more) of the policy changes upon publication, the Participant must provide written Documentation of the impact to their operational or systems environment and request an extension of up to three (3) months from the publication date. This extension would not be unreasonably withheld.
- Legally required change of any nature (L) - The implementation dates for these changes are determined in accordance with legal and regulatory requirements.
- Information only (I) - No changes are necessary and the article is provided for information only.

1.3.1 Distribution of Materials

This manual and subsequent *Network Participant Updates (NPU)* will be posted to Knowledge Base (www.amexglobalnetwork.com/knowledgebase).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1.4 Related AEGNS Manuals, Guidelines, and Resources

Reference may be made in this edition of the *Business and Operational Policies manual* to one or more of the following:

- *American Express Foreign Withholding Tax Substantiation Form*
- American Express SafeKey® Documentation:
  - American Express SafeKey Acquirer - Merchant Implementation Guides
  - American Express SafeKey Issuer Implementation Guides
  - American Express SafeKey Protocol Specifications
  - *American Express SafeKey Guidelines*
- *Brand Protection Guide for Acquirers*
- Card Design Guidelines:
  - *Blue Box Line Card Design Guidelines*
  - *Enterprise Line Card Design Guidelines*
  - *GNS Card Design Guidelines*
- *Card-On-File Tokenization Issuer/Acquirer Implementation Guide*
- Chip Card Documentation:
  - *Acquirer Chip Card Implementation Guide*
  - AEIPS Chip Card Specifications
  - *AEIPS Terminal Implementation Guide*
  - *AEIPS Terminal Technical Manual*
  - *American Express Automated Fuel Dispenser Guide (US Region)*
  - *American Express Contactless Terminal Implementation Guide*
  - Expresspay Card Specifications
  - Expresspay EMV Implementation Guide Bulletin
  - *Expresspay Mobile Device Certification Process Guide*
  - *Expresspay Mobile HCE Issuer Implementation Guide*
  - *Expresspay Mobile HCE Product Approval Guide*
  - *Expresspay Mobile HCE Security Requirements Guide*
  - Expresspay Mobile HCE Specifications
  - *Expresspay Mobile Secure Element Certification Process Guide*
  - *Expresspay Mobile Specifications*
  - Expresspay Terminal Specifications
  - *Issuer Chip Card Implementation Guide*
  - *Issuer Expresspay Mobile Implementation Guide*
- *Click to Pay Issuer Implementation Guide*
- *Codes Reference Guide*

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Debit Documentation
  - *American Express U.S. Multi-Network Debit Acceptance Implementation Manual*
- *Digital Wallet API Implementation Guide*
- *Digital Wallet Fraud Baseline Principles*
- *Dual Card Account Marketing Requirements Guide*
- *Enhanced Global Management Information Systems Guidelines*
- *GNS FraudNet User Guide*
- *GNS Social Media Guidelines*
- *Hardware Security Module (HSM) Function Requirements*
- *Industry Spend-Based Incentive Program Guidelines*
- *Issuer Personalization Certification Guide*
- *Live Terminal Parameters AEIPS & Expresspay Guide*
- *Network Cardmember Information Guide*
- *Network Connectivity manual*
- *Network Disputes Manager - User Guide*
- *Network Participant Updates*
- Network Specifications manuals:
  - *Network Specifications - Authorization*
  - *Network Specifications - Financial/Non-Financial*
  - *Network Specifications - Instructions*
- Participant Directory on Knowledge Base
- Product Guidelines:
  - *Centurion Card Product Guidelines*
  - *Platinum Card Product Guidelines*
- *POS Device Certification Process Guide*
- *Promotional Program Capability Implementation Guide*
- QR Code Documentation:
  - *Consumer-Presented QR Code Implementation Guide*
  - *Consumer-Presented QR Code Specification*
  - *Merchant-Presented QR Code Implementation Guide*
  - *Merchant-Presented QR Code Specification*
  - *QR Code Communication Guidelines*

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1.5 Network Participation

1.5.1 Authorized Activities - Overview

AEGNS may, at its sole discretion and subject to the terms and conditions of the applicable Participant Agreement, authorize a Participant to conduct one or more of the following activities:

- Card Issuing
- Merchant Acquiring

Except for fees of general applicability as set out in this and other AEGNS manuals, all fees and other financial terms have been negotiated bilaterally between American Express and the Participant and captured in the relevant Participant Agreement

Note: Participants may also act as ATM Acquirers in accordance with Section 4.6, "ATM Requirements," on page 241 and a separate agreement between the Participant and an American Express Entity.

1.5.2 Merchant Acquiring - General

The Merchant Acquiring Business is the business engaged in by an Acquirer whereby the Acquirer: (i) recruits and acquires S/Es, and contracts with such S/Es, to enable such S/Es to accept Cards as payment for Goods and Services; (ii) transfers and settles Charges and other Transactions transacted by its S/Es, which have been authorized and accepted by an Issuer; (iii) renders statements of account to its S/Es; and (iv) renders related services to S/Es.

An Acquirer may conduct only the acquiring activities that it has been specifically authorized to conduct under its Participant Agreement, and may process and settle Charges only in the specific Authorized Currency set out in its Participant Agreement. American Express reserves all rights and approvals not expressly granted to a Participant. An Acquirer may only operate the Merchant Acquiring Business in the Territory specified in its Participant Agreement.

1.5.2.1 Conduct of Merchant Acquiring Business

Each Acquirer is responsible for all aspects of its Merchant Acquiring Business including, without limitation: marketing, acquisition and retention activities, credit assessment, pricing, risk management, the routing of requests for Authorizations through Clearing Center(s) to the appropriate Issuers, customer service, settlement, statementing, complaint handling, etc., in accordance with the standards set out herein and in other AEGNS manuals and in compliance with all applicable laws. Except as otherwise set out in Section 2.9.3.3.1, "Multinational Accounts (MNAs)," on page 88, each Acquirer has the sole right to set the Merchant Discount, speed of pay, and other fees in respect of Card Acceptance applicable to its S/Es. Issuers have no role in establishing or influencing pricing to S/Es. Each Acquirer has the right to determine the terms of its S/E agreements, subject to the terms hereof and its Participant Agreement. Neither AEGNS nor any Acquirer will disclose any aspects of Card acceptance pricing to any other Participant.

1.5.3 Card Issuing - General

The Card Issuing Business is the business engaged in by an Issuer whereby the Issuer: (i) issues Cards to their customers pursuant to an agreement with their customers; (ii) authorizes their Cardmembers to charge purchases of Goods and Services by means of the Card at S/Es or to access cash at ATMs; (iii) accepts and settles Charges and other Transactions transacted by their Cardmembers, which have been captured and processed by an Acquirer; (iv) renders statements of Account to their Cardmembers; and (v) renders related services to Cardmembers.

An Issuer may issue only the Cards it has been specifically authorized to issue under its Participant Agreement, including the specific type, Authorized Currency, Product Family and Product Functionality associated with such Cards. American Express reserves all rights and approvals not expressly granted to a Participant. An issuer may only operate the Card Issuing Business in the Territory specified in its Participant Agreement.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1.5.3.1 Conduct of Card Issuing Business

Each Issuer is responsible for all aspects of its Card Issuing Business including, without limitation: marketing, acquisition and retention activities, credit assessment, risk management and Transaction decisioning, customer service, pricing, billing, statementing and collections, provision of benefits in relation to Cards issued, etc., in accordance with the standards set out herein and in other AEGNS manuals and in compliance with all applicable laws. Each Issuer has the sole right to set the annual fees, annual percentage rates (APRs) and other fees in respect of its Cards, and to determine the terms of its Cardmember Agreements, subject to the terms hereof and its Participant Agreement.

1.6 Network Services

AEGNS provides the services listed in Table 1-1 to Participants. A description of each service follows the table.

Table 1-1. Services Provided by AEGNS

Access to the Amex Shared ATM Network	Exception File
ATM Transaction Routing	Fraud Prevention Assistance
Authorization Transaction Routing	Management Information System
BIN Blocking Services	Policy and Technical Manuals
Chargeback Routing and Processing	Recurring Billing Cancellation Service
Clearing	Service Establishment Network Acceptance
Currency Conversion	Settlement and Funds Exchange
Debit Card BIN File	Stand-In Authorization

Refer to the "Product Features and Specifications" chapter beginning on page 125 for additional services information.

1.6.1 Access to the Amex Shared ATM Network

Except as otherwise agreed by AMEX or an American Express Entity, Issuers are required to provide their Cardmembers with access to the Amex Shared ATM Network and must prioritize routing their Cardmembers' ATM Transactions through the Amex Shared ATM Network (i.e., Issuers must use the Amex Shared ATM Network as the first choice to route their Cardmembers' ATM Transactions).

1.6.2 ATM Transaction Routing

AEGNS provides ATM Transaction routing services to Issuers. ATM Transaction routing refers to the flow of data necessary between Issuers and ATM Acquirers to allow Cardmembers access to cash. See the "Authorizations" chapter beginning on page 245.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1.6.3 Authorization Transaction Routing

AEGNS provides Authorization Transaction routing services that facilitate the flow of information between Acquirers and Issuers during the Authorization of Transactions. See the "Authorizations" chapter beginning on page 245.

1.6.4 BIN Blocking Services

Blocking of inactive BINs is available through AEGNS to provide Issuers with the means to manage fraud risk on inactive BINs. Following placement of a BIN block, Global Network Services Authorization System (GNSAS) will generate an "Invalid Card" or "Deny" Authorization Response on any Authorization Requests on a Card Account number within the blocked BIN or sub-range. This will provide the Issuer protection from liability for fraudulent Transactions at or above the Network Floor Limit on the blocked BIN. Issuers will remain liable for Transactions under the Network Floor Limit.



Issuers may request blocking of BINs through their Partner Operations Manager.

1.6.5 Chargeback Routing and Processing

The Chargeback process involves handling Transactions disputed by the Cardmember or by the Issuer and sets forth the requirements with which Issuers must comply in order to be reimbursed for a Charge for which the Issuer has financial liability. See the "Chargeback Policies" chapter beginning on page 280 for details.

1.6.6 Clearing

AEGNS shall provide Clearing of Card Transactions to Acquirers and Issuers. Clearing is the non-financial process of routing Transactions submitted by Acquirers to the Issuers whose Card numbers are referenced in the Transaction records. See the "Clearing and Settlement" chapter beginning on page 269.

1.6.7 Currency Conversion

AEGNS provides Currency Conversion services to Issuers. Currency Conversion is the process by which the Transaction currency used by the S/E at the Point of Sale (POS) is converted into the currency of Settlement for the Transaction Authorization and Settlement. See the "Clearing and Settlement" chapter beginning on page 269.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1.6.8 Debit Card BIN File

Debit Card BIN information is available through AEGNS to provide Acquirers with a means to identify Debit Cards. Utilizing the Debit Card BIN file enables Acquirers to accurately apply policy. Acquirers should contact their AEGNS representative to obtain access to the Debit Card BIN file. See Section 3.2.6, "Debit Cards," on page 131.

1.6.8.1 Debit Card BIN File Usage

There may be instances when a Participant wishes to obtain, from AEGNS, a Debit Card BIN file. Requests for a Debit Card BIN file must be sent to AEGNS, and not requested or obtained from other sources.

AEGNS may publish and provide a Debit Card BIN file to support specific Debit Card requirements. Publication of the Debit Card BIN file must only be used for the purposes specified in writing by AEGNS.

Participant shall not use the Debit Card BIN file for any marketing purpose or to suppress acceptance of Debit Cards. BIN ranges are confidential information of AEGNS, and Participants shall treat the Debit Card BIN file data accordingly.

AEGNS may discontinue publication of the Debit Card BIN file, wholly or partially, at any time. Participants' confidentiality obligations shall survive with respect to any accessed Debit Card BIN files.

1.6.9 Exception File

The Exception File stores Card Account numbers that have been reported as lost, stolen, not received, altered Card/counterfeit, confirmed fraud (including On-Us Transactions), or where a Cardmember has withdrawn their consent for Recurring Transactions from certain S/Es. The Card Account numbers may also be misappropriated or cancelled (negative) accounts or Very Important Persons (VIPs). AEGNS will store the information provided by Issuers on such Cards in the Exception File, which will be utilized to support various services offered by AEGNS, including, but not limited to:

- The Stand-In Authorization process
- The Recurring Billing Cancellation Service

Issuers must supply AEGNS with current and accurate information to maintain the Exception File. See Section 5.3.15, "Stand-In Authorization Service," on page 251 and Section 5.8.7, "Exception File," on page 260 for more detailed information. Issuers may submit Exception File updates in real time or through batch input. Mass updates must be submitted through batch processing only. The Network will acknowledge receipt of the batch Exception File transmission.

For Stand-In, the Exception File is sent to the host component of the AEGN Authorization system within twenty-four (24) hours and to the remote component of the AEGN Authorization system within forty-eight (48) hours. Until the information received from the Issuers is uploaded into the Stand-In Tables, AEGNS will not act on that information. Liability for Authorization decisions during Stand-In remains the financial liability of the Issuer.

Issuers participating in the Recurring Billing Cancellation Service must submit the cancellation information using the appropriate file format and data elements. Recurring Billing cancellation information can only be submitted in the batch input process, not in the real-time input process. Refer to the Network Specifications manuals for more detailed information.

Notwithstanding any contrary confidentiality obligation in the Participant Agreement, AEGNS has the right to disclose information contained in the Exception File to Acquirers in order to mitigate the risk of fraud or other harm or otherwise, to the extent appropriate, to operate the Network.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1.6.10 Fraud Prevention Assistance

AEGNS has instituted anti-fraud systems and techniques to lessen the risk of misuse of Cards. General descriptions of fraud prevention systems and techniques can be found in the "Security and Fraud" chapter beginning on page 375.

1.6.11 Management Information System

Management Information System (MIS) refers to the process of gathering, processing, and interpreting data that flows through the AEGN. AEGNS will provide Issuers with MIS reporting appropriate for each Network-provided service. Refer to the Network Specifications manuals for additional information.

1.6.12 Policy and Technical Manuals

AEGNS provides policy and technical manuals designed to inform Acquirers and Issuers of the requirements and standards of the Network. A set of AEGN manuals is provided to each Participant upon executing a Participant Agreement with AEGNS. Policies are established and maintained by AEGNS. Updates are published regularly.

1.6.13 Recurring Billing Cancellation Service

The Recurring Billing Cancellation Service is available through AEGNS to Issuers in AEGNS-designated markets.

The Recurring Billing Cancellation Service uses the information obtained from participating Issuers to block cancelled Recurring Billing Transactions.

1.6.14 Service Establishment Network Acceptance

Cardmembers may make purchases of Goods and Services at S/Es worldwide. Issuers may not contact any S/E concerning American Express, American Express Entities, or any American Express program. American Express and American Express Entities have no responsibility or liability for actions or omissions of S/Es.

1.6.15 Settlement and Funds Exchange

AEGNS provides Settlement and Funds Exchange of Card Transactions to Acquirers and Issuers. Funds Exchange is the financial process of transferring funds between Participants. See the "Clearing and Settlement" chapter beginning on page 269 for details.

1.6.16 Stand-In Authorization

When an Issuer cannot respond to an Authorization Request because of a scheduled or unscheduled outage, the AEGN will provide an Authorization Response to the Acquirer based on the parameters provided by the Issuer. The Issuer is responsible for all Authorizations provided as a result of Stand-In Authorization. Refer to the "Authorizations" chapter beginning on page 245.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

1.7 The Transaction Life Cycle

The Transaction Life Cycle is a key component to the policies of AEGNS. It is referenced throughout this manual.

The Transaction Life Cycle describes all the steps involved in processing Charge or Credit Transactions as viewed from the perspective of the Network. Transactions that require Authorization are first "seen" by the Network when an Authorization Request message is passed from the Acquirer to the Network on its way to the Issuer. The corresponding Authorization Response message is initiated by the Issuer or by the Network itself, if standing in for the Issuer. For Transactions that do not require Authorization (e.g., those with amounts below the Network Floor Limit), the entry point into the Network is upon Presentment by the Acquirer.

Figure 1-1, "Transaction Life Cycle," on page 10 illustrates the Network Transaction processes that may occur for a single Transaction. Horizontal arrows indicate the direction of information flow, from source to destination, including processing performed by the Network as the information flows through it. Time flows from top to bottom of the diagram. Only Transactions that have been disputed by the Issuer or Cardmember will require any Network processing beyond Presentment (see Section 7.3.3, "Disputes Process Transaction Life Cycle," on page 286 for more information for those Transactions that have been disputed by the Issuer or Cardmember).

For each Participant, the terms under which Transactions are settled are set out separately in bilateral agreements between each Participant and AEGNS.

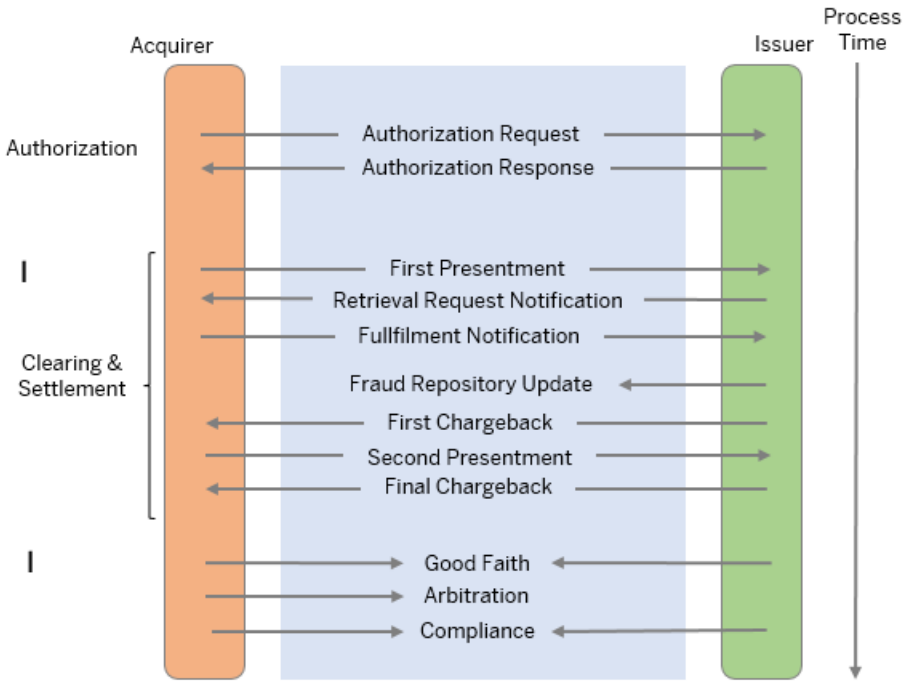


Figure 1-1 Transaction Life Cycle

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2 Business Policies and Rules

2.1 Introduction

This chapter contains general policies of the American Express Global Network (AEGN) applicable to all AEGN Participants and defines certain duties and responsibilities required of Acquirers, Issuers, and third parties.

The chapter describes:

- General Participant requirements including regulatory-related and the use of Authorized Processors
- Requirements concerning privacy policies, alternative dispute resolution, and rights of the AEGN
- Data security requirements that Participants must follow in order to conduct their business on the Network
- Acquirer-specific policies and rules including information on qualifications for S/Es (Service Establishment(s)), S/E agreement requirements, S/E Transaction processing, Internet requirements, and marketing, advertising, and public relations guidelines
- Issuer-specific policies and rules, including the Issuer's responsibilities as a Participant, general policies including Certification of Card issuing programs, marketing, advertising and public relations, and reporting requirements

2.2 General Requirements for AEGN Participants

This section includes general policies and rules that are applicable to all AEGN Participants, as well as specific minimum requirements for Issuers and Acquirers.

2.2.1 Initial Eligibility Requirements for Participants

Following is a list of initial eligibility requirements for prospective Participants:

1. All Participants must execute an agreement with AEGNS that authorizes the Participant to issue Cards under their assigned BIN ranges and/or to acquire S/Es to accept the Card ("Participant Agreement").
2. Participants must have adequate resources, financial and otherwise, to enable them to meet their obligations as Participants.
3. If such Participants are banks, they must meet acceptable ratio pertaining to capital adequacy and, in the discretion of AEGNS, they must be judged financially sound and/or provide satisfactory assurance such as a guarantee of performance and payment substantially in the form set out in "Exhibit 4. Guaranty Agreement" on page 448 from an acceptable guarantor, a letter of credit, or a cash collateral agreement. If Participants are not banks, they must meet similar financial soundness standards judged to be sufficient by AEGNS.
4. The long-term debt rating of a Participant shall be rated by a recognized debt-rating agency, including the Central Rating and Underwriting Team (CRU), at no less than "investment grade" (i.e., in the case of Fitch, Standard and Poor's, and the CRU, no less than "BBB-", and in the case of Moody's, no less than "Baa3").
   AEGNS will use the lowest rating of the above rating agencies. If a Participant is not rated by one (1) of the rating agencies, it will be rated on a similar scale by internal AEGNS rating teams.
   If the Participant's debt ratings ever fall below "investment grade," or their volumes exceed an amount determined by AEGNS, the Participant must obtain a standby letter of credit, cash collateral agreement, or guarantee from an acceptable guarantor above "investment grade."
5. Participants must have all licenses and legal and regulatory permissions necessary to conduct the business they have been licensed by AEGNS to conduct.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6. Participants must at all times operate their business in a safe and sound manner and in compliance with applicable law, and must not directly or indirectly engage in or facilitate any action that is illegal.
7. Participants are required to maintain an effective anti-money laundering and anti-terrorist financing program.
8. Participants must protect Cardholder Data and Sensitive Authentication Data by adhering to the AEGNS Data Security Policy. Refer to Section 2.4, "Participant Data Security Policy," on page 38 for details.
9. Acquirers must demonstrate the ability, either directly or through a certified Authorized Processor, to acquire S/Es consistent with the AML and ATF requirements in Section 2.3.1.1, "AML/ATF Transaction Monitoring," on page 32, pay S/E accounts in the Authorized Currency of the relevant Territory, and service S/Es in such Territory in accordance with applicable law and to standards judged acceptable by AEGNS.
10. Issuers must demonstrate the ability, either directly or through a certified Authorized Processor, to acquire Cardmembers consistent with the AML and ATF requirements in Section 2.3.1.1, "AML/ATF Transaction Monitoring," on page 32, bill Cardmember Card Accounts in the Authorized Currency of the relevant Territory, and service Cardmembers in such Territory in accordance with applicable law and to standards judged acceptable by AEGNS.
11. Continued compliance with the advertising and marketing standards and with all Participant Agreement contractual terms and manual provisions is required. Issuers must properly and accurately disclose to Cardmembers and prospective Cardmembers all legal and financial terms as required by applicable local law and by AEGNS policies, including, for example, the requirements detailed in Section 3.9.1.6, "Cardmember Agreement/Solicitation Materials," on page 207 relating to disclosure of the AEGN assessment of the Foreign Currency Factor and the amount of such assessment.

2.2.2 Ongoing Eligibility Requirements for Participants

Each Participant must continue to meet the eligibility requirements in Section 2.2.1, "Initial Eligibility Requirements for Participants," on page 11, as well as the standards contained in this section and in their Participant Agreement(s), which agreement(s) must remain in effect and valid to maintain their ongoing eligibility. AEGNS reserves the right at all times to determine whether Participants are conducting their business in a prudent and stable manner, including without limitation, the Participant, its agents, and its Authorized Processor(s) maintaining an acceptable level of financial safety and soundness and operational capabilities.

Minimum financial safety and soundness standards may include, but are not limited to, ratios and ratings covering assets, holdings, debt, other liabilities, and credit.

A Participant must notify American Express if the Participant believes that applicable law prevents it from carrying out any of its obligations under its Participant Agreement or AEGNS policy. If requested by AEGNS, the Participant must provide copies of such laws and, if required by American Express, a legal opinion from a reputable law firm validating the Participant's interpretation of the laws.

If AEGNS reasonably establishes that any of the licensed activities of a Participant are contrary to law or regulation and/or may bring the American Express Brand to disrepute, the Participant must discontinue or modify its practices following AEGNS notice.

If a Participant undergoes a Change of Control, the Participant must notify AEGNS as promptly as practicable, but in any event at least sixty (60) days before such Change of Control is consummated, and shall respond to all "due diligence" inquiries of AEGNS relating to such Change of Control. The Participant shall use best efforts to obtain any and all information responsive to such inquiries from any third parties involved in such Change of Control, including any prospective beneficial owners.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.3 Financial Safety and Soundness of Participants

Participants must provide AEGNS each year with copies of its current published annual audited accounts for review in order to assist AEGNS in determining whether the Participants meet AEGNS' minimum financial safety and soundness standards. In the event that any card association or network of which a Participant is a member requires more frequent and/or additional financial information, a Participant shall also provide such additional and/or more frequent financial information to AEGNS. AEGNS may also require a Participant to provide more frequent and/or additional information or to take such curative or other action as AEGNS may reasonably require to assure AEGNS of such Participant's compliance with these requirements.

2.2.3.1 Participant Selection and Monitoring of Settlement Bank

Each Participant is responsible for assessing the financial, operational, and security risk when selecting its settlement banks in line with its own institutional risk appetite and standards. Participants must have the necessary controls in place to monitor the soundness, operational reliability, and security of their settlement banks; controls should include adequate reporting to the Participant's decision-making bodies to enable remedial actions, which should be reported to AEGNS if relevant. AEGNS recommends Participants to work with settlement banks with a long-term debt rating by Standard & Poor's, Moody's, or Fitch. The lowest of any such ratings must be of the following "investment grade" or better: in the case of Fitch and Standard & Poor's, no lower than "BBB-"; in the case of Moody's, no lower than "Baa3".

2.2.4 Participant Books of Account

Each Participant must keep true and accurate books of account and records concerning the conduct of its business in accordance with sound accounting practices, employing standards, procedures, and forms in conformity with generally accepted accounting principles in their Territory.

2.2.5 Security Requirements for Participants

Participants must have adequate security controls in place to protect Cardholder Data, Sensitive Authentication Data, and other sensitive data and equipment that may reside on their premises. In order to ensure that Participants have appropriate controls in place, AEGNS will require Participants to complete the following activities prior to Beta Test and/or the time they begin to conduct business on the Network and periodically thereafter as determined by AEGNS Information Security:

- Adhere to the Participant Data Security Policy (refer to Section 2.4, "Participant Data Security Policy," on page 38 for details).
- Site survey - Shall be completed by AEGNS or its agent for all sites that house AEGN hardware.
- Vulnerability assessment - Participants that host American Express information, including Cardholder Data on Internet accessible websites, must complete vulnerability scanning.
- Physical site review - To be completed as required and recommended by AEGNS Information Security following any of the security requirement activities.
- Third-party audit - Participants may be asked to submit the results of any third-party audit of their internal security controls completed within the most recent 12-month period.

Participants are required to work with AEGNS to remediate any deficiencies that may be uncovered by any of the security requirement activities. Participants failing to complete the security requirements as determined by AEGNS may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.6 Network Infrastructure Access and Certification

AEGNS releases into production new and/or upgraded Network technical functionality on a periodic basis, which is necessary, in AEGNS' judgment, to conduct its business in accordance with the standards and specifications required by AEGNS. AEGNS uses various methods to communicate these standards and specifications, including, but not limited to:

- *Network Participant Updates*
- Network Specifications manuals
- *Codes Reference Guide*
- *Network Connectivity* manual

Participants and Authorized Processors are required to:

- Support all business critical or mandatory functions of the Network,
- Certify for mandatory features as specified in the related technical publications, and
- Support any conditional features where Participant type, product, or market dependencies apply.

2.2.7 Systems Development and Maintenance

Each Participant must, at its expense, develop, install, maintain, and/or update computer systems, functions, and technical requirements which are necessary, in AEGNS' judgment, to conduct its business in accordance with the standards and specifications required by AEGNS. AEGNS will communicate these standards and specifications using various methods, including, but not limited to:

- *Codes Reference Guide*
- *Network Connectivity* manual
- *Network Participant Updates*
- Network Specifications manuals

Each Participant must, at its expense, develop and install (and be responsible for the maintenance of) computer systems and functions which are, in AEGNS' judgment, necessary to conduct its business in accordance with the standards and specifications required by AEGNS.

Each Participant will be required to pay, in a manner and in a currency designated in writing by AEGNS, all initial and ongoing connectivity costs required to connect its systems or its Authorized Processor's systems to the AEGN. Each Participant shall be responsible for any delays in the performance of its obligations resulting from its own failure or its Authorized Processor's failure to comply with the AEGN system requirements.

2.2.7.1 AEGNS Assistance Prior to Launch

AEGNS will provide assistance to Participants prior to the time they begin to conduct business on the Network including:

- Working with a Participant and its Authorized Processor(s) to explain the technical specifications as set forth in the technical specifications manuals and certifying compliance with those specifications,
- Assigning Settlement parameters, currency code and Participant number ranges,
- Ensuring that questions regarding implementation and launch inquiries are processed accurately and in a timely manner by providing access to the necessary systems and AEGNS staff,
- Establishing procedures for submitting or transmitting Clearing and Settlement files and non-financial messages (e.g., fraud file),

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Working with Participants' staff to explain AEGNS quality standards and reporting requirements, the *Business and Operational Policies* manual, Network Disputes Manager, FraudNet, and
- Working with Participants' marketing staff and advertising agency to help ensure compliance with marketing, advertising, and public relations guidelines.

2.2.7.2 Participant Training

All Participants with access to AEGNS systems must ensure their employees, contractors, temporary workers, and vendors complete training prior to gaining access to the following:

- FraudNet
- Network Disputes Manager
- Program Progress Report

Please register through Knowledge Base to request access to Navigator to complete the trainings: www.amexglobalnetwork.com/knowledgebase.

AEGNS offers regular webinar sessions covering use of Knowledge Base and how to access and use helpful documents, such as product and capability guides. Self-paced, online training that is free of charge is available to all Participants.

All Participants must review which learning modules are applicable and encourage active participation. Appropriate and timely training will help ensure compliance with AEGNS policy.

Any Participant found to be non-compliant with any AEGNS policy that has an associated training module and who cannot demonstrate training has been completed may be subject to compliance action, including the assessment of non-compliance fees. Refer to Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.2.8 Data Quality

Data quality refers to the completeness, validity, accuracy, and degree to which data satisfies the requirements in the *Business and Operational Policies* manual, the Network Specifications manuals, and the *Codes Reference Guide*. If AEGNS identifies deficiencies in the quality of data that a Participant is sending to the Network, AEGNS reserves the right to assess non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

An Acquirer must ensure that the Merchant Category Code (MCC) in the POS First Presentment (1240) message matches the MCC used in the POS Authorization Request (1100) message of the same Transaction.

An Acquirer may, in some cases, replace the Merchant Category Code (MCC) received from an S/E or the S/E's processor in the submission and/or Authorization message with data available in such Acquirer's system of record for its S/Es, which may not match the data received directly from the S/E or from the S/E's processor. For information regarding the use of the MCC for incentive programs, please see Section 2.10.8.2, "Incentive Programs," on page 117 and the *Industry Spend-Based Incentive Program Guidelines* located on Knowledge Base.

Additionally, the Network may, in some cases, replace Transaction data values received from an Acquirer in the submission and/or Authorization message when the data quality of the provided value is determined by the Network to be deficient based on other or additional data available to the Network.

AEGNS makes no representation or warranty regarding the completeness, validity, or accuracy of any Transaction data that is passed to Issuers or Acquirers on the AEGN. Participants are responsible for ensuring that their use of the MCC and other Transaction data values is appropriate for any and all purposes for which Participants use such Transaction data, and that any activities that rely on Transaction data include independent internal controls sufficient to meet the needs of the end use of such data elements contemplated by the Participant.

Participants may contact their AEGNS representative with any questions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.9 Program Progress Reports

Participants, at their expense, shall compile and submit Program Progress Reports to AEGNS on a monthly basis to enable AEGNS to fulfill its shareholder and regulatory reporting obligations, as well as to calculate and settle certain commercial terms and fees, and for other purposes AEGNS deems necessary to support the Network and enhance the American Express Brand.

Where appropriate, these reports shall reflect actual figures in the currency in which the GNS Product (as defined on the Program Progress Report) is denominated against the forecasted amounts in the Annual Plan Disclosure.

These reports must be accurate and must be submitted (including approval by the Participant) to AEGNS no later than fifteen (15) calendar days after month-end, regardless of weekends or local holidays. Participants that fail to submit accurate Program Progress Reports within the stated deadline may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

Additional information regarding these reports is included in the *Network Specifications - Instructions* manual on Knowledge Base. Use the Knowledge Base Search function to locate this manual. Contact your AEGNS representative for more information.

2.2.9.1 Annual Attestation of Accuracy

Participants must provide AEGNS with an attestation of accuracy for Program Progress Reports on an annual basis. The attestation submission period for a given Participant will be determined by AEGNS and communicated to the Participant together with instructions for completing the attestation. An attestation must be executed by an individual (such as a Vice President for Finance, or another designee authorized by the Chief Financial Officer or Chief Executive Officer of the Participant and acceptable to AEGNS) with the authority to speak for and bind the Participant to the requirements set forth in this section. If AEGNS deems a Program Progress Report to be inaccurate after receiving the attestation from the Participant, AEGNS may assess a non-compliance fee to the Participant as described in Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.2.10 Marketing, Advertising, and Public Relations

Participants must adhere to the following policies for development, review, and approval of all marketing, advertising, and public relations materials developed for or in connection with their Card Issuing or Merchant Acquiring Businesses.

2.2.10.1 General Advertising Policies

All Participants must adhere to the policies, standards, and guidelines (including, but not limited to, the product naming conventions, product feature requirements, Blue Box logo usage, and Card design requirements) outlined in the *Business and Operational Policies* manual and the Marketing section of Knowledge Base. Use the Search function to locate this information.

2.2.10.1.1 Use of the Registration Mark (®)

On all forms of communication, when referring to products, the registration mark (®) must be placed after the word "American Express," either the first time or in the most prominent position American Express appears, or when American Express is used as an adjective (e.g., "The [Issuer Name] American Express® Card." It is acceptable to use the registration mark in the text and not in the headline if the text immediately follows or is placed next to the headline. In addition, the registration mark (®) must always appear on the lower left side of the Blue Box logo.

Note: The registration mark (®) shall not be placed after the word "American Express" when referring to the corporate name alone (e.g., "...brought to you by American Express").

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.10.1.2 Use of Amex Licensed Marks

Participants may not place any Amex Licensed Mark on any product or service without the prior written approval of AEGNS. For Issuers, American Express Enterprise Line Card communications may not use American Express sign off, tag lines, or slogans without prior written AEGNS approval.

2.2.10.1.3 Use of the Words "Card" and "Cardmember"

The Card is always referred to as "the Card" or "your Card," and always with a capital "C." Persons carrying an American Express® Card may be referred to as "Cardmembers" or the local language equivalents. The use of the term "Cardmember" is encouraged.

2.2.10.1.4 Communication Standards

All American Express-branded communications must be characterized by high standards of quality and good taste. Advertising for American Express-branded products and services may never condone excessive alcohol consumption (e.g., display of drunkenness), smoking, gambling, gratuitous sex, or violence in any direct or indirect way.

American Express-branded products must always be positioned as aspirational and premium products in line with the American Express Brand attributes and brand promise and within the guidelines in the Marketing section on Knowledge Base.

No Person or group may be depicted in any stereotypical fashion that might be construed as reflecting unfavorably upon the member of a certain age, gender, ethnic, religious, sexual orientation, or any other group.

2.2.10.1.5 Accuracy and Truth in Advertising

American Express-branded communications may promise only that which can be delivered. No claim may be made that cannot be fully supported by evidence. Furthermore, claims must relate to normal performance and not to maximum or exaggerated performance of particular products and/or services. Advertising for American Express products and services must never intentionally mislead the customer. A Participant may make benefit-specific superiority or comparative claims as long as these claims are factual and do not violate local laws or regulations.

Additionally, any comparative advertising must be (a) factually accurate, (b) complete, and (c) not misleading, and must not be a comparison only against other American Express-branded Cards or related services, but must include comparison of at least one (1) other general purpose card and/or related services bearing the brand of at least one (1) other major general purpose card network brand in the country in which the comparative advertising is to be published or otherwise disseminated. Advertising done by American Express for the American Express Brand in general (and not for specific card products), may include comparisons of different Card products issued by an American Express Entity and AEGN Issuers as reference data in an Issuer-neutral format.

2.2.10.1.6 Disclosure Requirements - Prohibited Countries

Participants are prohibited from engaging in any American Express-related business with or in the Prohibited Countries. Section 2.3.6, "Prohibited and Restricted Countries and Persons," on page 36 for a complete list.

An Issuer's Card may not be marketed in any way which appears to promote the acquisition of, or use of the Card in, or receipt of AEGN services in or through, a Prohibited Country. Subject to applicable laws, and when relevant and appropriate, such as, for example, when becoming aware that a Cardmember will be traveling to a Prohibited Country, an Issuer must inform Cardmembers that they will not be able to use the Card or receive any American Express-related services in such Prohibited Country. Any American Express-related advertising or marketing communications concerning the sale of products or services relating to or received in a Prohibited Country (which products and services must be non-AEGNS-related) must disclose that the Card is not accepted, nor are any American Express-related services available in such Prohibited Country.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.10.1.7 Material Facts

Material facts (i.e., fees, products benefits and features, etc.) must be included in all communications if they are: 1) important to the customer in evaluating the product service; 2) judged not to be known or otherwise not available to the customer in the normal marketing of the product or service; 3) legally required in the jurisdiction or required by AEGNS policy, such as foreign currency conversion as in Section 3.9.1.6, "Cardmember Agreement/Solicitation Materials," on page 207.

2.2.10.1.8 Use of Exaggerated Claims

Exaggerated claims should be avoided and are not acceptable support for product claims. Claims that may be construed as literally true must be supported by verifiable facts.

2.2.10.2 Advertising and Marketing Review Requirements

American Express-branded advertising and marketing materials must be reviewed and approved by AEGNS prior to their first-time use or prior to re-introduction after an extended period of non-use (typically six (6) months). "American Express-branded" is defined as any advertising or marketing communication, and/or promotional materials that incorporate at least one (1) of the following:

- American Express Enterprise Line Card artwork;
- Blue Box Line Card artwork;
- Prepaid Card artwork;
- Printed references to American Express, its trademarks, sign offs or slogans;
- Narration or audio tracks containing references to American Express or utilizing any of its trademarks, sign offs or slogans;
- Blue Box logo;
- Product naming conventions; and/or
- Any of the visual graphical brand elements described in the Marketing section of Knowledge Base that are associated with the American Express name or trademark.

Participants are also required to submit at least one (1) copy of all final advertising, marketing, or promotional materials to AEGNS.

References to advertising material include communications utilizing mass media channels (i.e., television, print, radio, Internet, and outdoor).

Marketing materials refer to communications utilizing one-on-one sales and promotions or direct marketing channels (i.e., branch acquisition, personal sales, direct mail, welcome packages, promotional brochures, statement inserts, email marketing, and telemarketing scripts).

2.2.10.2.1 Creative Brief and Pre-Production Material Submission

For any advertising material mass media channels (i.e., television, print, radio, Internet, and outdoor), Participants must submit to AEGNS thirty (30) days prior to the campaign launch date for review and approval by AEGNS:

1. A copy of the creative brief or campaign strategy document prepared by the advertising agency and approved by the Participant.
2. Upon approval of the first phase, all pre-production advertising materials (storyboard, TV/radio scripts, mechanical stage copy, and artwork, etc.). Participants shall not notify their advertising agency to begin production of advertising materials until final campaign concepts approvals are obtained from AEGNS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3. Upon approval of the second phase, a final post-production advertising copy for final sign off (recorded TVC, radio voice-overs, Web banners, etc.). AEGNS will, within at least seven (7) Business Days, but no more than ten (10) Business Days of receipt, review, and either:
   - Approve as is - approve the Participant submission with no changes,
   - Approve with changes - request changes that are required by AEGNS prior to launch, or
   - Not approve - resubmission required; indicate to the Participant what revisions must be made to obtain campaign approval.

Participants shall not notify their advertising agency to complete production of advertising materials for release into direct or mass communications channels until final campaign approval is obtained from AEGNS.

All submissions shall include an English language translation of all copy (when materials are in a language other than English).

2.2.10.2.2 Approval of Advertising Campaigns

Advertising campaigns requiring AEGNS review and approval prior to use fall into four (4) categories:

- American Express-branded mass media advertising used for new product launches. This includes marketing materials that the Participant proposes for the initial marketing of each type of product or service.
- American Express-branded mass media advertising and direct channel materials that use creative developed by AEGNS for Participant use (provided in the form of "templates").
- American Express-branded mass media advertising used to generate product demand and Brand awareness, increase product usage, and/or promote special offers including any associated direct channel materials.
- American Express-branded mass media advertising re-introduced two (2) years or more after final AEGNS approval was obtained.

2.2.10.2.3 Additional Policies for Blue Box Line Card and Prepaid Card Issuers

The following policies apply to both Blue Box Line Cards (Network Card License (NCL) Cards) and Prepaid Cards:

- Blue Box Line Cards may not be marketed implicitly or explicitly as being identical to an American Express Enterprise Line Card.
- Blue Box Line communications may never use American Express sign offs or slogans. Prepaid Card communications require written consent from American Express prior to using American Express sign offs or slogans.
- Blue Box Line Issuers may not mimic, ridicule, copy or alter any past or present American Express sign offs or slogans for marketing purposes. Prepaid Card Issuers must obtain written consent from American Express prior to copying any past or present American Express sign offs or slogans for marketing purposes.
- Communications must not disparage American Express or its affiliates.
- Communications must not state:
  - That it has superior acceptance by S/Es, and
  - That Cards issued by American Express or its affiliates or other Participants are not valid or are inferior.
- When incorporating Card visuals in communications, the Issuer Name and the Blue Box must be complete and undistorted in all communications.
- The [Issuer Name] American Express® Card may be shown in full or partially represented, but if only partially represented, the name of the Issuer must be clear and the Blue Box logo and radial lines, if included in the art, must be complete and undistorted.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- American Express-branded advertising and marketing materials that mention the name of an S/E must be reviewed and approved in their final form by AEGNS prior to first-time use as outlined in Section 2.2.10.2.1, "Creative Brief and Pre-Production Material Submission," on page 18.

2.2.10.3 Production Costs and Talent Rights

2.2.10.3.1 Translation Costs

All translation and production costs associated with the development and adaptation of campaign materials created by AEGNS for Participant use must be borne by the Participant. Translation must adequately convey the meaning of the original English language version.

2.2.10.3.2 Talent Rights

All talent rights (also known as "usage rights") associated with the campaign materials created by AEGNS for Participants' use will be communicated to Participants when materials are requested. Usage rights are the costs associated with the payment of the talent (i.e., musicians, actors, models, photography, etc.) that was cast or selected for the advertising. The cost of all usage rights to use campaign materials in the Participant market must be borne by the Participant and paid to AEGNS, as necessary, prior to production.

Under no circumstances shall Participants use American Express-branded advertising materials or re-introduce previously approved materials with expired usage rights without payment for usage rights. Usage rights shall not be considered part of the product license fee paid by the Participant to AEGNS.

2.2.10.4 Changes to AEGNS-Approved Advertising and Marketing Materials

Participants shall not materially alter final advertising and marketing materials or use such materials in a manner not approved by AEGNS. If previously approved materials are altered (creative and/or copy changes) or if the Participant adds new materials to a campaign previously approved by AEGNS, the altered or new materials must be submitted for review and approval prior to their first time use as outlined in Section 2.2.10.2.2, "Approval of Advertising Campaigns," on page 19.

2.2.10.5 Post Review of Advertising and Marketing Materials

AEGNS may, from time to time, conduct a post review of Participant American Express-branded marketing and advertising materials to assure compliance with American Express policy as outlined in this chapter or the Marketing section of Knowledge Base. Use the Search function to find the Marketing section.

Participants must provide samples of marketing and advertising materials in advance of their use to AEGNS if requested for this purpose.

2.2.10.6 AEGNS Internet Marketing Communications Policies and Guidelines

The AEGNS Internet Marketing Communications Policies and Guidelines establish a set of rules for Participants on the AEGN regarding the publishing of American Express-branded communications on the Internet. Participants' American Express-branded content on Participant Web pages that communicate information about American Express products and/or services (Participant site), and all materials that mention such Participant site, must meet certain criteria relating to legal requirements and disclosures, design, content, hyperlinking, security and privacy. The Participant site must be approved by AEGNS prior to publishing (launching) and before hyperlinks may be established to and/or from www.americanexpress.com. AEGNS reserves the right to shut down, or require the Participant to shut down, any non-compliant Participant site within a period of twenty-four (24) hours of AEGNS notifying the Participant that the site is non-compliant. AEGNS will not approve the re-launch of the site until the site has been brought into compliance with American Express Policies. Vulnerability scanning must be completed for all Participant sites that host American Express data.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

To view the entire GNS Internet Marketing Communications Policies and Guidelines for Independent Operator/Joint Venture Card Issuing Participants, refer to "Exhibit 1. AEGNS Internet Marketing Communications Policies and Guidelines (IO/JV)" on page 427.

To view the entire AEGNS Internet Marketing Communications Policies and Guidelines for Network Card Issuing Participants, refer to "Exhibit 2. AEGNS Internet Marketing Communications Policies and Guidelines (NCL)" on page 438.

In addition to the Marketing and Communications guidelines described in this section, Participants must also adhere to the *GNS Social Media Guidelines*. See Section 2.2.13, "Social Media," on page 22 for additional details.

2.2.10.6.1 Paid Search Policies and Guidelines

This section provides guidelines for Participants who want to purchase certain keywords as either paid search or paid placement, which can improve visibility and drive traffic to their websites and help optimize Internet search results for the American Express Brand and/or American Express Cards in their relevant Territories.

Paid search refers to the purchase of certain keywords to improve visibility and drive traffic to particular websites. Paid placement refers to search engine advertising programs that allow sponsors to bid on keywords for preferred placement on search result pages. These paid listings are usually segregated from editorial results and labeled as "Sponsored Results" or "Sponsored Links" or marked with an "Ad" icon. Each paid listing contains a headline, along with a description of and a hyperlink to the sponsor's website.

Participants shall adhere to the following guidelines for purchase and use of American Express trademarks such as "American Express," "AMEX," "AXP," and any derivatives thereof (including local language equivalent) when making paid search or paid placement purchases with Internet search engine providers in order to improve visibility and drive traffic to their American Express-branded Card products.

These guidelines are intended for Participants as they develop their online marketing programs for their American Express-branded Card programs. Any purchase or use of American Express trademarks in such paid search or paid placement related to any such Card programs are is subject to approval by AEGNS and may require execution of an additional license agreement with American Express. Accordingly, Participants must submit lists of keywords, headlines, and descriptions to be used in Card programs to AEGNS for approval prior to the purchase or use of American Express trademarks in any such keywords, headlines, and descriptions for Card programs. AEGNS has the sole discretion in approving or rejecting such lists.

Keywords of general terms, such as "Credit Card" or "Charge Card," can be purchased by Participants, without approval by American Express. Participants do not need American Express approval for paid search or paid placement that is not related to Card programs, and Participants should make their own independent decisions regarding keyword bidding outside of the Card programs.

AEGNS reserves the right to request Participants to remove keyword search terms from Internet search engines that are deemed unapproved within a period of twenty-four (24) hours of AEGNS notifying the Participant that the keyword search term is unapproved.

2.2.10.7 Failure to Comply With AEGNS Advertising and Marketing Policies

If AEGNS notifies a Participant of any failure to comply with AEGNS policies concerning advertising or marketing, the Participant must immediately cease any such use and must correct any failure to comply within ten (10) days of notification by AEGNS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.10.8 Compliance to Local Regulatory Requirements

Participants, not AEGNS or any American Express Entity, shall be responsible for ensuring that their advertising and marketing materials, letters, emails, and any other communications, as well as any marketing and advertising placed in mass media, comply with applicable legal and regulatory requirements of the jurisdiction(s) where materials are to be used in communications. Participants also bear a responsibility to ensure that appropriate Participant and service marks, as required by AEGNS on marketing and advertising communications, are accurately and correctly included in communications, regardless of channel.

2.2.10.9 Participant Eligible Marketing Region

Participants generally may not advertise, promote, or market products or services or engage in the Card Issuing Business or Merchant Acquiring Business in any geographic territory other than the Territory specified in the Participant Agreement. This restriction shall not be construed to prohibit Participants in the European Union/European Economic Area and United Kingdom from concluding passive sales within the EU/EEA & UK (regarding which, for purposes of definition only, reference should be made to the guidelines to EC Regulation 330/2010).

2.2.10.10 Right to Request Removal of Unapproved Communications

AEGNS reserves the right to require removal of marketing and communications deemed inappropriate for the brand, are out of compliance, do not meet AEGNS marketing and brand standards or marketing guidelines, or that have been placed in the market without prior approval from AEGNS. Issuers shall have materials removed from market within twenty-four (24) hours of AEGNS notifying the Participant. AEGNS will not approve the re-launch of the materials until the materials have been brought into compliance with American Express Policies.

2.2.11 Press Releases/Publicity

Any disclosure to the media in the form of a press release concerning a Participant's participation in the Card business, or the execution or existence and the timing and content of such disclosure, must be mutually agreed in advance by AEGNS and the Participant. All Participants shall consult with AEGNS before making any disclosure to the media concerning AEGNS, the Network, or the American Express Brand.

As long as a Participant operates on the AEGN, it will not be necessary for American Express to obtain permission to disclose the fact of that Participant's participation on the AEGN in documents describing the AEGN.

2.2.12 Participants' Key Contacts

Participants shall submit information regarding key contact personnel for their AEGNS business as requested by AEGNS. Participants must promptly update AEGNS when contact information changes. Such information shall be retained by AEGNS and may be shared with other Participants via the Participant Directory on Knowledge Base. Use the Search function to find that information.

2.2.13 Social Media

Social media, encompassing a wide range of personal and professional communication channels, allows for an interactive dialogue between businesses and customers while providing an opportunity for them to collaborate, network, and share information. Some prominent examples of social media are: Facebook, Instagram, LinkedIn, YouTube, and Twitter.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Recognizing the impact of the rapidly evolving social media channels, AEGNS has developed the *GNS Social Media Guidelines* to maximize the benefits for and minimize the risk to AEGNS and Participants. The *GNS Social Media Guidelines* provide an overview of the policies that must be adhered to when Participants engage in American Express-branded social media initiatives. The guidelines are intended to protect the American Express Brand, confidential information, and the reputation of American Express and Participants.

Participants are permitted to initiate and manage social media initiatives that utilize the American Express Brand, provided:

- They execute a Social Media Licensing Amendment to the Trademark Licensing Agreement with American Express.
- They follow the approval process detailed in the *GNS Social Media Guidelines*.

The *GNS Social Media Guidelines* can be found in the Marketing section on Knowledge Base. Use the Search function to find this document.

2.2.14 Privacy Policies

Participants are obligated to comply with applicable laws and regulations concerning privacy and/or data protection. Participants are also encouraged to use the American Express Privacy Principles set out in this section as a framework within which to develop their own privacy guidelines. Laws and regulations relating to privacy and data protection can differ from country to country, and Participants are responsible for being aware of and adhering to privacy and data protection laws in all countries in which they conduct their licensed activities, including, without limitation, specific and adequate disclosures to Cardmembers (customers) of collection, use, and processing of personal data. The American Express Privacy Principles include:

- Collect only customer information that is needed to administer customer Accounts, provide customer services, offer new products and services, and fulfill any legal and regulatory requirements. Inform customers about the general uses of information collected about them, and be willing to provide additional explanation if the customer requests it.
- Give customer choices about how their data will be used. Upon becoming a Cardmember and, thereafter on a regular basis, give customers the option to decide whether or not they wish to have their names removed from lists used for mail, telephone, and online marketing.
- Ensure information quality. Ensure that customer data is processed promptly, accurately, and completely. Require high standards of quality from consumer reporting agencies and others who provide information about prospective customers.
- Use information security safeguards. Limit access to customer data to those who specifically need it to conduct their business responsibilities and use security techniques designed to protect customer data.
- Limit the release of customer information. In addition to providing customers with the opportunity to "opt-out" of marketing offers, release information only with the customer's consent or request, or when required to do so by law or other regulatory authority. When a court order or subpoena requires release of customer information, notify the customer promptly to give the customer an opportunity to exercise his or her legal rights. The only exceptions are when a Participant is prohibited by a court order or law from notifying the customer, or cases in which fraud and/or criminal activity is suspected.
- Be responsive to customers' requests for explanations. If a Participant denies an application for services or ends a customer's relationship, to the extent permitted by applicable law, provide an explanation and state the reason for the action taken and the information upon which the decision was based, unless the issue involves potential criminal activity.
- Extend these customer privacy principles to business relationships. Require that companies selected as business partners and third-party vendor(s) abide by these privacy principles in the handling of customer Information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Hold employees responsible for complying with these privacy principles. Conduct training and communication programs to educate employees about the meaning and requirements of these customer privacy principles, and audit compliance.

2.2.15 Transaction Data Use

Subject to applicable law, American Express Entities and Participants have the right to use Transaction data that they receive or process in their role on the Network, including, without limitation, for the purposes deemed reasonably necessary by them to support or promote the Network, help reduce fraud on the Network and/or enhance the American Express Brand, Network-wide offer fulfillment, statistical analysis of offer and advertising effectiveness, and other market research.

2.2.16 Alternative Dispute Resolution

Except as otherwise provided herein or in the applicable Participant Agreement, Trademark License Agreement, or other agreement, this section applies to all disputes between a Participant and AMEX or any American Express Entity. This section does not apply to disputes for which a specific AEGN process has been developed (e.g., disputes relating to Chargebacks which are covered in the "Chargeback Policies" chapter beginning on page 280, which provides the sole remedy for Issuers and Acquirers with respect to Chargebacks). For such disputes, the specific AEGN process shall be followed.

Except as otherwise provided in the applicable Participant Agreement, disputes between a Participant and AMEX or any American Express Entity should generally be settled in the ordinary course of business. Therefore, neither a Participant nor AMEX or any American Express Entity shall have the right to resort to litigation or any other procedure prior to exhausting the arbitration procedures set forth in this section.

1. If any dispute shall arise between a Participant and AMEX or an American Express Entity, the Participant and AMEX or such American Express Entity shall, except as provided in the applicable Participant Agreement, attempt to resolve such dispute promptly by negotiation between executives who have authority to settle the controversy and who are at a higher level of management than the Persons with direct responsibility for administration of the relationship, unless said Persons have the authority to settle the controversy. Either a Participant, AMEX or the applicable American Express Entity may give the other party written notice, in accordance with the Participant Agreement, of any dispute not resolved in the normal course of business. Within fifteen (15) days after delivery of the notice, the receiving party shall submit to the other a written response.

   The notice and the response shall include, respectively:

   a. A statement of the party's position and a summary of arguments supporting that position, and

   b. The name and title of the executive who will represent that party and of any other Person who will accompany the executive.

   Within thirty (30) days after delivery of the disputing party's notice, the executives of both parties shall meet at a mutually acceptable time and place, and thereafter as often as they reasonably deem necessary, to attempt to resolve the dispute. All reasonable requests for information made by one (1) party to the other will be honored. The foregoing time deadlines may be extended by mutual written agreement. If the parties mutually agree that it would aid resolution of the dispute, each party may have its attorney attend such meetings.

   All negotiations pursuant to this section shall be confidential and shall be treated as compromise and settlement negotiations for purposes of applicable rules of evidence.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2. If the dispute has not been resolved by negotiation between the executives referred to in subsection 1 above, and if the parties have not agreed to extend the applicable time deadlines, within ninety (90) days of the disputing party's notice, the parties shall endeavor to settle the dispute by mediation under the rules and procedures of the dispute resolution forum specified in the Participant Agreement. Each party shall bear its own costs of such mediation. The parties agree that the mediator, not the parties, shall decide when the parties are unable to reach agreement on the resolution of this dispute, and that mediation shall continue until the mediator so decides. The parties shall refrain from demanding arbitration for a period of sixty (60) days from the date of the mediator's decision that the parties have failed to reach agreement. Any applicable statute of limitations with respect to a dispute subject to this section shall be tolled for the period beginning from the date of delivery of the original notice regarding the dispute referred to in subsection 1 above, through the period ending five (5) days after the end of the sixty (60) day "cooling off" period referred to in this section.

   Notwithstanding the foregoing, the negotiation and mediation procedures set out in this Section 2.2.16 shall not apply to disputes involving issues of law (but not of fact) only, such as where one (1) of the parties challenges the existence and/or validity of the Participant Agreement or any part thereof, in which case either party may initiate arbitration pursuant to subsection 3 below without first observing the provisions of subsections 1 and 2 above.

3. After the expiration of the sixty (60) day period, a party may elect to initiate binding arbitration to be administered by the arbitration association and in a place specified in the Participant Agreement. Each party shall bear its own costs of arbitration.

   Arbitration shall be governed by and construed in accordance with the laws governing the Participant Agreement. Unless otherwise agreed, the arbitration tribunal shall consist of three (3) arbitrators, and the language of the arbitration shall be English. With respect to the arbitration of any dispute:

   a. Neither a Participant nor AMEX will have the right to participate in a representative capacity or as a member of any class of claimants pertaining to any claim.

   b. Disputes shall be arbitrated on an individual basis. There shall be no right or authority for any disputes to be arbitrated on a class action basis or in a purported representative capacity on behalf of the general public or other Persons or entities similarly situated.

   c. The arbitrator's authority to resolve disputes and to make awards is limited to disputes between the parties to the Participant Agreement alone, and is subject to the Limitations of Liability set forth in such Participant Agreement.

   d. Disputes brought by one (1) party to a Participant Agreement against the other may not be joined or consolidated in arbitration with disputes brought by or against any third party, unless agreed to in writing by all parties.

   e. The arbitrators shall have the power to grant any remedy or relief that they deem just and equitable, including without limitation, injunctive relief, whether provisional and/or final, and any such remedy or relief ordered by the arbitrators may be specifically enforced by any court of competent jurisdiction.

   f. No arbitration award or decision on any disputes shall be given preclusive effect as to issues or claims in any dispute with anyone who is not a party to the arbitration.

   g. Judgment upon the award rendered by the arbitrator(s) may be entered by any court having jurisdiction thereof.

   Should any portion of subsection (a) through (g) above be deemed invalid or unenforceable, then the provisions of this Alternative Dispute Resolution section (other than this sentence) shall not apply.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4. The parties and the mediators and arbitrators utilized shall maintain the confidentiality of the proceedings, except to the extent otherwise required under applicable law. It shall be a condition to the engagement of any mediator and/or arbitrator that such mediator and/or arbitrator shall agree to maintain the confidentiality of the proceeding and the decision and any award.
5. The mediators/arbitrators and the parties may by agreement hold hearings in any location convenient to the mediators/arbitrators and the parties, including by teleconference and video conference.
6. Notwithstanding anything herein to the contrary, with respect to disputes between a Participant and AMEX or any American Express Entity arising out of or relating to the use of Amex Licensed Marks, each party shall have the right to seek provisional measures from a judicial authority, and any such request shall not be deemed incompatible with or a waiver of rights under this Section 2.2.16 or the applicable Participant Agreement. Each party hereby (a) submits to the non-exclusive jurisdiction of the courts of New York, both federal and state, with respect to any application for provisional measures, (b) waives any objection which it may have at any time to the laying of venue of any such proceedings brought in such courts, (c) waives any claim that such proceedings have been brought in an inconvenient forum, and (d) further waives the right to object with respect to such proceedings that any such court does not have jurisdiction over such party.

2.2.17 Audit Rights

AEGNS reserves the right to conduct procedural and financial audits of all Participants and their agents. Participants must fully cooperate with the inspection process including providing statistical information, test Cards, contracts, and any other information requested by AEGNS concerning the Participant's financial, AML/ATF compliance, or operational environment.

AEGNS shall have the right at any time at its expense and upon giving a Participant thirty (30) days advance written notice, to audit the books and records of such Participant or their Authorized Processor(s) to determine whether the required standards of financial soundness, AML/ATF compliance, and operational capability are being met, using AEGNS' own auditing personnel or a firm of independent public accountants selected by AEGNS.

Additionally, AEGNS reserves the right to conduct a complete audit and Vulnerability Threat Analysis (VTA) of any GLOBE infrastructure or functional equivalent to ensure compliance with applicable American Express policies and standards. Technology infrastructure which lies between the GLOBE or its equivalent and facilitates connection to the AEGN will also be subject to audit. The audits and VTAs will include Network security assessments.

AEGNS shall require that the auditors maintain the confidentiality of any confidential information of the Participant in question. Participants must cooperate fully with any such audit.

A report of any audit conducted pursuant to this section shall be deemed to be confidential information of the Participant, and will be shown only to the AEGNS employee(s) who are responsible for supporting the Network operations on a "need to know" basis. If such audits indicate that a Participant's operations are deficient with respect to the required standards, AEGNS shall have the right to demand that the Participant remedy such deficiencies to AEGNS' satisfaction by the dates specified by AEGNS.

AEGNS may investigate an S/E outlet at any time when suspicious activity has been identified. A Participant is obligated to correct any deficiencies identified in the AEGNS audit. AEGNS reserves the right to levy fines to Participants in accordance with the *Business and Operational Policies* manual for violations identified during the aforementioned audits.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.17.1 Network Assessment Program

On an annual basis, AEGNS will contract external Service Providers, at its own expense, to assess and report on the effectiveness of its internal control environment and key systems that are used by and in support of Participants.

A series of reports will be available to Participants, which will be known as the Network Assessment Library. The reporting standards and external Service Providers to be used, as well as the timing, scope, and fees associated with such reports are exclusively at the discretion of AEGNS and subject to change. Participants may request a copy of any or all of these reports as they are made available. The Network Assessment Library comprises the following reports:

- Service Organization Controls 1 (SOC 1) is a report on controls at a service organization that are relevant to user entities' internal control over financial reporting. The scope of SOC 1 includes the following:
  - Network Transaction Processing (including Participant Setup, Authorization, and Clearing and Settlement process)
- Service Organization Controls 2 (SOC 2) is a report on a business' non-financial reporting controls as they relate to security and availability. The scope of SOC 2 includes the following:
  - Information technology general controls
  - Authorizations
  - Clearing and Settlement
  - Network Disputes Manager
  - Partner Setup Utility
  - FraudNet
  - Knowledge Base
  - GNS Reporting Center
  - Global Pricing Platform
  - User Certification Tool on Knowledge Base
- Ethical Hacking, performed by skilled computer experts, is the use of programming skills to determine vulnerabilities in computer systems. The ethical hacker evaluates security weaknesses and suggests changes to systems to make them less likely to be penetrated by malicious hackers. Web service applications in scope for Ethical Hacking include the following Knowledge Base applications:
  - User Certification
  - File Tracker
  - FraudNet
  - Network Disputes Manager
  - Program Progress Reports
  - Reporting Center

Table 10-25, "Report Availability and Fees," on page 414 describes the availability of reports and costs associated with the Network Assessment Program.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Participants may request additional Ethical Hacking reports related to applications other than those Knowledge Base applications described above. These requests must meet the following criteria:

- Requests must be submitted to AEGNS by November to obtain an additional Ethical Hacking report the following year.
- Participants must pay the associated operational support fees detailed in Table 10-26, "Operational Support Fee Schedule," on page 414.

As an alternative to these reports, Participants may request an assessment. These requests must meet the following criteria and are subject to AEGNS approval:



- Participants must provide a minimum of six (6) months' written notice to AEGNS defining the scope, timing, objective, method to be used, and level of support required from AEGNS.
- Participants must pay the associated operational support fees detailed in Table 10-26, "Operational Support Fee Schedule," on page 414.

2.2.18 Taxes on Fees and Assessments

The fees payable by Participants are exclusive of Value-Added Tax (VAT), withholding tax, and any other applicable taxes assessed by the relevant taxation authorities. Any VAT or other taxes (other than withholding taxes discussed below) assessed on the fees and assessments payable by a Participant under the Participant Agreement shall be exclusively borne and paid by such Participant. If necessary, Participant shall gross up the amounts of all fees due to AEGNS to ensure that AEGNS actually receives the correct amount net of any taxes of any kind (other than the withholding income tax).

If any of the fees or assessments payable by a Participant under the Participant Agreement is subject to withholding taxes in any jurisdiction in its Territory, no gross up obligation shall apply and the Participant shall withhold and pay within the time provided by law the required amounts to the appropriate tax authorities in such jurisdiction and shall furnish to AEGNS the official receipts of the tax authorities for the taxes involved. Receipts must be furnished to AEGNS within ninety (90) days of the Tax Withheld Date unless local market procedures dictate otherwise in which case the receipts must be furnished to AEGNS as soon as they are available from appropriate tax authorities in the country. If a Participant fails to make timely submission of the official receipts as required by the previous sentence, it may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411. The American Express Entity that is party to the Participant Agreement shall reserve the right, through AEGNS, to offset or collect the amount that was withheld against any amounts due to a Participant under the Participant Agreement.

Receipts provided to AEGNS for foreign tax withholding must be accompanied by an *American Express Foreign Withholding Tax Substantiation Form* to help AEGNS interpret the information provided on the tax receipt (which can often be expressed in local currency, local language, etc.). The *American Express Foreign Withholding Tax Substantiation Form* is located on Knowledge Base and contains instructions Participants must follow to complete the form and submit it with the accompanying tax receipts. Use the Knowledge Base Search function to find this form.

In the event U.S. or applicable local laws or regulations are altered or amended so as to disallow the U.S. foreign tax credit for withholding income taxes, AEGNS shall give written notification to affected Participants, and such Participants shall thereafter gross up the amounts of fees payable to AEGNS so as to ensure that AEGNS actually receives said fees net of such withholding taxes.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.19 Global Disputes Monitoring Program

The goal of the Global Disputes Monitoring Program (GDMP) is to ensure that Participants monitor their dispute rates and do not exceed acceptable levels of disputes. Refer to Table 2-1, "Regional Retrieval Request Threshold," on page 29 and Table 2-2, "Regional First Chargeback Threshold," on page 29 for additional information.

If a Participant exceeds these thresholds, then that Participant must take appropriate steps to reduce their dispute rates. Participants that fail to reduce their dispute rates may be subject to non-compliance fees. Refer to Section 10.7.1, "General Non-Compliance Fees," on page 411 for additional information.

2.2.19.1 Retrieval Request Threshold Standard

A Participant's monthly Retrieval Request threshold must not exceed the regional Retrieval Request threshold listed in the following table:

Table 2-1. Regional Retrieval Request Threshold

Region	Retrieval Request Threshold[1]
United States/United States Territories/Canada	0.20%
Europe/Middle East/Africa	0.60%
Asia Pacific	0.60%
Latin America/Caribbean	0.75%

1. A Participant's Retrieval Request rate is calculated by dividing the number of Retrieval Requests by the number of First Presentments for a specific month. For example, calculating the Retrieval Request rate for October 2010 would be determined by dividing the number of Retrieval Requests in October 2010 by the number of First Presentments from October 2010.

Participants that exceed regional Retrieval Request thresholds may be subject to Compliance action, including the assessment of non-compliance fees. Refer to Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.2.19.2 First Chargeback Threshold Standard

A Participant's monthly First Chargeback threshold must not exceed the regional First Chargeback threshold listed in the following table:

Table 2-2. Regional First Chargeback Threshold

Region	First Chargeback Threshold[1]
United States/United States Territories/Canada	0.20%
Europe/Middle East/Africa	0.60%
Asia Pacific	0.60%
Latin America/Caribbean	0.75%

1. A Participant's First Chargeback rate is calculated by dividing the number of First Chargebacks by the number of First Presentments for a specific month. For example, calculating the First Chargeback rate for October 2010 would be determined by dividing the number of First Chargebacks in October 2010 by the number of First Presentments from October 2010.

Participants that exceed regional First Chargeback thresholds may be subject to Compliance action, including the assessment of non-compliance fees. Refer to Section 10.7.1, "General Non-Compliance Fees," on page 411.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.2.19.3 Participant GDMP Status

A Participant's dispute rates compared to their regional threshold will determine their GDMP status, as shown in the following table:

Table 2-3. Participant GDMP Status

Participant Dispute Rate Against Regional Thresholds	Participant GDMP Status
A Participant's dispute rates are below a regional threshold	Passive Monitoring
A Participant's dispute rates have exceeded a regional threshold	Active Monitoring
A Participant's dispute rates have exceeded a regional threshold for three (3) consecutive months[1]	Active Monitoring and Compliance

1. AEGNS, at its discretion, may assign a Participant to "Active Monitoring and Compliance" status if their dispute rate could cause damage to the American Express Brand or financial harm to other Participants.

The following descriptions apply for purposes of the GDMP:

- Passive Monitoring - AEGNS will provide reporting to Participants.
- Active Monitoring - AEGNS will notify a Participant that their dispute rates are in excess of regional thresholds and advise them that action is needed to reduce dispute rates below regional thresholds.
- Active Monitoring and Compliance - A Participant may be required to submit a dispute reduction plan and take appropriate action to reduce their dispute rates. Participants that fail to do so may be subject to non-compliance fees. Refer to Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.2.20 Crisis Preparedness and Service Continuity Program

Participants must maintain an effective crisis preparedness and service continuity program to minimize the potential negative impacts of disruptions to business processes or technology. At a minimum, such program must provide for plans and strategies to ensure business continuity, disaster recovery, and technology solution governance in respect of their authorized activity. If relevant, Participants should ensure that their Authorized Processors maintain similar crisis preparedness and service continuity programs in respect of activities outsourced to them. If required by AEGNS, Participants must provide evidence of the existence and effectiveness of the programs referred to in this paragraph.

2.3 Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements

Money laundering has generally been defined as the process by which the proceeds of criminal activity are moved through the financial system in order to hide all traces of their criminal or illegal origin. The transactions need not, and frequently do not, involve cash and the movement of funds can involve any variety of financial instruments, products, or services.

Terrorist financing involves the movement of funds (legitimately or illicitly derived) undetected through the financial system so that terrorists can use these funds to support their activities. Dollar values related to terrorist financing tend to be significantly smaller than those associated with the proceeds of money laundering related to crime and therefore can be much more difficult to identify when moved through the financial system.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The U.S. government, and other governments around the world, maintain trade and economic sanctions against individuals, entities, and countries for participating in or providing support to various criminal, terrorist, or human rights-violative activities. As a U.S. company, American Express must comply with all sanctions administered and enforced by the U.S. government through the Treasury Department's Office of Foreign Assets Control (OFAC), and also must comply with applicable local sanctions regimes in the foreign jurisdictions in which it operates.

Participants are required to maintain an effective anti-money laundering, anti-terrorist financing, and sanctions compliance program to prevent the use of Participant operations for criminal purposes and to satisfy AEGNS that the Participant's business is not being conducted in circumstances that would in any way facilitate money laundering or the financing of terrorist activities or pose a sanctions, money laundering, terrorist financing, or other regulatory risk to AEGNS. Elements of this program should include:

- Internal policies, procedures, and controls (including an automated screening tool) related to anti-money laundering, sanctions compliance, and anti-terrorist financing;
- Dedicated personnel responsible for the compliance function;
- A regular employee training program on the identification and prevention of money laundering, sanctions, and terrorist financing;
- Record-keeping;
- Periodic audits (internal and/or external); and
- Background checks on the owners, members of the management board, direct or indirect shareholders, holding companies, directors, officers, and employees of Participant.

In order to support AEGNS' obligations under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001, Participants are required to cooperate with AEGNS to understand and document Participants' AML/ATF program, prior to becoming a Participant on the AEGN and on an ongoing basis thereafter as determined by AEGNS.

The ongoing monitoring of Participants' AML/ATF/sanctions compliance programs may include, but is not limited to, an initial risk assessment and due diligence process to be satisfactorily completed prior to Participant joining AEGNS, risk assessment update at least annually, update of Compliance due diligence periodically based on the risk assessment, onsite inspection and testing, reporting of metrics relevant to Participant's AML/ATF programs, and other requests for information about Participant's AML/ATF program as may be required by AEGNS or by law. AEGNS will determine and communicate specific requirements to the Participant at the time it is requested.

2.3.1 General Requirements

At a minimum, an effective anti-money laundering, sanctions, and anti-terrorist financing program should incorporate the following policies and procedures:

- Know Your Customer (KYC) provisions requiring reasonable measures to establish the identity of existing and potential customers (Cardmembers and S/Es, as applicable). KYC programs must be sufficient at all Points of Sale to determine and document the customers' identity and source of funds, including collecting full legal name, DBA name, and address information, in addition to other data points as available and applicable (e.g., date of birth, national ID, and beneficial owner);
- A sufficient monitoring program of Cardmember and/or S/E Account activities consistent with the Cardmember's and/or S/E's business and risk profile. This profile should include, at a minimum, the monitoring required by Section 2.3.1.1, "AML/ATF Transaction Monitoring," on page 32, sanctions screening by an automated tool of all collected demographic information, and incorporate a review of the results for money laundering, sanctions prohibited, and/or terrorist financing activity;
- Regular management reporting on money laundering, sanctions, and terrorist financing issues;

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- A requirement to report to the Participant's management any reasonable suspicion of money laundering, ongoing activity that is prohibited under a sanctions program, or terrorist financing;
- Periodic training for relevant employees on the program and its requirements;
- A requirement to report to AEGNS material activity that is prohibited under U.S. or local sanctions programs;
- A requirement to report to the authorities any reasonable suspicion of money laundering, sanctions prohibited activities, or terrorist financing, consistent with the Participant's local legal requirements;
- Compliance with applicable AML/ATF/sanctions laws and regulations; and
- Sufficient record keeping to demonstrate compliance with each of the above requirements.

2.3.1.1 AML/ATF Transaction Monitoring

Participants must maintain policies, procedures, and processes that ensure effective transaction monitoring, research, and reporting of suspicious activity. Suspicious cases must be handled in accordance with applicable local requirements. AEGNS requires Participants to perform AML/ATF transaction monitoring, including, at a minimum, the following:

Issuers

In addition to the Cardmember Transaction monitoring required in Section 8.10.3, "Cardmember Risk Management," on page 392, Issuers must monitor Cardmember accounts for:

- The existence and reimbursement of credit balances
- Cash payments of outstanding balances
- Unusual patterns of cash (e.g., load, reload, ATM) Transactions

Acquirers

In addition to the S/E Monitoring required in Section 8.9.3, "S/E Risk Management," on page 388, Acquirers must monitor S/E accounts for unusual patterns of POS refund transactions.

2.3.2 Customer Screening Program

AEGNS requires that Participants have a process in place to screen their potential and existing customers (Cardmembers and/or S/Es, including purchasers of reloadable Prepaid Cards) for entities and individuals identified by OFAC and any equivalent foreign authority as subject to sanctions or associated with terrorism, money laundering, or drug-related activities. Specifically, AEGNS requires that Participants:

- Screen potential and existing customers against the most current lists maintained by OFAC of Specially Designated Nationals (which includes Specially Designated Global Terrorists and Specially Designated Narcotics Traffickers) and additional Consolidated Sanctions lists[1], in addition to similar lists maintained by the appropriate government authority in the jurisdiction in which the Participant operates including, but not limited to, United Nations and European Union lists; and
- To determine whether potential and existing customers operate in a foreign jurisdiction subject to comprehensive, country-wide sanctions.

1. At the time of publication, the Consolidated Sanctions List includes: the Sectoral Sanctions Identifications (SSI) List; Non-SDN Palestinian Legislative Council (NS-PLC) List; the list of Foreign Financial Institutions Subject to Part 561 (the Part 561 List); list of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 (the 13599 List); the Non-SDN Iranian Sanctions Act (NS-ISA) List; and the Foreign Sanctions Evaders (FSE) List.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Please see the following OFAC websites for the relevant OFAC lists:

- https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx
- https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx

In summary, AEGNS requires that Participants not do business with customers with whom American Express, as a U.S. company, may not do business under OFAC sanctions programs and to maintain a sufficiently robust screening and interdiction program to ensure that they are able to comply with this restriction.

Screening of applicants/potential customers must occur prior to accepting the relationship. Additionally, periodic screening must be performed against required watchlists whenever the lists are updated, and not less than once a month. AEGNS requires that Participants automate their screening activities.

In the event of a potential match against the OFAC or other list, Participants must take necessary steps to determine if such match is a confirmed match. Unless prohibited under Participant's local law, Participants must terminate the subject relationship with the Cardmember or S/E upon confirmation of the match.

If Participants are unable to terminate the subject relationship, they must contact their AEGNS representative to determine the best course of action. AEGNS is available to assist Participants with assessing best practices in the area of sanctions screening.

2.3.2.1 Certifications and Ongoing Due Diligence

Participants are required to cooperate with AEGNS to understand, document, report, and certify that Participant's customer screening program complies with the requirements set forth in this section. In determining whether a Participant is in compliance with this section, AEGNS may consider the following factors, among others:

- Compliance due diligence Documentation
- Onsite inspection and testing
- Reporting of metrics relevant to Participant's customer OFAC screening program
- Responses to requests for information about Participant's customer OFAC screening program

AEGNS will also require Participants to:

- Periodically provide responses to ongoing due diligence questionnaires, and
- Submit Certifications on a schedule and in a form to be determined by AEGNS to ensure that the Participant remains in compliance with the requirements set forth in this section.

AEGNS reserves the right in any case and at its discretion to require additional due diligence, which may include conducting an onsite audit of the Participant in accordance with Section 2.2.17, "Audit Rights," on page 26.

2.3.2.2 Non-Compliance

Participants that are not in compliance with Section 2.3.2, "Customer Screening Program," on page 32 will be subject to the requirements provided in Section 2.3.5, "Non-Compliance," on page 35.

2.3.3 Additional Anti-Money Laundering (AML) Requirements for Cash Disbursements

The unique nature of Cash Disbursements makes these types of Transactions particularly vulnerable to money laundering. The requirements listed in Section 2.3.3.1, "Activation for Cash Disbursement Transactions," on page 34 and Section 2.3.3.2, "Other Cash Disbursement Requirements," on page 34 are intended to ensure Participants offering Cash Disbursements have processes and procedures in place to mitigate the risk associated with this service.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.3.3.1 Activation for Cash Disbursement Transactions

In order to be certified or activated for Cash Disbursement Transactions, Participants must:

- Complete the AEGNS anti-money laundering due diligence questionnaire related to their policies and procedures for Cash Disbursements; and
- Cooperate with AEGNS in its review of the anti-money laundering due diligence questionnaire (e.g., provide any requested supporting Documentation) and be approved by AEGNS Compliance.

2.3.3.2 Other Cash Disbursement Requirements

In addition to the requirements contained in Section 2.10.4, "Use of Cardmember Information," on page 113, Section 2.9.13, "Requirements for Acquirers of Cash Disbursements," on page 103, Section 2.10.5, "Cash Disbursement Issuer Requirements," on page 114, and Section 4.5.1, "Card Acceptance Requirements for Cash Disbursement Providers," on page 240, Participants that have been activated for Cash Disbursement Transactions must (consistent with applicable local laws and regulations):

- Administer an anti-money laundering training and awareness program for all staff who support Cash Disbursements, developed to address the unique money laundering risks associated with these Transactions;
- Complete in-person customer identification prior to processing a Cash Disbursement Transaction;
- Monitor Cash Disbursement Transactions, including implementing and maintaining specific monitoring, escalation, and reporting as directed by AEGNS based on review of the due diligence questionnaire, or other risk and fraud factors; and
- Upon request by AEGNS, provide ongoing reporting relevant to the compliance aspects of their Cash Disbursement business including, but not limited to:
  - Information relating to local regulatory reporting, such as Suspicious Activity Reports (SARs);
  - The number and average value of Cash Disbursement Transactions; and
  - High value Cash Disbursement Transactions.

2.3.4 AML/ATF Requirements for All Prepaid Cards

Many Prepaid Cards offer features that make them potentially more susceptible to money laundering, misuse, or abuse. Such features include: anonymity or limited identity verification, Reload capability, and the transfer possibility in the case of anonymous Cards. In addition to the policies of an effective AML program detailed in Section 2.3.1, "General Requirements," on page 31 and the Cardmember Transaction monitoring required in Section 8.10.3, "Cardmember Risk Management," on page 392, Participants issuing Prepaid Cards must:

- Cooperate with AEGNS in its review of the AML due diligence questionnaire (e.g., provide any requested supporting Documentation) and be approved by AEGNS Compliance.
- Cooperate with AEGNS Compliance to review, understand, and document their Prepaid programs.
- Complete customer screening activities and sanction screening (KYC) before the Prepaid Cards it issues can be activated for use, except in the case of Anonymous Non-Reloadable Prepaid Cards sold individually.
- Implement appropriate processes based on risk management that identify the source of funds for the purchase of Prepaid products.
- Implement product limits (e.g., purchase limit, reload maximum, and maximum spend within a defined period) designed to ensure that the Cards are not viable platforms for money laundering or terrorist financing (consistent with local laws and regulations).

Prepaid Card Issuers must obtain approval from AEGNS Compliance before issuing new or modifying existing Prepaid Cards.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.3.4.1 AML/ATF Requirements for Non-Reloadable Prepaid Cards

In addition to the policies detailed in Section 2.3.4, "AML/ATF Requirements for All Prepaid Cards," on page 34, Participants issuing non-reloadable Prepaid Cards must:

- Restrict bulk sales of non-reloadable Prepaid Cards to third-party distributors and companies that demonstrate a legitimate business purpose, both of which must be approved by AEGNS. Bulk purchasers must not be permitted to resell or redistribute non-reloadable Prepaid Cards in bulk.
- Ensure KYC procedures are followed for the bulk sale of non-reloadable Prepaid Cards to third-party distributors. KYC procedures are not required for individual purchases unless required by local law or regulation.

Issuers of Prepaid Cards are not required to examine individual purchasers of Anonymous Non-Reloadable Prepaid Cards for the source of their funds unless required by applicable local laws or regulations.

2.3.4.2 AML/ATF Requirements for Reloadable Prepaid Cards

In addition to the policies detailed in Section 2.3.4, "AML/ATF Requirements for All Prepaid Cards," on page 34, Participants issuing reloadable Prepaid Cards must:

- Implement risk-based processes to identify purchasers of reloadable Prepaid Cards (KYC) as well as the source of funds used to reload the Cards, and conduct sanctions screening on all collected demographic data points.
- Ensure that funding of reloadable Prepaid Cards originates in the country where the Prepaid Card was issued.
- Include in the terms and conditions for reloadable Prepaid Cards that the product is not transferable.
- Ensure that third-party distributors adhere to all aspects of the AEGNS AML/ATF policy requirements set forth herein or otherwise communicated to Participants.
- Impose limits and restrictions on Prepaid Cards that are compliant with local laws and regulations to ensure the AML/ATF risks associated with these products remain at an acceptable level, including without limitations:
  - Purchase limit (initial Loading).
  - Restrict the maximum number of reloadable Prepaid Cards to be issued to a customer.
  - Maximum number of Reloads in a defined period.
  - Maximum frequency of Reloads in a defined period.
  - Maximum number of ATM withdrawals in a defined period.
  - Controls regarding Card use at foreign merchants, if applicable.
- Review the Prepaid Card Transaction history, if available, whenever a Prepaid Card is reloaded.
- Implement monitoring as detailed in Section 8.10.3, "Cardmember Risk Management," on page 392.

2.3.5 Non-Compliance

If AEGNS determines that a Participant is not in compliance with any part of the AML, screening, U.S. sanction, and anti-corruption requirements, consistent with Section 2.13, "Operating Policy Compliance and Enforcement," on page 123, AEGNS may require the Participant to:

- Implement additional policies, procedures, or controls;
- Require termination of its agreement with its S/E, Service Provider, or Cardmember;
- Provide written confirmation to AEGNS that termination of its agreement with the S/E, Service Provider, or Cardmember has been completed; and
- Take any other action that AEGNS, in its sole discretion, determines is appropriate with respect to the Participant.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Participants who do not comply with any part of the AML, screening, U.S. sanction, and anti-corruption requirements may be subject to non-compliance fees of up to $100,000 (USD) per incident. Refer to Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30 for more information.

2.3.6 Prohibited and Restricted Countries and Persons

Participants are prohibited from engaging in any American Express-related business with or in any country or region on which the United States has imposed comprehensive or highly restrictive economic sanctions (as set out below). This prohibition includes business with any individuals working for or on behalf of the government of any sanctioned country, regardless of their location, such as individuals working for embassies or consulates. In addition, Acquirers must not allow Transactions with Merchants that involve a sale of Goods that originated from a Prohibited or Restricted Country or Region, unless such Transactions are expressly and individually authorized by a license provided by OFAC.

Participants are also restricted from establishing any business for American Express with or in any country that appears on the U.S. State Department list of State Sponsors of Terrorism. In the following sections AEGNS has identified those countries that are currently prohibited or restricted under AEGNS policy for sanctions reasons. This list of countries may change from time to time. AEGNS will inform Participants of these revisions as they occur.

2.3.6.1 Prohibited Countries and Regions

The following jurisdictions, among others, are currently subject to comprehensive or highly restrictive sanctions programs administered by OFAC. As a result, Participants on the AEGN are prohibited from engaging in any American Express-related business with individuals or entities residing or located in, or incorporated under the laws of any of the following:

- The Crimean Region of Ukraine (including Sevastopol), and the so-called Donetsk People's Republic and Luhansk People's Republic regions of Ukraine
- Iran
- Democratic People's Republic of Korea (North Korea)
- Syria

Additionally, Participants are prohibited from engaging in any American Express-related business with any Cardmember, S/E, or other customer that is owned or controlled by the government of a prohibited country, including agencies and subdivisions and any entity owned, controlled by or acting on behalf of such governments (whether or not physically located in these countries, such as embassies and state-owned businesses).

If a Participant becomes aware that an Authorization Request has originated in one (1) of the Prohibited Countries and Regions, or by a government or related entity of one (1) of the Prohibited Countries and Regions, the Participant must immediately notify AEGNS.

2.3.6.2 Other Prohibited Countries

American Express policy prohibits Participants from engaging in any American Express-related business with Cards issued in any of the following countries or with Service Establishments located in or incorporated under the laws of any of the following countries:

- Russia
- Belarus

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.3.6.3 Restricted Countries

American Express policy restricts Participants from engaging in any American Express-related business with parties from the countries listed below as "restricted." Participants must obtain approval from AEGNS prior to doing business with individuals or entities residing in, located in, or incorporated under the laws of any of the following:

- Cuba

Participants may contact their AEGNS representative for more information.

2.3.6.4 Additional Prohibited Persons, Entities, and Governments

Participants are prohibited from engaging in any American Express-related business with any Person or entity, wherever located, or any entities 50% or more owned (in aggregate), controlled by, or acting on behalf of a Person or entity designated on any list of sanctioned Persons maintained by OFAC and/or targeted by sanctions maintained by U.S. authorities, including OFAC, or any equivalent foreign authority.

Participants are also prohibited from engaging in any American Express-related business with any of the following:

- The Government of Venezuela
- Entities owned by the Government of Venezuela
- Any individuals that are current employees or contractors of the Government of Venezuela, or that otherwise currently act on its behalf

2.3.7 Foreign Corrupt Practices Act and Anti-Bribery Requirements

Participants are prohibited from engaging in activity that would violate the United States Foreign Corrupt Practices Act of 1977, the United Kingdom Bribery Act of 2010, or any other anti-bribery or anti-corruption laws of any country in which the Participant is located or conducts any American Express-related business (collectively, "Anti-Corruption Laws"). Without limiting the foregoing, Participants may not directly or indirectly provide, offer, solicit, or accept anything of value for the purpose of improperly influencing or inducing an action or decision, inducing someone to influence improperly one's employer to affect an act or decision of such employer, or securing any improper advantage.

Participants shall ensure their officers, directors, and employees, and every other Person or company acting on their behalf or with their authority, foster a culture of compliance with Anti-Corruption Laws in connection with any American Express-related transactions or services.

Therefore, Participants shall incorporate best practices and activities designed to prevent violations of Anti-Corruption Laws such as, but not limited to:

- Well-defined policy and/or code of conduct addressing Anti-Corruption Laws
- Periodic anti-corruption training for all employees
- Business records are retained regarding the giving and receiving of meals, gifts, and entertainment
- Assessment of the anti-corruption risk of third-party relationships with the Participant's organization
- Dedicated resource(s) with oversight for the Participant's anti-corruption program

Should a Participant learn or have reason to suspect any violation of the Anti-Corruption Laws, in connection with any American Express-related transactions or services, the Participant must immediately notify AEGNS and take appropriate remedial measures.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4 Participant Data Security Policy

The AEGNS Data Security Policy (DSP) is a set of comprehensive policy requirements designed to protect Account Data whenever such data is stored, processed, or transmitted. Compromised data negatively impacts consumers, S/Es, and Card Issuers. Addressing this threat by implementing security operating policies can help improve customer trust, reduce potential liability, and enhance the security of the Network.

AEGNS has endorsed and incorporated into DSP the following:

- Payment Card Industry Data Security Standard (PCI DSS)
- Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS)
- Payment Card Industry PIN Security Standard Requirements
- Payment Card Industry PIN Transaction Security, Point-of-Interaction (PCI PTS POI) Standard
- Payment Card Industry Point-to-Point Encryption (PCI P2PE)
- Payment Card Industry Secure Software Lifecycle (PCI Secure SLC) Standard
- Payment Card Industry Secure Software Standard (PCI SSS)
- Payment Card Industry Software-based PIN Entry on Commercial off-the-shelf (COTS)

For details on requirements specific to PCI PIN Security, see Section 2.4.8, "Encryption Data Security Requirements," on page 44.

AEGNS recommends Participants and their Service Providers use a PCI Qualified PIN Assessor (QPA) to assess/demonstrate compliance to PCI PIN Security Standard Requirements.

These standards include requirements for security management, policies, procedures, network architecture, software design, POS and PIN acceptance devices, payment application security, and other critical protective measures. The standards are intended to help organizations proactively protect Account Data.

Details regarding the PCI standards and how to comply with their requirements can be found at www.pcisecuritystandards.org.

All Participants, S/Es, and Service Providers must comply with the AEGNS DSP. As part of that requirement, Participants must:

1. Comply with the PCI DSS, as outlined in Section 2.4.2, "Acquirer Data Security Compliance Requirements," on page 40 and Section 2.4.4, "Issuer Data Security Compliance Requirements," on page 42; and
2. Validate their compliance with the PCI DSS as outlined in Section 2.4.3, "Acquirer Data Security Compliance Validation Requirements," on page 41 and Section 2.4.5, "Issuer Data Security Compliance Validation Requirements," on page 43; and
3. Report to AEGNS their compliance validation with the PCI DSS, as outlined in Section 2.4.6, "Participant Data Security Compliance Validation Documentation," on page 43.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Participants must also ensure their agreements with S/Es and Service Providers include:

- A requirement to comply with the following:
  - PCI DSS
  - PCI PA-DSS
  - PCI PIN Security Standard
  - PCI PTS POI
  - PCI P2PE
  - PCI Secure SLC
  - PCI SSS
  - PCI Software-based PIN Entry on COTS
- Provisions requiring that S/Es and Service Providers report all instances of a Data Compromise immediately to the Participant, and in no case later than seventy-two (72) hours after discovery of the incident. See Section 2.4.11, "Notification of Data Compromise from AEGNS to Potentially Impacted Issuers," on page 49 for details.

  Note: "Exhibit 7. European Economic Area Data Protection Model Contracts" on page 454 will be deemed incorporated into the DSP for all Issuers that are European Economic Area (EEA) Participants.

AEGNS reserves the right, at its sole discretion, to request from Participants, at any time, information validating their own compliance as well as the compliance of their S/Es and Service Providers with any of the requirements stated in the DSP.

2.4.1 PCI Assessment and Reporting Relief for S/Es

The PCI Assessment and Reporting Relief program allows S/Es that implement Risk-Mitigating Technologies at the POS, such as EMV® or Point-to-Point Encryption (P2PE), to qualify for relief from PCI assessment and validation reporting requirements.

2.4.1.1 PCI Assessment and Reporting Relief Program

S/Es are not required to complete the PCI-related assessment and reporting if they meet the following criteria:

1. Continue to adhere to the PCI DSS, including the requirement prohibiting the storage of Sensitive Authentication Data, and
   a. Process at least 75% of Transactions through EMV-compliant terminals, or
   b. Process at least 75% of Transactions using PCI-listed P2PE solutions, or
   c. Process at least 75% of Transactions using a P2PE solution approved by a Qualified Security Assessor, and
2. Have not been involved in a Data Compromise in the last twelve (12) months.

The PCI Assessment and Reporting Relief program is not applicable to Service Providers.

Acquirers are responsible for ensuring that their S/Es qualify, and must obtain an attestation of eligibility at least annually from S/Es in the program. The attestation must include an acknowledgment from their S/Es that American Express requires all S/Es to adhere to the PCI DSS. For additional information, please contact your AEGNS representative.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

S/Es that do not qualify for PCI Assessment and Reporting Relief are subject to the current PCI-related policy reporting requirements outlined in Table 2-4, "S/E and Service Provider Compliance Validation Requirements," on page 42 and the related sections of the DSP.

AEGNS reserves the right to, at any time, and at its sole discretion:

1. Instruct Acquirers to remove S/Es from the PCI Assessment and Reporting Relief program, or
2. Request information from Acquirers regarding the S/Es participating in the PCI Assessment and Reporting Relief program.

2.4.2 Acquirer Data Security Compliance Requirements

Acquirers are responsible for determining their own internal compliance with the PCI DSS and applicable provisions of the following:

- PCI PTS POI
- PCI P2PE
- PCI PA-DSS
- PCI SSS
- PCI Secure SLC
- PCI Software-based PIN Entry on COTS requirements

AEGNS requires all Acquirers that deploy new and/or replaced POS devices, including PIN-acceptance devices, to utilize approved and validated PCI PTS POI devices and/or PCI Software-based PIN Entry on COTS Devices at the time of deployment. This requirement does not include unattended terminals, such as Customer Activated Terminals (CATs).

AEGNS requires attended and unattended CATs, Chip Card-enabled POS devices, PIN acceptance devices, and attachments or peripherals used by Acquirers, their Service Providers, S/Es, and their Service Providers for the processing of Offline and Online PIN Transactions to:

- Obtain a valid EMVCo approval for contact and/or Contactless devices, and
- Comply with the PCI POS device-related requirements as set forth in this section, and
- Complete an end-to-end Certification in accordance with the *POS Device Certification Process Guide*.

AEGNS requires all Acquirers that deploy new and/or replaced payment applications to utilize an active and validated PCI Payment Application at the time of deployment. This requirement is applicable to payment applications that are subject to the following:

- PCI PA-DSS validation, as defined in the *PCI Payment Application Data Security Standard (PA-DSS) Guide*, or
- PCI SSS, as defined in the *PCI Software Security Framework Secure Software Standard Program Guide*, and
- PCI Secure SLC, as defined in the *PCI Software Security Framework Secure Software Life Cycle (Secure SLC) Standard Program Guide*.

Acquirers must ensure that their Service Providers store Account Data only to facilitate Transactions in accordance with their agreements with the Acquirer. See Section 2.4.3, "Acquirer Data Security Compliance Validation Requirements," on page 41 and Section 2.4.6, "Participant Data Security Compliance Validation Documentation," on page 43 for additional details.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.2.1 Acquirers' S/Es and Service Providers Data Security Compliance Requirements

Acquirers must ensure that, in addition to themselves, Acquirers' Service Providers and Acquirers' S/Es comply with the AEGNS DSP, which incorporates the following requirements under the current PCI DSS:

- PCI PA-DSS
- PCI PTS POI
- PCI P2PE
- PCI Secure SLC
- PCI SSS
- PCI Software-based PIN Entry on COTS

AEGNS requires all Acquirers' Service Providers and S/Es that deploy new and/or replaced POS devices, including PIN-acceptance devices, to utilize approved and validated PCI PTS POI devices and/or PCI Software-based PIN Entry on COTS Devices at the time of deployment. This requirement does not include unattended terminals, such as Customer Activated Terminals (CATs).

AEGNS requires all Acquirers' Service Providers and S/Es that deploy new and/or replaced payment applications to utilize an active and validated PCI Payment Application at the time of deployment. This requirement is applicable to payment applications that are subject to PCI PA-DSS or to the PCI SSS and PCI Secure SLC (as referenced in Section 2.4.2, "Acquirer Data Security Compliance Requirements," on page 40).

2.4.3 Acquirer Data Security Compliance Validation Requirements

Acquirers must comply with PCI DSS and validate their compliance by submitting a PCI DSS Attestation of Compliance with authorized representative signature to AEGNS. All Documentation must be sent to SecureTrust, which administers the data security compliance program, via a secure Web portal, secure fax, or email at americanexpresscompliance@securetrust.com. Compliance validation is carried out at the expense of Acquirers, S/Es, or Service Providers.

2.4.3.1 Acquirers' S/Es and Service Providers Data Security Compliance Validation Requirements

Acquirers are responsible for obtaining the required compliance validation Documentation from their S/Es and Service Providers.

Compliance validation requirements for each S/E or Service Provider are based upon the volume of Transactions processed by the S/E or the Service Provider over a one (1) year period.

Transaction volume must be determined based on the aggregate number of Transactions conducted at all of the S/Es' locations, including all types of Card products.

S/Es and Service Providers are categorized into four (4) levels. Each level has specific criteria and validation requirement(s) as set forth in Table 2-4, "S/E and Service Provider Compliance Validation Requirements," on page 42.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Acquirers are responsible for determining the compliance validation levels of their S/Es and Service Providers and assigning them to the appropriate level.

Table 2-4. S/E and Service Provider Compliance Validation Requirements

Level	Definition/Criteria	Complete Compliance Validation Assessment[1]	Submit Validation Documentation to Acquirer[2]
1	An S/E or Service Provider is defined as Level 1 if it meets one (1) of the following criteria: • 2.5 million Transactions or more completed per year, or • Any S/E or Service Provider that AEGNS deems a Level 1.	**Mandatory** - Annual PCI Data Security Assessment	**Mandatory** - PCI DSS Attestation of Compliance with authorized representative signature
2	An S/E or Service Provider is defined as Level 2 if it completed 50,000 to 2.5 million Transactions per year.	**Mandatory** - Self- Assessment Questionnaire (SAQ) (unless PCI DSS Attestation of Compliance with authorized representative signature is provided)	**Mandatory** - Self- Assessment Questionnaire (SAQ) and the Approved Scanning Vendor (ASV) Report (unless PCI DSS Attestation of Compliance with authorized representative signature is provided)
3	An S/E or Service Provider is defined as Level 3 if it completed 10,000 to 50,000 Transactions per year.	**Recommended** - Self-Assessment Questionnaire (SAQ) (mandatory if required by American Express)	**Recommended** - Self-Assessment Questionnaire (SAQ) (mandatory if required by American Express)
4	An S/E or Service Provider is defined as Level 4 if it completed fewer than 10,000 Transactions per year.		

1. Refer to Section 2.4.6, "Participant Data Security Compliance Validation Documentation," on page 43 for details on specific validation Documentation.
2. AEGNS may request evidence of compliance with PCI DSS at any time.

Note: AEGNS reserves the right to request from Participants, at its own discretion, Documentation validating the correct level has been assigned to an S/E and/or Service Provider.

2.4.4 Issuer Data Security Compliance Requirements

Issuers are responsible for ensuring their own internal compliance with the PCI DSS and applicable provisions of the PCI PTS POI, PCI PA-DSS, PCI SSS, and PCI Secure SLC requirements.

AEGNS requires all Issuers and their Service Providers that deploy new and/or replaced payment applications to utilize active and validated PCI Payment Applications at the time of deployment. This requirement is applicable to payment applications that are subject to the following:

- PCI PA-DSS validation, as defined in the *PCI Payment Application Data Security Standard (PA-DSS) Guide*, or
- PCI SSS, as defined in the *PCI Software Security Framework Secure Software Standard Program Guide*, and
- PCI Secure SLC, as defined in the *PCI Software Security Framework Secure Software Life Cycle (Secure SLC) Standard Program Guide*.

Issuers must comply with the PCI DSS requirements. Issuers must also comply with a current version of the PCI PA-DSS, PCI SSS, and PCI Secure SLC requirements, where applicable to their business. They are responsible for determining their own internal compliance with the PCI DSS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.4.1 Issuers' Service Provider Data Security Compliance Requirements

In addition to complying with all requirements detailed in Section 2.4, "Participant Data Security Policy," on page 38, Issuers must validate the PCI DSS compliance status of their Service Providers.

Issuers are also required to determine the compliance validation levels of their Service Providers and assigning them to the appropriate level in accordance with the criteria detailed in Table 2-4, "S/E and Service Provider Compliance Validation Requirements," on page 42.

2.4.5 Issuer Data Security Compliance Validation Requirements

Issuers must comply with PCI DSS and validate their compliance by submitting a PCI DSS Attestation of Compliance with authorized representative signature to AEGNS. All Documentation must be sent to SecureTrust, which administers the data security compliance program, via a secure Web portal, secure fax, or email at americanexpresscompliance@securetrust.com. Compliance validation is carried out at the Issuer's expense.

2.4.5.1 Issuers' Service Provider Data Security Compliance Validation Requirements

Issuers are responsible for validating the PCI DSS compliance status of their Service Providers, as well as obtaining the required compliance validation Documentation from their Service Providers.

The Documentation must be submitted, upon request, to SecureTrust via a secure Web portal, secure fax, or email at americanexpresscompliance@securetrust.com.

2.4.6 Participant Data Security Compliance Validation Documentation

Participants are responsible for maintaining appropriate records to ensure the compliance validation Documentation requirements are met.

AEGNS will notify each Participant of the due dates for the specific annual and biannual data security-related compliance Documentation the Participant must submit to the Network.

2.4.6.1 Annual PCI Data Security Assessment

An Annual PCI Data Security Assessment includes a detailed examination of a Participant's, S/E's or Service Provider's equipment, systems, and networks (and their components) where Account Data is processed, stored, or transmitted.

The assessment can be conducted by a Qualified Security Assessor or prepared by the Participant, S/E, or Service Provider.

Note: Additional information regarding Qualified Security Assessors capable of performing Data Security Assessments can be found at www.pcisecuritystandards.org.

2.4.7 Participant Data Security Non-Compliance

Participants that fail to comply with the requirements relating to PCI data security compliance and validation, or the policy requirements of the Service Provider policy as outlined in Section 2.7, "Service Provider," on page 78 will provide AEGNS a PCI Prioritized Approach Template no later than 30 days following AEGNS' notification of the Participant as non-compliant.

The PCI Prioritized Approach Template will include a remediation date not to exceed twelve (12) months following the date the PCI Prioritized Approach Template was submitted, for achieving compliance. Participants will submit the PCI Prioritized Approach Template either to SecureTrust (via a secure Web portal or secure fax), or email at DataSecurityPolicy@aexp.com, or submit to your local AEGNS representative.

For more information about the PCI Prioritized Approach Template, contact your AEGNS representative.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

AEGNS will not impose non-compliance fees prior to the remediation date; however, Participants remain liable to AEGNS for all indemnity obligations for a Data Compromise, and are subject to all other provisions of the DSP. See Section 2.4.12, "Cardholder Data Compromise Recovery Process (CDCRP)," on page 49 for details on the CDCRP.

AEGNS, at its sole discretion, retains the right to impose non-compliance fees if:

- A PCI Prioritized Approach Template has not been submitted in accordance with the requirements stated in this section,
- The remediation steps outlined in the PCI Prioritized Approach Template for Non-Compliant Status were not met,
- Any of the requirements of the PCI Prioritized Approach Template for Non-Compliant Status were not fulfilled, or
- The mandatory validation Documentation was not provided to AEGNS by the applicable deadline or upon request.

Participants that do not comply with the requirements detailed in Section 2.4, "Participant Data Security Policy," on page 38 may be subject to fees as stated in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

2.4.8 Encryption Data Security Requirements

AEGNS implemented Encryption data security requirements designed to protect Account Data and to assist Participants to effectively manage Cryptographic Keys associated with Account Data. AEGNS endorsed the PCI PIN Security Standard Requirements and the Qualified PIN Assessor (QPA) Program, and along with the existing AEGNS DSP security requirements, AEGNS will continue to enhance policies for Account Data protection and key management. See the "Definitions" chapter beginning on page 495 for the definition of the term "Encryption."

Details regarding the PCI PIN Security Standard Requirements can be found at: www.pcisecuritystandards.org.

The key management requirements outlined in this section reflect industry best practices and controls for Cryptographic Keys. As such, the control objectives set out in the PCI PIN Security Standard Requirements must be applied to all keys used in the processing, generation, loading and/or protection of Account Data. This includes, but is not limited to, the following:

- Hardware Master Keys
- Key Encrypting Keys (KEKs)
- Security Domain Master Keys
- Sensitive Authentication Data Keys
- Sensitive Authentication Data Protection Keys

All Participants are required to use a Two-Key Triple Data Encryption Algorithm (TDEA) as a minimum Encryption standard.

Participants are encouraged to transition to Advanced Encryption Standard (AES) according to the PCI PIN directive.

Non-compliant Participants may be subject to Data Security Policy non-compliance fees as detailed in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.8.1 Online PIN Encryption Requirements

The PCI PIN Security Standard Requirements define the requirements for secure PIN management, processing, and transmission of PIN data at ATMs and attended and unattended Point of Sales (POS) terminals.

All Issuers and Acquirers must abide by the requirements as defined by PCI.

Details on the effective dates can be found at www.pcisecuritystandards.org.

Issuers and Acquirers must comply with the Network Specifications manual components specific to the PCI PIN Security Standard Requirements they have adopted.

2.4.8.2 Issuer Compliance Requirements

AEGNS requires that all Issuers incorporate the control objectives set out in the PCI PIN Security Standard Requirements as guidelines regarding key management and the protection of Account Data.

Any Account Data stored, processed, or transmitted within an Issuer's systems must be protected in compliance with the AEGNS DSP. For key management and additional PIN data protection requirements, the networks used to transmit payments of Issuers and their Service Providers must comply, as applicable, with the control objectives of the PCI PIN Security Standard Requirements.

Issuers' and their Service Providers' PIN processing must be conducted in accordance with the requirements as detailed in Section 2.4, "Participant Data Security Policy," on page 38.

Issuers should plan to transition to Advanced Encryption Standard (AES) according to the PCI directive for all cryptographic activities, including, but not limited to, Card Security Code keys (CSCKs), PIN Key management, PIN blocks, and Key Encrypting Keys (KEKs).

Issuers and their Service Providers,if using dynamic key exchange, must support key blocks as indicated in the PCI PIN Security Standard Requirements and defined in the Network Specifications manuals.

Non-compliant Issuers may be subject to Data Security Policy non-compliance fees as detailed in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

2.4.8.3 Acquirer Compliance Requirements

Any Account Data stored, processed, or transmitted within an Acquirer's systems must be protected in compliance with the AEGNS DSP. For key management and additional PIN data protection requirements, the networks used to transmit payments of Acquirers and their Service Providers, and S/Es and their Service Providers must comply, as applicable, with the control objectives of the PCI PIN Security Standard Requirements.

Acquirers and their Service Providers, and S/Es and their Service Providers' PIN processing should also be conducted in accordance with the requirements listed for POS terminals as detailed in Section 2.4, "Participant Data Security Policy," on page 38.

Acquirers are encouraged to transition to Advanced Encryption Standard (AES) according to the PCI PIN directive.

Acquirers must ensure Encryption algorithms are set for all cryptographic activities including, but not limited to, Card Security Code Keys (CSCKs), PIN Key management, PIN blocks, and Key Encrypting Keys.

For Online PIN, refer to Section 2.4.8.1, "Online PIN Encryption Requirements," on page 45 for more information on Online PIN requirements.

Acquirers and their Service Providers, and S/Es and their Service Providers, if using dynamic key exchange, must support key blocks as indicated in the PCI PIN Security Standard and defined in the Network Specifications manuals.

Non-compliant Acquirers may be subject to Data Security Policy non-compliance fees as detailed in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.8.4 Third-Party Compliance Requirements

AEGNS requires that all third parties involved in the processing, transmission, or storage of Account Data or Sensitive Authentication Data must be protected in compliance with the control objectives of PCI DSS Security Requirements.

Card Production environments must also comply with the control objectives defined in the *PCI Card Production and Provisioning Logical Security Requirements* and *PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

2.4.8.5 Use of Alternate Encryption

Subject to AEGNS' approval, Participants may elect to use other cryptographic techniques to secure Transactions. In such instances, Participants must submit to AEGNS, prior to implementation, a request to use any such alternate methods.

2.4.8.6 Key Management Program Compliance Requirements

All Participants are required to define and implement procedures for a key management program to manage all Cryptographic Keys used to support American Express-related activities, including, but not limited to, protecting PIN Keys and keys used to generate or validate CSCKs. The program must cover the management of keys and materials related to POS Transactions, ATM Transactions, Card issuance, and messages among terminals and Participants throughout the Transaction Life Cycle. The procedures will also contain the defined roles for key management personnel to address separation of duties, dual control, and split knowledge. These procedures must align with the principles prescribed by PCI PIN Security Standard Requirements for the types of the Cryptographic Keys being used. Key management programs being implemented by Participants must be done in a manner consistent with the PCI PIN Security Standard Requirements as detailed in Section 2.4.8, "Encryption Data Security Requirements," on page 44.

2.4.8.7 Participant Responsibilities Following Data Compromise

All instances of Data Compromise, including any form involving Encryption keys, must be reported to AEGNS. The Participant must follow the requirements as detailed in Section 2.4.9, "Requirements for Notification of Data Compromise," on page 47 and Section 2.4.10, "Participant Responsibilities Following Discovery of Data Compromise," on page 48.

Participants who do not comply with the notification requirements of this section will be responsible for all costs incurred by AEGNS in addition to non-compliance fees as stated in Section 10.6.2, "Notification of Data Compromise Non-Compliance Fees," on page 411.

Additionally, Participants who do not comply with any of the requirements of the "Participant Responsibilities Following Discovery of Data Compromise" will be responsible for all costs incurred by AEGNS in addition to non-compliance fees as stated in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

2.4.8.8 Encryption Security Policy Validation Requirements

In accordance with the requirements stated in Section 2.4.6, "Participant Data Security Compliance Validation Documentation," on page 43, Participants may be responsible for submitting to AEGNS their compliance validation Documentation. AEGNS reserves the right to request from Participants at its sole discretion, Documentation validating that the Participants, their Service Providers, S/Es and their Service Providers are correctly executing and monitoring cryptographic policies, programs, and standards.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.9 Requirements for Notification of Data Compromise

In order to enable AEGNS and Participants to respond promptly and to mitigate losses involved in a Data Compromise, Participants are required to do the following:

1. Cause all S/Es, Service Providers, and agents of the Participant to report to the Participant immediately, and in no case later than seventy-two (72) hours after the breached entity's discovery of the following:
   - A Data Compromise,
   - Any suspected or confirmed loss, theft, or misappropriation by any means of any materials, records, or information, including Encryption keys, in any form containing Account Data, and
   - Any such loss, theft, or misappropriation by an S/E, Service Provider, or agent of the Participant.
2. Report to AEGNS immediately and in no case later than seventy-two (72) hours after discovery of the following:
   - A Data Compromise,
   - Any suspected or confirmed loss, theft, or misappropriation by any means of any materials, records, or information, including Encryption keys, in any form containing Account Data, and
   - Any such loss, theft, or misappropriation by an S/E, Service Provider, or agent of the Participant.

If a Data Compromise occurs at an Issuer, irrespective of whether the Issuer provided notification to AEGNS that the Card or Account number in question was lost, stolen, not received, or otherwise misappropriated, the Issuer shall have the risk of loss for Charges on Cards for which the Issuer provided an Authorization.

Participants who do not comply with any of the requirements of this section will be responsible for all costs incurred by AEGNS in addition to non-compliance fees as stated in Section 10.6.2, "Notification of Data Compromise Non-Compliance Fees," on page 411.

Notwithstanding any contrary confidentiality obligation in the Participant Agreement, AEGNS has the right to disclose information about any Data Compromise to Participants on the Network and/or the general public, as required by applicable law, by judicial, administrative, or regulatory order, decree, subpoena, request, or other process, in order to mitigate the risk of fraud or other harm or otherwise, to the extent appropriate, to operate the Network.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.10 Participant Responsibilities Following Discovery of Data Compromise

In addition to the notification requirements stated in Section 2.4.9, "Requirements for Notification of Data Compromise," after the discovery of a Data Compromise, Participants are required to do the following:

1. Contact American Express Enterprise Incident Response Program (EIRP) by phone or email:
   - Within the United States call 888-732-3750
   - Outside the United States call +1 602-537-3021
   - Email: EIRP@aexp.com. Please include AEGNS in the subject line.

   Submit a report to EIRP that shall contain, to the extent possible, the following information:
   - Name of Participant and breached entity (for example, S/E, Service Provider)
   - Number of Account numbers compromised
   - Type of Account Data compromised
   - Pertinent details regarding the suspected or confirmed loss or theft and ensuing investigation
   - Name and telephone number of Person to contact for additional information
   - Name and telephone number of Person reporting the suspected or confirmed loss, theft, or misappropriation
   - List of specific Account numbers compromised
   - Law enforcement information

Note: The above information must be sent using a secure channel. Prior to submission, contact EIRP at EIRP@aexp.com for instructions.

2. Immediately conduct an investigation of the incident and limit the potential exposure of Cardholder Data and/or Sensitive Authentication Data.
3. Fully cooperate with AEGNS to rectify issues resulting from the incident, including providing access to the premises involved. In addition, AEGNS must be given access to all pertinent records and Documentation as soon as they are available including analysis and reporting from forensics companies, as well as access to information needed to verify the ability to prevent future Data Compromises in a manner consistent with the requirements of the DSP, which may include, but are not limited to, a validation by a Qualified Security Assessor that issues from the incident have been remediated.
4. AEGNS may require an independent forensic investigation. The forensic investigation must be conducted in accordance with the Payment Card Industry Forensic Investigator (PFI) program unless otherwise agreed upon by AEGNS. Information on the PFI program and requirements can be found at www.pcisecuritystandards.org.
5. The final forensic report must be provided to AEGNS within ten (10) Business Days of the completion of the report. AEGNS will not be responsible for any costs incurred related to the forensic investigation.
6. Should AEGNS determine the Participant, its S/Es, or their agents are deficient or negligent in maintaining Cardholder Data or Sensitive Authentication Data securely, and/or reporting, and/or investigating the loss of such data, the Participant must immediately comply with any corrective action required by AEGNS. For a fee, AEGNS will provide Investigative services, which may include training, investigative coordination, and actual investigations in the case of substantial losses that occurred across markets or any incidents involving significant losses.

Participants who do not comply with any of the requirements of this section will be responsible for all costs incurred by AEGNS in addition to non-compliance fees as stated in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.11 Notification of Data Compromise from AEGNS to Potentially Impacted Issuers

Upon learning a Data Compromise may have occurred, AEGNS will notify all impacted Issuers of potentially compromised Account numbers by way of one (1) or more alerts through the AEGNS FraudNet Participant Communication Platform (PCP). Refer to Section 8.10.3.4, "Issuer Participant Communication Platform (PCP)," on page 396 for more information.

Multiple alerts about a single Data Compromise can be identified by the common reference number associated with the PCP. When AEGNS provides multiple alerts about a single Data Compromise, all Account numbers included in those alerts may be eligible for consideration for compensation under the Cardholder Data Compromise Recovery Process (CDCRP), provided the required conditions to invoke the CDCRP exist. The Account numbers included in multiple alerts are also subject to the limitations stated in Section 2.4.12.6, "CDCRP Liability Calculations," on page 52. Account numbers included in alerts may have been received from the compromised entity or provided by another authority (i.e., American Express Global Security, law enforcement).

If a Participant does not provide a complete list of Account numbers involved in the Data Compromise, as required by Section 2.4.10, "Participant Responsibilities Following Discovery of Data Compromise," on page 48 or if the list is incomplete or inaccurate, as determined by the forensic company or as provided by the Participant, AEGNS will conduct an internal data analysis on behalf of the Participants to identify the Account numbers involved in the Data Compromise. In conducting the internal analysis, AEGNS will rely on the information known about the Data Compromise at that time. AEGNS will provide the impacted Issuers the resulting list of Account numbers involved in the Data Compromise.

Issuers must take action immediately after receiving an alert to minimize any fraud activity on the identified Account numbers including, but not limited to, monitoring, closing, or blocking these Account numbers. By notifying Issuers of Account numbers in this way, AEGNS is in no way confirming, explicitly or implicitly, that an Issuer will subsequently be eligible to file a claim under Section 2.4.12, "Cardholder Data Compromise Recovery Process (CDCRP)."

2.4.12 Cardholder Data Compromise Recovery Process (CDCRP)

The Cardholder Data Compromise Recovery Process (CDCRP) provides a mechanism for Issuers to seek recovery from an Acquirer for a Data Compromise Event under the conditions set forth in this section. Issuers are required to use the regular Chargeback process as described in the "Chargeback Policies" chapter beginning on page 280 to recover fraud losses whenever this remedy is available to them.

The CDCRP is the exclusive remedy for Issuers to recover from an Acquirer the incremental fraud losses and operational costs associated with a Data Compromise Event. The CDCRP limits fraud liability for Acquirers to Transactions with a Transaction Date that falls within the Data Compromise Event Window. The Data Compromise Event Window is calculated as follows: up to 365 days prior and 30 (thirty) days following the date the last notification of the potentially involved Account numbers in a Data Compromise was sent by AEGNS to the Issuer.

2.4.12.1 Data Compromise Event Criteria

All of the following criteria must be met before AEGNS will declare the Data Compromise to be a Data Compromise Event:

1. The Data Compromise occurred at an entity who has the relationship with an Acquirer that is located in the United States, United States Territories, or Canada.
2. The Data Compromise involved a minimum of 10,000 distinct Account numbers.
3. The Data Compromise involved the compromise of the Primary Account Number, and Sensitive Authentication Data or Expiration Date.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Once AEGNS has determined that the Data Compromise Event criteria listed above have been met, AEGNS, at its sole discretion, and no later than forty-five (45) days after the final forensic report is received, will inform the Issuer of its claim eligibility. The Issuer Notification Date (IND) is defined as the date on which AEGNS notifies the Issuer of its claim eligibility under the CDCRP.

2.4.12.2 CDCRP Financial Liability Relief for S/Es

The CDCRP Financial Liability Relief Program provides a reduction of financial liability for a Data Compromise Event to qualifying S/Es that utilize Risk-Mitigating Technologies to protect Cardholder and Sensitive Authentication Data.

2.4.12.2.1 CDCRP Financial Liability Relief Program

An S/E may qualify to receive a reduction of financial liability for a Data Compromise Event if it meets all of the following criteria:

- S/E is using Risk-Mitigating Technologies, such as EMV, P2PE, and/or Tokenization.
- S/E must have implemented Risk-Mitigating Technologies prior to the Data Compromise Event and such technologies were in use during the Data Compromise Event Window.
- S/E conducted a thorough forensic investigation in accordance with the Payment Card Industry Forensic Investigator (PFI) program, unless otherwise agreed upon by AEGNS.
- The forensic report clearly indicates the Risk-Mitigating Technologies used to process, store and/or transmit the Cardholder Data and/or Sensitive Authentication Data.

AEGNS, at its sole discretion, will evaluate financial liability reduction and determine how Risk-Mitigating Technologies were used to process, transmit, and/or store the Cardholder Data and/or Sensitive Authentication Data.

AEGNS will grant relief based on the parameters outlined in the following table:

Table 2-5. CDCRP Financial Liability Relief

Technology	Criteria	Relief Percentage
EMV - **or** Risk-Mitigating Technologies (i.e., P2PE, Tokenization)	75% or more of total Transactions were processed using a Chip-Enabled Device during the Data Compromise Event Window at the S/E locations impacted by the Data Compromise Event.	50% Reduction
	Forensic report indicates Risk-Mitigating Technologies were used during the Data Compromise Event Window at 75% or more of the S/E locations impacted by the Data Compromise Event.	
EMV - **and** Risk-Mitigating Technologies (i.e., P2PE, Tokenization)	75% or more of total Transactions were processed using a Chip-Enabled Device during the Data Compromise Event Window at the S/E locations impacted by the Data Compromise Event - **and** Forensic report indicates Risk-Mitigating Technologies were used during the Data Compromise Event Window at 75% or more of the S/E locations impacted by the Data Compromise Event.	75% to 100% Reduction[1]

1. The percentage of the reduction is determined by the lowest percentage of adoption of all Risk-Mitigating Technologies. For example, if an S/E meets all criteria to receive a reduction of financial liability, 95% of their total Transactions were processed using a Chip-Enabled Device during the Data Compromise Event Window at the S/E locations impacted by the Data Compromise Event, and 80% of their total Transactions utilized P2PE during the Data Compromise Event Window at the S/E locations impacted by the Data Compromise Event, the S/E's total liability amount will be reduced by 80%, the lower percentage of adoption of the two (2).

AEGNS reserves the right, at its sole discretion, to request information validating the use of these technologies from its Participants.

For additional information, please contact your AEGNS representative.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.12.3 Issuer Responsibilities under the CDCRP

All of the following criteria must be met before AEGNS will accept and begin processing a claim from an Issuer under the CDCRP:

- In order to qualify to present a CDCRP claim for a Data Compromise Event, the Issuer must have a minimum of 500 distinct Account numbers involved in the referenced Data Compromise Event.
- The Issuer must demonstrate that it was in compliance with the required fraud-related policies stated in the "Security and Fraud" chapter beginning on page 375 during the Data Compromise Event Window.

To initiate a claim under the CDCRP, the Issuer must prepare a CDCRP claim form and submit it to AEGNS within thirty (30) days from the Issuer Notification Date as communicated by AEGNS at the time of the claim eligibility notification. The claim form must be filled out completely and include all Documentation necessary to support the claim.

Once the Issuer has filed a claim with AEGNS, the Issuer is not allowed to file another claim for the same Data Compromise Event. See "Exhibit 14. AEGNS CDCRP Issuer Claim Form" on page 481 for a sample form and further instructions on its use. CDCRP claim forms should be submitted to gnsfraud@aexp.com.

2.4.12.4 AEGNS Responsibilities to Acquirers under the CDCRP

AEGNS will inform the Acquirer involved in the Data Compromise Event of its actual CDCRP financial liability no later than fifteen (15) days after the deadline by which an Issuer must file claims. Liability figures are based on the number of Account numbers claimed to be involved during the Data Compromise Event Window multiplied by a per-Account number rate, as described below in Section 2.4.12.6, "CDCRP Liability Calculations."

Acquirers will have up to thirty (30) days from the date that AEGNS provides this figure to lodge an appeal with AEGNS for consideration. AEGNS will consider the merits of the appeal within thirty (30) days of the appeal submission and reserves the right to take additional time as needed to consider the appeal. Once the appeal has been reviewed, AEGNS will provide a final decision to the Acquirer.

Acquirers may determine when and how to notify their compromised S/Es or agents of the estimated and final liability amounts.

2.4.12.5 AEGNS Responsibilities to Issuers under the CDCRP

Upon receipt of an Issuer's claim under the CDCRP, AEGNS will review the claim and determine whether the Issuer has met all of the CDCRP criteria listed above in Section 2.4.12.3, "Issuer Responsibilities under the CDCRP,"

Issuers will be credited in approximately sixty (60) calendar days after AEGNS has collected the funds from the Acquirer(s). AEGNS will notify Issuers of their actual recovery amount and expected date to be credited typically within 180 days following the date the Acquirer was notified of its CDCRP financial liability. This notification may take longer depending on Acquirer appeals or other extenuating circumstances.

AEGNS will compensate Issuer(s) claims based on the per-Account number rate, and reserves the right to adjust that amount based on the amount recovered from the Acquirer. If the amount collected is less than the amount claimed by all Issuers, AEGNS will proportionally adjust all Issuer recoveries, if any. Under no circumstances will AEGNS be liable to any Issuer for any amount claimed hereunder.

All decisions by AEGNS relative to recovery and compensation under this section are final.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.4.12.6 CDCRP Liability Calculations

For eligible claims, AEGNS will calculate the recovery amount by multiplying the total number of distinct Account numbers claimed in the Data Compromise Event by a per-Account number rate of $5 (USD). For example, if a Cardmember's Account has a total of three (3) Cards issued with the Account and only two (2) Cards are compromised, AEGNS will include only those Account numbers that were compromised in the calculation; the calculation would be ($5 x 2 = $10). AEGNS will exclude from this calculation any Account number that was included in a prior claim within the twelve (12) months prior to the reporting date of the current event in the claim.

The total recovery amount may also be reduced if the compromised S/E qualifies for the CDCRP Financial Liability Relief Program. Refer to Section 2.4.12.2.1, "CDCRP Financial Liability Relief Program," on page 50.

2.5 Digital Capabilities

This section includes policies that are associated with the digital capabilities enabled by AEGNS. The section outlines the digital and Token services offered by AEGNS and defines Participant responsibilities.

AEGNS recommends all Participants who deploy digital capabilities adhere to the requirements in the following sections:

- Section 4.2 "S/E Card Acceptance Procedures" on page 214
- Chapter 5, "Authorizations," beginning on page 245

2.5.1 Digital Capabilities Enablement

Issuers should support core features to facilitate certain digital capabilities on the AEGN. The digital capabilities supported by Digital Capabilities Enablement (DCE) are described in the remainder of Section 2.5, "Digital Capabilities," on page 52.

2.5.1.1 Digital Capabilities Enablement Issuer Guidelines

The following list describes the requirements Issuers should adhere to:

Table 2-6. Digital Capabilities Enablement Issuer Guidelines

Token BIN Allocation - Issuers should adhere to requirements in Section 2.5.2.4.1, "Token BIN and BIN Management," on page 56 and Section 2.10.1.5, "Issuer Liability for Licensed BINs," on page 112.
Life Cycle Management - Life Cycle Management (LCM) allows Issuers to provide up to date Cardmember Account details to the AEGN. LCM is the management of changes related to a Token, PAR, Card-on-file, Card art, or other Cardmember data. Issuers should integrate LCM to provide updated Cardmember Account details to the AEGN. Cardmember Account details which require LCM may differ by digital payment type.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.1.2 Digital Capabilities Enablement AEGNS Optional On-Behalf-Of Services

The following list describes the services AEGNS may perform on behalf of Issuers to support Digital Capabilities Enablement:

Table 2-7. Digital Capabilities AEGNS Optional On-Behalf-Of Services

Token BIN Allocation - AEGNS will allocate Issuers a Token BIN range to facilitate Tokenization of Cardmember Transactions.
Token Creation and Management - For each provisioning request, AEGNS allocates a Token to the PAN contained in the provisioning request.
Dynamic Data Validation - Dynamic Data is an AEGN-generated Transaction-unique value used for Authorization. The AEGN validates the Dynamic Data in the POS Authorization Request (1100) message on behalf of the Issuer.
Limited Use Key (LUK) Creation, Refresh, and Management - The AEGN creates Limited Use Keys (LUKs), or payment keys, and loads these onto a Mobile Device to facilitate digital payments.

Not all On-Behalf-Of Services are available for all digital capabilities. Contact your AEGNS representative for more information.

2.5.2 Tokenization

Tokenization is the process that involves replacing a Primary Account Number (PAN) with a surrogate value called a Token. Using Tokens mitigates fraud by removing sensitive data from a Cardholder Data environment.

Different Tokenization solutions may be applied for Transaction processing involving a variety of payment form factors such as Cards and Mobile Devices, as well as different Transactions types, including Near Field Communication (NFC), mobile-based, Card-on-file, in-app, etc. AEGNS may offer Tokenization Services to any Token Requestor (including, but not limited to, Participants and S/Es).

To further enhance data security in the payments ecosystem, the use of Tokens may be restricted to specific Transaction types, Merchants, or payment channels.

The end-to-end Tokenization process entails the participation of a number of entities as well as key functional components, all of which play specific roles and responsibilities in the process.

Regardless of the Tokenization solution, the ecosystem includes, at a minimum, the following functions:

- Token Request and Token Requestor
- Token Service Provider (TSP)
- Token process management
- Token BIN management strategy
- Token Domain management
- Token Life Cycle Management

All entities involved in any aspect of the Tokenization process addressed in this policy, must comply with the requirements detailed in Section 2.7, "Service Provider," on page 78 and/or the *EMV Payment Tokenization Specification - Technical Framework*, as applicable.

Participants may also be required to adhere to any relevant Tokenization-related technical specifications or Certification requirements published by AEGNS, as applicable.

AEGNS strongly recommends that Participants and their Service Providers consider PCI's Tokenization Product Security Guidelines when developing their own Tokenization ecosystem or relying on a third-party solution that provides a Tokenization-related service.

For more information, please see PCI's Tokenization Product Security Guidelines at www.pcisecuritystandards.org.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.2.1 Token Request and Token Requestor

A Token Requestor is an entity that initiates requests that PANs be tokenized, by submitting Token Requests to a TSP.

Token Requestors may include: S/Es, Acquirers, Issuers, third-party processors, Digital Wallet Program Providers, etc.

Token Requestors must be registered by a TSP prior to Tokens being requested. After successful registration with a TSP, the Token Requestor will be assigned a Token Requestor ID (TRID).

TSPs may remove a Token Requestor's registration and/or Token Requestor IDs at any time. Once a Token Requestor's ID has been removed no new Tokens will be issued under the TRID and existing Tokens may be deactivated.

2.5.2.2 Token Service Provider

Token Service Providers (TSPs) are entities that generate and issue Tokens in response to Token Requests submitted by registered Token Requestors.

TSPs perform a number of Tokenization ecosystem functions which may include, but are not limited to, Token Generation and Issuance, application of data security-related controls in adherence to PCI DSS, Token Mapping, Token Request-related functions, ID&V, maintaining the Token Vault, and Token Life Cycle Management.

AEGNS, Participants, as well as third-party vendors may perform the role of a TSP. All entities that choose to provide Tokenization-related services as a TSP, must comply with the policy requirements outlined in Section 2.7, "Service Provider," on page 78 as well as the *EMV Payment Tokenization Specification - Technical Framework*. Participants may also be required to adhere to any relevant Tokenization-related technical specifications and/or Certification requirements published by AEGNS, as applicable. In addition, TSPs must comply with all
data security-related requirements detailed in Section 2.4, "Participant Data Security Policy," on page 38.

2.5.2.3 Token Process Management

This section describes the Tokenization ecosystem elements and processes involved in the Token process management.

2.5.2.3.1 Token Types

Tokens may be generated, depending on the intended use, as different Token types. Tokens may be used for initiating payment Transactions, or non-financial processes such as rewards, marketing and/or loyalty tracking.

Payment Tokens are Tokens that may be used to initiate payment Transactions.

Payment Tokens intended to be used in the context of an EMV environment must conform to the standards detailed in the *EMV Payment Tokenization Specification - Technical Framework*.

Tokens can be generated for limited time use (Dynamic Tokens), or across multiple Transactions completed with a unique Account number (Static Tokens), such as in Card-on-file environments.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.2.3.2 Token Generation

TSPs are responsible for generating Payment Tokens requested by registered Token Requestors. Each Token must be linked to the Token Requestor via an identification value unique to the requestor called Token Requestor ID.

Individual Tokens must have an expiry date that may be the same as the Primary Account Number (PAN) expiry date or may differ, depending on the type of Token generated and any additional conditions agreed upon between the Token Requestor and the TSP.

Several Payment Tokens may be generated for a single PAN but the same Payment Token cannot be generated for more than one (1) PAN.

Payment Tokens generated by a TSP may only be used for conducting Transactions within the Token Domain assigned for each Token. See Section 2.5.2.5, "Token Domain Management," on page 56 for details.

Payment Tokens are generated and issued based on the capabilities provided by a Token Vault, which is operated by the TSP, and serves as a repository for all Payment Tokens. In addition to generating and issuing Payment Tokens, a Token Vault performs the following functions:

- Maintain the Payment Token-to-PAN mapping
- Provide security and processing controls pursuant to the PCI DSS and any other relevant requirements as determined by AEGNS
- Make the Payment Token-to-PAN mapping available, as applicable, during the Transaction Life Cycle
- Apply Domain Restrictions Controls during Transaction processing, as required

TSPs are responsible for employing strict physical and logical security measures to protect Cardholder Data and Sensitive Authentication Data throughout all phases of the Tokenization process. PAN-related data stored in the Token Vault must be secured by means that will render all sensitive data unreadable.

TSPs must ensure the managing and protection of all data stored in the Token Vault in accordance with the data security requirements of the PCI DSS. Details regarding the PCI standards and how to comply with their requirements can be found at www.pcisecuritystandards.org.

2.5.2.3.3 Token Assurance ID&V

ID&V refers to a risk-based set of methods providing a level of Authentication for data such as Cardholder and Card Account-related information, One-Time Password (OTP), etc. resulting in a Token Assurance Level set by the TSP, and provided to the Issuer.

Different Token ID&V steps may be performed by the TSP, the Token Requestor, the Issuer or a third party. The Token Assurance Level provides a confidence level as to the Payment Token-to-PAN binding and Cardholder Authentication.

The Payment Token Assurance ID&V process is critical in supporting secure and reliable Transactions initiated with Payment Tokens, throughout the Transaction Life Cycle.

Token Assurance Levels may be updated if additional ID&Vs are subsequently performed.

2.5.2.3.4 Token Mapping

Token Mapping is the process of assigning a Token to an original PAN, resulting in a trusted Token-to-PAN association based on the type of Token requested and the method used to generate it.

Token Mapping allows for the retrieval of either the PAN or its corresponding Token(s) from the Token Vault, as needed, during Transaction processing. Any component of the Tokenization ecosystem intended to facilitate the PAN retrieval from the Token Vault, must be secured in accordance with the PCI DSS. (www.pcisecuritystandards.org).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.2.3.5 De-Tokenization

De-tokenization refers to the process of retrieving the PAN from its associated Token, based on the Token-to-PAN mapping stored in the Token Vault. The method used to generate the Token determines whether or not a PAN is retrievable.

De-tokenization should not be possible based solely on knowing the Token value. A Token should never be de-tokenized with the goal of using the PAN during Transaction processing except to allow for completion of a Transaction.

The TSP must ensure that the ability to retrieve the PAN is restricted to explicitly designated entities, systems and individuals. TSPs must also have access controls in place in adherence to the PCI DSS, as well as the capability to validate that any De-tokenization request is originated by an authorized and authenticated requestor.

If the PAN is retrievable by any entity involved in the Tokenization payment ecosystem, all PCI DSS requirements related to the storage, transmission and processing of Account Data by the S/E will apply as detailed in Section 2.4, "Participant Data Security Policy," on page 38.

2.5.2.4 Token BIN Management Strategy

This section describes the Tokenization ecosystem elements and processes involved in the Token BIN management.

2.5.2.4.1 Token BIN and BIN Management

Tokens must be generated only using specifically assigned Token BINs and Token BIN ranges for Issuers, to ensure the following:

- Maintaining the Token-to-PAN mapping to eliminate the possibility of generating a Token that conflicts with a PAN, and
- Preserving the payment processing interoperability throughout the Transaction Life Cycle.

TSPs are responsible for the setup and management of their Token BINs and BIN ranges separately from the BINs and BIN ranges assigned to other PAN portfolios.

Once Token BIN ranges have been created and assigned, TSPs must make them available to all entities involved in the Transaction processing that need to make decisions based on those BIN ranges.

AEGNS reserves the right, at its sole discretion, to direct all facets of the generation and assignment of American Express Token BIN ranges regardless of the entity acting as the TSP.

2.5.2.5 Token Domain Management

This section describes the Tokenization ecosystem elements and processes involved in the Token Domain management.

2.5.2.5.1 Token Domain and Domain Restriction Controls

A Token Domain defines the types of Transactions for which a Payment Token may be used. Token Domains may be payment channel-specific, S/E specific, digital wallet-specific, etc. TSPs, at their discretion, will define Token Domains to maintain the integrity and security of all the Tokenization ecosystem functions and elements during Transaction processing.

TSPs must ensure that each Token Requestor has sufficient domain controls in place that reduces the potential for fraud to occur across channels and acceptance environments before issuing a Token. TSPs are also responsible for the establishment, implementation, and application of Token Domain Restriction Controls, which are a set of parameters to mitigate fraud by ensuring Payment Tokens are used as intended throughout all phases of the Transaction Life Cycle.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Token Domain Restriction Controls are Token Requestor-specific and are established based on information made available to the TSP during the Token Requestor registration process.

TSPs must coordinate with all relevant entities involved in the Tokenization ecosystem when determining Token Domain Restriction Controls in accordance with the requirements outlined in the *EMV Payment Tokenization Specification - Technical Framework*.

2.5.2.6 Token Life Cycle Management

TSPs are responsible for the management of Payment Tokens and the Token-to-PAN mapping in case of any changes to the PAN and its expiry date, which may have a direct impact on Payment Tokens or Transactions.

Token Life Cycle Management may involve, but is not limited to, events such as:

- Updates to the Token Assurance Level
- Token activation
- Token deactivation
- Token suspension
- Updates to PAN attributes
- Updates due to lost/stolen devices

2.5.3 Card-on-File Tokenization

Issuers in the United States, United States Territories, and Canada should adhere to the guidelines in Section 2.5.1, "Digital Capabilities Enablement," on page 52 to support Card-on-file Tokenization.

Refer to the *Card-On-File Tokenization Issuer/Acquirer Implementation Guide* for full details on configuration options, implementation procedures, and optional features.

Contact your AEGNS representative for specifications and additional information.

2.5.4 Digital Wallet Programs

Digital wallets allow Cardmembers to perform Transactions initiated from Mobile Devices.

AEGNS supports the following Digital Wallet Programs:

- **Digital Wallet Payments** - Digital wallet models where AEGNS is the TSP. Digital Wallet Payments include Transaction types conducted through a digital wallet residing on a Mobile Device operated by an AEGNS-recognized Digital Wallet Program Provider.

  Transaction types include:

  - Digital Wallet Contactless-initiated Transactions,
  - Digital Wallet Application-initiated Transactions and/or
  - Digital Wallet Magnetic Secure Transmission (MST) Transactions

  See Section 2.5.4.5, "Digital Wallet Payments," on page 63 for information specific to identifying Digital Wallet Payments.
- **Consumer-Presented Quick Response (CPQR)** – Digital wallet model where AEGNS may be the TSP. CPQR are Transactions where a Cardmember uses the Issuer application on a Mobile Device to generate a QR Code® that is scanned at a POS device.

  See Section 2.5.4.7, "Consumer-Presented Quick Response," on page 65 for additional information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Expresspay Mobile** – Digital wallet models where there is no TSP or AEGNS is not the TSP. Expresspay Mobile is a mobile version of Expresspay. Expresspay Mobile Transactions include: Contactless Transactions where:
  - The Expresspay application is hosted in a secure element of a Mobile Device, or
  - A software-based version of Expresspay Mobile where an Expresspay Mobile Host Card Emulation (HCE) Application resides on the operating system of a Mobile Device

  See Section 2.5.4.6, "Expresspay Mobile," on page 64 for additional information.

2.5.4.1 General Requirements for Digital Wallet Programs

Issuers and Digital Wallet Program Providers may participate in the development and deployment of Digital Wallet Programs subject to AEGNS approval.

Except as otherwise agreed to by AEGNS in its sole discretion, Issuers and Digital Wallet Program Providers must adhere to the following requirements in order for a Digital Wallet Program to be enabled as AEGNS-recognized:

- Each Issuer and Digital Wallet Program Provider must execute an agreement with AEGNS for each Digital Wallet Program.
- AEGNS digital wallet components and Issuer Certification must be completed prior to deployment of any Digital Wallet Program as detailed in the applicable service guides:
  - *Digital Wallet API Implementation Guide*
  - *Expresspay Mobile Device Certification Process Guide*
  - *Expresspay Mobile HCE Issuer Implementation Guide*
  - *Expresspay Mobile HCE Product Approval Guide*
  - *Expresspay Mobile HCE Security Requirements Guide*
  - *Expresspay Mobile Secure Element Certification Process Guide*
  - Issuer Personalization Certification Guide
- AEGNS Security Risk Assessment must be completed for all Digital Wallet Programs and Mobile Devices deployed as part of Digital Wallet Programs. Digital Wallet Application-initiated Transactions do not qualify for Fraud Liability Shift (FLS), unless an exception is granted during the Risk Assessment. The FLS exception is not applicable to person-to-person payments. Digital Wallet Application-initiated Transactions that qualify for the FLS Risk Assessment exception are identified by the Wallet Provider ID in both the POS Authorization Request (1100) and/or POS First Presentment (1240) messages. Refer to the Network Specifications manuals for additional information on Wallet Provider IDs. Wallet Provider IDs qualified for the Digital Wallet Application-initiated FLS exception include "YK."
- Digital Wallet Programs must adhere to the requirements detailed in the *Digital Wallet Fraud Baseline Principles.*
- Digital Wallet Programs utilizing Consumer Device Cardholder Verification Method (CDCVM), either on a Mobile Device using a secure element or HCE cloud software-based security, must comply with the CDCVM technical security requirements of the AEGNS Security Risk Assessment.
- Beta Testing with AEGNS must be completed prior to the release of a Digital Wallet Program. The result of the Beta Test must demonstrate to the satisfaction of AEGNS that the proposed Digital Wallet Program complies with AEGNS requirements, and can be accepted operationally by S/Es, and that Transactions initiated with Mobile Devices can complete the Transaction Life Cycle.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Digital Wallet Programs must adhere to the AML/ATF program requirements established in Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30.
- Digital Wallet Programs must adhere to the Marketing and Branding requirements established in Section 2.9.19, "Marketing, Advertising, and Public Relations," on page 108.
- Digital Wallet Programs must adhere to the Data Security requirements as established in Section 2.4, "Participant Data Security Policy," on page 38.

Issuers must demonstrate they have conducted their own due diligence and security assessment of the Digital Wallet Program.

AEGNS makes no representation or warranty concerning any Digital Wallet Program or any Digital Wallet Program Provider's performance of its obligations under any agreement with an Issuer.

2.5.4.2 Digital Wallet Program Participant Terms

For each Digital Wallet Program that a Participant elects to utilize, the Participant must execute a Digital Wallet Program Addendum to its Participant Agreement. In addition, Participants and AEGNS will each enter into independent agreements with the Digital Wallet Program Provider governing each party's participation in such program (respectively, the "Participant-Mobile Entity Agreement" and the "AEGNS-Mobile Entity Agreement").

- **Use of Data -** As between AEGNS and a Participant, their respective rights to use data received in connection with Digital Wallet Programs shall be as set forth in the respective Participant Agreement. With respect to a particular Mobile Entity, AEGNS' and each Participant's rights to use data shall be as set forth in the AEGNS-Mobile Entity Agreement and Participant-Mobile Entity Agreement, respectively.
- **Intellectual Property** - Except as explicitly set forth in a Digital Wallet Program Addendum, a Participant's participation in a Digital Wallet Program shall not transfer, convey, or restrict any interest in the intellectual property rights of AEGNS or such Participant. For the avoidance of doubt, AEGNS and Participants retain their rights with respect to any intellectual property, proprietary designations, patents, copyright registrations or trademark or service mark registrations or such other protection as may be appropriate to the subject matter, and any extensions and renewals thereof.
- **Suspension of Participation** - AEGNS may immediately suspend a Participant's participation in a Digital Wallet Program:
  - If AEGNS determines that such action is reasonably necessary to protect Network Participants and/or the safety or soundness of the Network,
  - To address Network security issues,
  - To comply with applicable law or changes in applicable law,
  - To protect the American Express Brand, or
  - For other risk or security purposes, as determined by AEGNS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Term of Participation** - A Participant's participation in a Digital Wallet Program shall be effective upon the date set forth in the relevant Digital Wallet Program Addendum and, unless terminated earlier as provided herein or in the Digital Wallet Program Addendum, shall remain in effect until the earliest to terminate of (i) the Participant Agreement; (ii) the Participant-Mobile Entity Agreement; or (iii) the AEGNS-Mobile Entity Agreement. AEGNS and Participant will promptly notify the other of any notice delivered by such party to the Digital Wallet Program Provider or by the Digital Wallet Program Provider to such party expressing an intent to terminate any agreement referenced in clause (ii) or (iii) above.
  In addition, AEGNS and the Participant will promptly notify the other of any notice received from a Digital Wallet Program Provider concerning such provider's intent to suspend, terminate, or alter a Digital Wallet Program. However, a Participant's participation in a Digital Wallet Program may be terminated by either AEGNS or Participant:
  - Upon thirty (30) days' notice of a material breach of the Digital Wallet Program Addendum or the terms set forth herein that has not been cured within the later of (1) thirty (30) days from date the breaching party is notified of the breach, or (2) the stated cure period for such breach; or
  - Upon ninety (90) days' prior written notice.
- **Wind Down** - Following the termination of a Digital Wallet Program Addendum, AEGNS and the Participant will work together to wind down participation in the Digital Wallet Program in an orderly manner and make proper and timely notifications to Cardmembers using such program, as required by applicable law or deemed reasonably necessary by the parties.
- **Obligations with Respect to Mobile Entity -** AEGNS makes no representation or warranty whatsoever concerning any Mobile Entity's performance of any of its obligations in respect of a Digital Wallet Program. Neither AEGNS nor any Participant shall hold the other accountable or responsible, or seek indemnification from the other, for a Mobile Entity's actions or failure to act in connection with Digital Wallet Program. AEGNS relies on certain data from Mobile Entities in order to perform certain services and provision eligible Cards. In the event that a Mobile Entity ceases or otherwise fails to provide such information, AEGNS shall have no liability to any Participant for any delays or inability to perform Network functions related to a Digital Wallet Program, including without limitation any services provided by AEGNS to a Participant pursuant to a Digital Wallet Program Addendum.
- **Incident Management** - In the event that a Participant experiences an issue with their participation in a Digital Wallet Program, the Participant should contact their AEGNS representative identified in the Digital Wallet Program Addendum, who will work to resolve the issue and provide regular updates to the Participant until the issue is resolved.

2.5.4.3 Digital Wallet Program Services

AEGNS provides services on behalf of Issuers in order to minimize host development required to process Digital Wallet Program Transactions. The following sections describe the services offered by AEGNS for Provisioning and Mapping, and Authorization Services.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.4.3.1 Provisioning and Mapping Services

AEGNS provides services on behalf of Issuers for provisioning and mapping Accounts to Mobile Devices. This service includes the following:

- **Personalization** - AEGNS generates all of the personalization data and scripts needed to support Digital Wallet Payments.
- **Provisioning Decisioning** - For Issuers electing the Provisioning Decisioning service, AEGNS reviews data received in the provisioning request and will make a decision based on parameters provided by Issuers. Issuers may choose from the following models:
  - **Risk score thresholds** - AEGNS will validate the data received from the wallet provider in the provisioning request against the thresholds provided by the Issuer in order to determine the provisioning decision.
  - **Pre-Authorization Network-based Dynamic Authentication (PANDA)** - Issuers may choose for AEGNS to perform an extended risk assessment in order to make the provisioning decision on their behalf

2.5.4.3.2 Authorization Services

- **Digital Wallet Payment Cryptogram Validation** - AEGNS validates the cryptogram received in the POS Authorization Request (1100) message on behalf of the Issuer. Issuers can elect for AEGNS to send the validation result in the Authorization Request for decisioning or for AEGNS to decline the Transaction on their behalf (in the event that AEGNS is unable to validate the cryptogram).

  For more information regarding the Expresspay Cryptogram Validation service, refer to the Network Specifications manuals.
- **Application Transaction Counter (ATC) Validation** - For Issuers that elect the ATC Validation service, AEGNS performs two (2) ATC validation checks:
  - AEGNS validates that the ATC value received in the Authorization Request has not been previously seen for the given Token or LUPC.
  - AEGNS validates that the ATC value received in the Authorization Request is within the expected range identified by the Issuer.

  If a replay attack is suspected, Issuers can elect for AEGNS to decline the Transaction on their behalf or for the Authorization Request to be sent to them for further validation (the AEGNS will not perform further risk checks in this instance).
- **EMV-to-Magstripe Processing** - For Digital Wallet Contactless-initiated Transactions initiated by an EMV capable Mobile Device transacting at an Expresspay EMV-enabled POS device, the Transaction will take place in EMV Mode. For Issuers that are unable to process EMV data, AEGNS offers an EMV to magstripe processing service. For Issuers using this service the EMV data contained in the original Authorization Request sent by the Acquirer to AEGNS is not sent to the Issuer.

  AEGNS validates key EMV data on behalf of the Issuer and records the validation results. The mag-stripe data, together with the EMV validation results and EMV-to-magstripe processing indicator, is sent to the Issuer.

  The POS First and Second Presentment (1240) messages sent to the Issuer will still contain the Chip Account Addendum (9240).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 2-8. Digital Wallet Program On-Behalf-Of Services

Provisioning and Mapping Services
AEGNS provides services on behalf of Issuers for provisioning and mapping Accounts to Mobile Devices. This service includes the following: • **Personalization** - AEGNS generates all of the personalization data and scripts needed to support Digital Wallet Payments.
Provisioning Decisioning - For Issuers electing the Provisioning Decisioning service, AEGNS reviews data received in the provisioning request and will make a decision based on parameters provided by Issuers. Issuers may choose from the following models: • **Risk score thresholds** - AEGNS will validate the data received from the wallet provider in the provisioning request against the thresholds provided by the Issuer in order to determine the provisioning decision. • **Pre-Authorization Network-based Dynamic Authentication (PANDA)** - Issuers may choose for AEGNS to perform an extended risk assessment in order to make the provisioning decision on their behalf
Authorization Services
Digital Wallet Payment Cryptogram Validation - AEGNS validates the cryptogram received in the POS Authorization Request (1100) message on behalf of the Issuer. Issuers can elect for AEGNS to send the validation result in the Authorization Request for decisioning or for AEGNS to decline the Transaction on their behalf (in the event that AEGNS is unable to validate the cryptogram). For more information regarding the Expresspay Cryptogram Validation service, refer to the Network Specifications manuals.
Application Transaction Counter (ATC) Validation - For Issuers that elect the ATC Validation service, AEGNS performs two (2) ATC validation checks: • AEGNS validates that the ATC value received in the Authorization Request has not been previously seen for the given Token or LUK. • AEGNS validates that the ATC value received in the Authorization Request is within the expected range identified by the Issuer. If a replay attack is suspected, Issuers can elect for AEGNS to decline the Transaction on their behalf or for the Authorization Request to be sent to them for further validation (the AEGNS will not perform further risk checks in this instance).
EMV-to-Magstripe Processing - For Digital Wallet Contactless-initiated Transactions initiated by an EMV capable Mobile Device transacting at an Expresspay EMV-enabled POS device, the Transaction will take place in EMV Mode. For Issuers that are unable to process EMV data, AEGNS offers an EMV to magstripe processing service. For Issuers using this service the EMV data contained in the original Authorization Request sent by the Acquirer to AEGNS is not sent to the Issuer. AEGNS validates key EMV data on behalf of the Issuer and records the validation results. The magstripe data, together with the EMV validation results and EMV-to-magstripe processing indicator, is sent to the Issuer. The POS First and Second Presentment (1240) messages sent to the Issuer will still contain the Chip Account Addendum (9240).

Not all On-Behalf-Of Services are available for all Digital Wallet Programs. Contact your AEGNS representative for more information.

2.5.4.4 Acquirer Certification Requirements for Digital Wallet Programs

Acquirers must complete AEGNS Network Certification to enable Digital Wallet Programs, including Certification for Expresspay and Expresspay Mobile.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.4.5 Digital Wallet Payments

There are three (3) types of Digital Wallet Payments:

- **Digital Wallet Contactless-initiated Transaction** - A Contactless Transaction initiated by a digital wallet within a Mobile Device through the Contactless interface at an Expresspay-enabled POS Device. This Transaction type is identified in the POS Authorization and Presentment messages with a "Y" value in Position 6 of the Point of Service Data Code field.

  Note: To identify Digital Wallet Contactless-initiated Transactions, the Network will assign a "Y" value in Position 6 of the Point of Service Data Code field in both the Authorization Request (1100) message and the First Presentment (1240) message.

- **Digital Wallet Application-initiated Transaction** (also referred to as "In App" Transaction) - A Transaction initiated by a digital wallet utilizing a Merchant application within the Mobile Device, and not through the Contactless interface. This Transaction type is identified in the POS Authorization and Presentment messages with a "Z" value in Position 6 and a "5" value in Position 7 of the Point of Service Data Code field.

- **Digital Wallet MST Transaction** - A Transaction initiated by a digital wallet within a Mobile Device through MST. This Transaction type is identified in the POS Authorization Request (1100) message by the Service Code value of 141.

Issuers should adhere to the requirements in Section 2.5.1, "Digital Capabilities Enablement," on page 52 before deploying Digital Wallet Payments.

AEGNS provides additional services for Digital Wallet Payments. Refer to Section 2.5.4.3, "Digital Wallet Program Services," on page 60 for additional information.

2.5.4.5.1 S/E Acceptance Procedures for Digital Wallet Contactless-Initiated Transactions

S/Es accepting Digital Wallet Contactless-initiated Transactions must follow the acceptance procedures as described in Section 4.2, "S/E Card Acceptance Procedures," on page 214 with emphasis on sections relating to Expresspay acceptance.

An Online Authorization must be obtained for Digital Wallet Contactless-initiated Transactions.

Additionally, Digital Wallet Contactless-initiated Transactions facilitated at Transit Access Terminals (TATs) must follow acceptance procedures described in Section 4.2.9, "Expresspay Transactions at Transit Access Terminals (TATs)," on page 218.

2.5.4.5.2 S/E Acceptance Procedures for Digital Wallet Application-Initiated Transactions

S/Es accepting Digital Wallet Application-initiated Transactions must follow the acceptance procedures described in Section 4.2, "S/E Card Acceptance Procedures," on page 214 with emphasis on sections relating to Card Not Present Charges.

An Online Authorization must be obtained for Digital Wallet Application-initiated Transactions.

In addition, S/Es participating in Digital Wallet Application-initiated Transactions must populate the "Z" value in Position 6 and the "5" value in Position 7 in the Point of Service Data Code field of both the POS Authorization Request (1100) message and the POS First and Second Presentment (1240) message. Refer to the Network Specifications manuals for more information.

2.5.4.5.3 S/E Acceptance Procedures for Digital Wallet MST Transactions

S/Es accepting Digital Wallet MST Transactions must follow the acceptance procedures as described in Section 4.2, "S/E Card Acceptance Procedures," on page 214.

An Online Authorization must be obtained for Digital Wallet MST Transactions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.4.5.4 Recurring Billing for Digital Wallet Payments

Recurring Billing and/or Charges that require an additional Authorization (subsequent Authorizations) are subject to the existing policies (including dispute policies) as defined throughout this manual and the Network Specifications manuals. See Section 5.6.2.2, "Card Not Present Recurring Billing Authorizations," on page 254 for more information.

Recurring Billing or subsequent Authorizations that contain a Token should not contain values of "Y" or "Z" in Position 6 of the Point of Service Data Code field but should contain values to identify the Transactions as Recurring Billing or subsequent Authorization in the appropriate Point of Service Data Code field.

2.5.4.5.5 Chargeback Policies for Digital Wallet Payments

Specific Chargeback rights are afforded to Issuers when presented with Digital Wallet Payment Transactions that meet the criteria set forth in the "Chargeback Policies" chapter beginning on page 280.

2.5.4.5.6 Credit ROCs for Digital Wallet Program Transactions

When providing a Credit for a Digital Wallet Program Transaction, S/Es must follow the requirements outlined in Section 4.2.22, "Credit ROCs," on page 237.

2.5.4.6 Expresspay Mobile

Expresspay Mobile is a mobile version of Expresspay where the Expresspay application is hosted in a secure element of a Mobile Device, or a software-based version of Expresspay Mobile where an Expresspay Mobile Host Card Emulation (HCE) Application resides on the operating system of a Mobile Device, and is capable of conducting Contactless Transactions.

An "X" value in Position 6 of the Point of Service Data Code field in the POS Authorization and Presentment messages identify this Transaction type. Refer to the Network Specifications manuals for additional information on mobile Service Codes and Application Interchange Profile (AIP) data in the POS Authorization message which will support identification of Expresspay Mobile and Expresspay Mobile HCE Transactions.

For additional information regarding Expresspay Mobile HCE, see Section 2.5.5, "Expresspay Mobile Host Card Emulation," on page 66.

Issuers and their Mobile Entities, including Service Providers as applicable, involved in the enablement and deployment of Expresspay Mobile on behalf of that Issuer must agree to meet all standards for Expresspay Transactions before being licensed to participate in the enablement and deployment of Expresspay Mobile.

In addition, to the extent that Mobile Entities have access to any American Express Information, Mobile Entities shall maintain internal protections, limitations, and other controls (including firewalls) necessary to prohibit and prevent any American Express Information from being accessed by, disclosed to, or used by any third party, including, without limitation, any third-party investor in, or Acquirer of, Mobile Entities. Without limiting the foregoing, this obligation shall prevent Mobile Entities from disclosing to, distributing to, or sharing any American Express Information with another general purposes card network that competes with American Express, including without limitation, any competitor that invests in, owns, controls, or is otherwise involved in, a Mobile Entity's business. American Express shall have the right to audit each Mobile Entity's compliance with this obligation.

Furthermore, Issuers who issue a Card to the Expresspay Mobile Cardmember and who, as an Issuer, choose to use Mobile Passcode as a Cardholder Verification Method (CVM) for Expresspay Mobile must ensure, prior to issuance of the Mobile Device to the Expresspay Mobile Cardmember, that the Mobile Passcode is not pre-set to the same value as that of the PIN issued for the Card.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.4.7 Consumer-Presented Quick Response

To perform Consumer-Presented Quick Response (CPQR) Transactions, a Cardmember uses the Issuer application on a Mobile Device to generate a Quick Response (QR) Code that is scanned at a POS device. The Token is included in the QR Code. To deploy CPQR, Participants must:

- Comply with the standards and requirements detailed in, but not limited to, the most current version of the following documents, as applicable:
  - *Consumer-Presented QR Code Specification*, which adheres to the *EMVCo QR Code Specification for Payment Systems: Consumer-Presented Mode*
  - *Consumer-Presented QR Code Implementation Guide*
- Adhere to any applicable local laws and regulations on QR Code standards.
- Support Tokenization. Where AEGNS is not the TSP, AEGNS strongly recommends that Participants and their Service Providers consider PCI's Tokenization Product Security Guidelines when developing their own Tokenization ecosystem or relying on a third-party solution that provides a Tokenization-related service.
- AEGNS may provide On-Behalf-Of Services such as Tokenization and Cryptogram services in support of CPQR. Refer to Section 2.5.2, "Tokenization," on page 53 and Section 2.5.4.3, "Digital Wallet Program Services," on page 60 for more information.
- Support value "1" in Position 6 and value "3" in Position 7 in the Point of Service Data Code field to identify CPQR Transactions.

2.5.4.7.1 Issuer Requirements for Consumer-Presented Quick Response

To deploy CPQR, Issuers must:

- Complete an AEGNS Security Risk Assessment for their application, which creates QR Codes in the Mobile Device.
- Ensure their application is compliant with the *Expresspay Mobile HCE Security Requirements Guide*.
- Ensure their application adheres to the Data Security requirements as established in Section 2.4, "Participant Data Security Policy," on page 38.
- Ensure their application is in accordance with AEGNS branding and style guidelines detailed in *QR Code Communication Guidelines*, available on Knowledge Base.
- Adhere to local legal and regulatory requirements for CPQR.
- CDCVM or Mobile Passcode must always be performed as a CVM for a CPQR Transaction. Other AEGNS-approved CVMs may also be incrementally requested by the POS device. See Section 5.10.2, "Cardholder Verification Methods," on page 263 and Table 5-3, "Cardholder Verification Methods," on page 263 for more information.

  Note: If an Issuer chooses to use Mobile Passcode as a CVM for CPQR Transactions, it must ensure, prior to enablement of an Issuer CPQR application on a Cardmember's Mobile Device, the Mobile Passcode is not pre-set to the same value as that of the PIN issued for the Card.
- Support value "1" in Position 6 and value "3" in Position 7 in the Point of Service Data Code field of the POS Authorization Request (1100) message.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.4.7.2 S/E Acceptance Procedures for CPQR Transactions

S/Es accepting CPQR Transactions must scan the QR Code presented by the Cardmember on their Mobile Device to initiate the Transaction. S/Es must also follow special acceptance procedures as follows:

- An Online Authorization must be obtained for CPQR Transactions.
- S/Es must complete a single ROC for the entire amount of the Transaction, except for airlines, cruise lines, and lodging S/Es, and Split Shipment Transactions of Goods. S/Es may accept separate forms of payment for the same Transaction (i.e., Cardmember wishes to pay for part of the Transaction as CPQR and the balance with another form of payment).
- If suspicious of a Cardmember presenting the Mobile Device, S/Es are instructed to call their Acquirer Authorization center with a Code 10. Refer to Section 4.3, "Code 10," on page 238 for additional information.
- S/Es are exempt from the requirements set forth in Section 4.2.7, "In-Person Charges," on page 216, Section 4.2.20.4, "No Signature/No PIN Program," on page 232, Section 4.2.10, "Card Not Present Charges," on page 221, and any other sections pertaining to Expresspay or Card Not Present Transactions.
- S/Es participating in CPQR Transactions must populate the "1" value in Position 6 and the "3" value in Position 7 in the Point of Service Data Code field of both the POS Authorization Request (1100) message and the POS First and Second Presentment (1240) message. Refer to the Network Specifications manuals for more information.

2.5.5 Expresspay Mobile Host Card Emulation

Host Card Emulation (HCE) allows NFC-enabled devices to conduct Contactless Transactions in a mode where all payment-related credentials are stored in the Mobile Device's operating system and/or a remote server (the "cloud") emulating the functionality of a Chip Card.

Expresspay Mobile HCE is a software-based version of Expresspay Mobile where an Expresspay Mobile HCE Application resides on the operating system (the "host") of a Mobile Device, and communicates with a server system (the "cloud") to facilitate Expresspay Mobile Transactions.

An HCE-based payment solution eliminates the reliance on an embedded physical secure element thereby enabling a direct communication between Cardmembers and Issuers while bypassing the need for intermediaries. In the absence of a secure element, any HCE payment functionality entails the implementation of HCE-specific requirements meant to ensure the security of sensitive data.

Regardless of the HCE solution, Issuers and their Mobile Entities involved in any aspect of HCE-based payment processing addressed in this policy must comply with the requirements detailed in, but not limited to, the most current version of the following documents, as applicable:

- *Expresspay Mobile HCE Issuer Implementation Guide*
- *Expresspay Mobile HCE Product Approval Guide*
- *Expresspay Mobile HCE Security Requirements Guide*
- *Expresspay Mobile HCE Specifications*

Those entities must also comply with the policy requirements of the AEGNS DSP as detailed in Section 2.4, "Participant Data Security Policy," on page 38 as well as the requirements detailed in Section 2.10.8, "Additional Marketing and Advertising Requirements for Issuers," on page 117. The applicability of the HCE requirements detailed in the above documents is subject to AEGNS approval.

For information related to "cloud" security, see the PCI DSS 2.0 Cloud Computing Guidelines to be found at www.pcisecuritystandards.org.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.5.1 Expresspay Mobile HCE Ecosystem

Transaction processing in an HCE ecosystem involves the participation of a number of entities, each playing a specific role and having associated responsibilities. A successful HCE ecosystem involves Issuers, Acquirers, S/Es, and HCE-certified vendors, for example, host providers, software development, cryptography, etc.

At a minimum, any HCE ecosystem consists of the following processes and functions:

- Identification and Verification (ID&V) management
- Expresspay Mobile HCE Application security
- Cryptogram management
- Expresspay Mobile HCE Application life cycle management
- Issuer and HCE-certified third-party responsibilities

Issuers and their HCE-certified vendors, as applicable, must, at a minimum, comply with the requirements related to the above processes and functions when adopting an HCE payment solution. Issuers are responsible for ensuring their HCE-certified vendors comply with the policy requirements.

2.5.5.1.1 ID&V Management

ID&V Management involves the use of specific, risk-based procedures aimed at identifying and authenticating the functional components involved in the completion of an Expresspay Mobile HCE Transaction, such as the Cardmember, the mobile application, the Mobile Device, and the Expresspay Mobile HCE Card:

Expresspay HCE Mobile Device Identification

Identification of the Mobile Device is a security-critical function during the issuance of the HCE application and the Expresspay Mobile HCE Card. Installing the application on the device it is intended for is essential to maintain data security and mitigate risk.

Device identifiers may be either generic, capable of performing across multiple Mobile Device-specific operating systems (cross-platform), or specific to a particular operating system. Refer to the *Expresspay Mobile HCE Issuer Implementation Guide* for details.

Expresspay Mobile HCE Cardholder Verification Methods (CVMs)

AEGNS strongly recommends the use of CVMs as a critical risk-mitigating factor. Issuers that decide not to utilize a CVM may be exposed to the risk of increased fraudulent activity.

The Cardmember's identity may be verified by implementing CVMs in accordance with the CVM-related requirements as detailed in the *Expresspay Mobile HCE Specifications* and the *Expresspay Mobile HCE Issuer Implementation Guide*.

Expresspay Mobile HCE Card Identification:

Within an Expresspay Mobile HCE Application, at least one (1) Expresspay Mobile HCE Card must be created. Each Expresspay Mobile HCE Card represents a virtual Expresspay Card.

Given the unique data security challenges in an HCE environment, Expresspay Mobile HCE Transactions are enabled through the use of Limited-Use Payment Credentials (LUPCs) or Limited Use Keys (LUKs), whose validity, as the name implies, is limited.

When issuing the LUPC or LUKs, the issuance system must make sure that they are issued to the correct Expresspay Mobile HCE Card residing on the correct HCE application.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.5.1.2 Expresspay Mobile HCE Application Security

The HCE application (applet) runs on the Mobile Device's operating system, and acts as a payment application thereby enabling HCE functionality to conduct an Expresspay HCE Mobile HCE Transaction. HCE application security consists of measures against threats exploiting potential vulnerabilities during the application's software life cycle, including architecture, design, development, implementation, and upgrade.

Mitigating HCE security risks is critical to the core functionality and usability of HCE. There are several fundamental mechanisms to provide a secure location for sensitive data within the HCE application. HCE applications must adhere to the requirements as detailed in the *Expresspay Mobile HCE Security Requirements Guide*.

2.5.5.1.3 Cryptogram Management and Tokenization

Cryptogram management refers to the methodologies and protocols governing the generation and maintenance of cryptograms required during HCE Transaction processing.

Cryptograms play a critical role in the management and security of the payment credentials, such as Cardholder Data. Credentials may be dynamically stored in the "cloud" as LUPCs or LUKs, which allow the Expresspay Mobile HCE Application to calculate unique cryptograms for each Expresspay Mobile HCE Transaction.

For more details on cryptogram management, see the *Expresspay Mobile HCE Security Requirements Guide*.

The use of Tokens in the HCE ecosystem is optional. If Tokens are part of an HCE-based solution, all Tokenization-related specifications must comply with the policy requirements detailed in Section 2.7, "Service Provider," on page 78.

2.5.5.1.4 Expresspay Mobile HCE Application Life Cycle Management

HCE applications have a life cycle that consists of the following steps:

1. Application management
2. User enrollment
3. Expresspay Mobile HCE Card issuance
4. Payment credentials issuance and maintenance

Issuers are responsible for the management of the Expresspay Mobile HCE Application life cycle phases and the underlying technical structure, functionality, and processes that enable Expresspay Mobile HCE Transactions.

No other NFC-based solution housed by the Mobile Device shall automatically override the functionality of the Expresspay Mobile HCE Application residing within the device's operating system.

Expresspay Mobile HCE Application Management

There are five (5) steps critical to Expresspay Mobile HCE Application management, as defined in the *Expresspay Mobile HCE Specifications*:

- Development
- Download
- Activation
- Updates and maintenance
- Removal

Issuers must comply with the requirements relevant to each of the above steps as detailed in the *Expresspay Mobile HCE Issuer Implementation Guide.*

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Issuers are required to use only applications that have received approval from AEGNS for functional approval (testing of the interface between the Expresspay Mobile HCE application and the terminal) as well as security approval (adherence to the security requirements for an HCE Application).

Issuers must also distribute the application in a manner that preserves the integrity and authenticity of the Expresspay Mobile HCE Application throughout the Expresspay Mobile HCE Transaction life cycle.

AEGNS recommends that Issuers have internal mechanisms in place to identify the individual installation and use of Expresspay Mobile HCE Applications on Mobile Devices.

User Enrollment

User Enrollment, also known as ID&V, is the process, as determined by the Issuer and meeting the minimum requirements as defined by AEGNS, of identifying and authenticating the user, the device, and application prior to the loading of payment data and credentials.

The ID&V requirements are defined in the *Expresspay Mobile HCE Security Requirements Guide* and the *Expresspay Mobile HCE Issuer Implementation Guide*.

Expresspay Mobile HCE Card Issuance

Once the user enrollment is completed and the Expresspay Mobile HCE Application is installed on the Mobile Device, the Issuer is responsible for issuing an Expresspay Mobile HCE Card to the Expresspay Mobile HCE Application.

Cardmember data must be loaded onto the Expresspay Mobile HCE Application in accordance with the requirements detailed in the *Expresspay Mobile HCE Specifications* and the *Expresspay Mobile HCE Security Requirements Guide*. Cardmember data is loaded both during the initial Expresspay Mobile HCE Card issuance and when an Expresspay Mobile HCE Card needs to be reissued.

Payment Credentials Issuance and Maintenance

The issuance of payment credentials are subject to the *Expresspay Mobile HCE Specifications.*

LUPCs and LUKs, which are provisioned following the issuance of an Expresspay Mobile HCE Card, allow the Expresspay Mobile HCE Application to conduct Expresspay Mobile HCE Transactions.

2.5.5.1.5 Certification of Expresspay Mobile HCE Products

This section outlines the obligations of Issuer and their Mobile Entities related to their respective roles and responsibilities within the HCE payment ecosystem.

In addition to the obligations detailed in the reference documents listed in Section 2.5.5, "Expresspay Mobile Host Card Emulation," on page 66, the following components of the HCE payment ecosystem are subject to approval by AEGNS:

- The Cardmember's Mobile Device as an acceptable payment device
- The Expresspay Mobile HCE Application installed on the Mobile Device
- The Issuer's (or its Service Provider's, if applicable) HCE platform/solution that manages the Expresspay Mobile HCE Application
- The authorization system of the Issuer
- The Expresspay-enabled S/E terminal
- The Token Service Provider (TSP), if applicable (optional)

Approval processes for Mobile Devices, HCE applications, and the issuance and the authorizations systems can be carried out independently from each other. The existing AEGNS approval process for Mobile Devices is extended to incorporate HCE-enabled Mobile Devices as well. For Certification requirements, see the *Expresspay Mobile HCE Product Approval Guide.*

AEGNS reserves the right to verify the physical and logical security controls of the issuance system, which, at AEGNS' discretion, may be subject to the requirements detailed in the American Express Participant Data Security and Physical Site Review, which is available from your AEGNS representative.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.6 Payment Account Reference

Payment Account Reference (PAR) is a non-financial reference generated by AEGNS that is associated with a Primary Account Number (PAN). PAR can be utilized by Acquirers and their S/Es to link the PAN and associated Tokens. PAR values are not intended to be a Cardmember identifier or PAN replacement and cannot be used to initiate a Transaction. AEGNS will assign PAR values to Accounts that have associated Tokens.

2.5.6.1 Payment Account Reference - Acquirer Requirements

Acquirers and their S/Es who adopt PAR must only use PAR for the following purposes:

- Facilitation of incremental services, including loyalty programs, with the Cardmember's express consent.
- Completion of Transactions where the Cardmember uses multiple form factors such as Cards and Mobile Devices (for example, Transactions at Transit Access Terminals).
- Management of Cardmember inquiries.
- Compliance with Credit ROC requirements and restrictions by verifying that the Token or PAN presented corresponds to the Account used for the original Transaction. Refer to Section 4.2.22.2, "Credit ROC Restrictions," on page 238.
- Management of Acquirer and S/E fraud risk.
- Support compliance with applicable laws and regulations.

PAR must not be used for other purposes without the prior written approval of AEGNS.

2.5.7 Secure Remote Commerce

Secure Remote Commerce (SRC) is an E-commerce checkout capability that creates a secure and consistent Cardmember checkout experience across digital channels, including Mobile Devices, web browsers, and other connected devices.

2.5.7.1 SRC Ecosystem

SRC is supported by the *EMV Secure Remote Commerce Specifications*. SRC establishes a streamlined E-commerce checkout capability through ecosystem roles.

2.5.7.1.1 SRC System

AEGN assumes the SRC System role. The SRC System is a technical platform that facilitates E-commerce payments and manages relationships between SRC Participants.

2.5.7.1.2 SRC Initiator

The SRC Initiator (SRCi) supports checkout and/or the secure retrieval of Digital Card and payment data from the SRC System on behalf of a payment-enabled application.

2.5.7.1.3 Digital Card Facilitator

The Digital Card Facilitator (DCF) facilitates the storage and display of Digital Card data for selection. The DCF receives Digital Card data from the Issuer.

2.5.7.1.4 Digital Payment Application

The Digital Payment Application (DPA) is the S/E's checkout application.

The DPA integrates SRC software into its Cardmember checkout experience, allowing integration with the SRCi and SRC System.

For more information on SRC and Participant roles in SRC, refer to the *EMV Secure Remote Commerce Specifications*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.7.2 General SRC Requirements

Participant deployment of SRC is subject to AEGNS discretion. Contact your AEGNS representative for more information.

Participants must adhere to the following requirements for SRC participation:

- Marketing and Branding requirements established in Section 2.9.19, "Marketing, Advertising, and Public Relations," on page 108 and any SRC branding guidelines as advised by AEGNS.
- Data Security requirements as established in Section 2.4, "Participant Data Security Policy," on page 38.
- Requirements detailed in the *EMV Secure Remote Commerce Specifications*.

Note: Anonymous Prepaid Cards are ineligible for SRC Transactions.

2.5.7.3 Issuer SRC Requirements

Issuers facilitate enrollment of Cardmembers into SRC and are responsible for providing Digital Card data.

Issuers that deploy SRC must adhere to the requirements listed below and should adhere to the guidelines in Section 2.5.1, "Digital Capabilities Enablement," on page 52.

During SRC implementation, Issuers that deploy SRC:

- Must select configuration options (described in the *Click to Pay Issuer Implementation Guide*).
- May provide Card Image(s) containing Card Artwork to AEGNS for display in SRC Cardmember experience. If an Issuer elects to provide its Card Image(s) for this purpose, the Issuer must select this configuration option during implementation.

If the Issuer does not elect to provide its Card Image(s), AEGNS will display a generic American Express Card Image.

Additional information about SRC terms and conditions can be found in "Exhibit 5. Secure Remote Commerce Terms and Conditions" on page 451.

Refer to the *Click to Pay Issuer Implementation Guide* for full details on configuration options, implementation procedures, and optional features.

2.5.7.4 Acquirer SRC Requirements

Acquirers must ensure S/Es that deploy SRC adhere to the requirements as specified in Section 2.5.7.5, "S/E SRC Requirements," on page 71.

2.5.7.5 S/E SRC Requirements

S/Es that deploy SRC must adhere to the following requirements:

- Integrate with an AEGNS-approved SRCi.
- Adhere to the requirements in Section 4.2.10, "Card Not Present Charges," on page 221.
- Contact their Acquirer if suspicious of an SRC Transaction.

2.5.7.6 SRC Chargeback Policies

S/Es that process SRC Transactions must adhere to dispute requirements for Card Not Present Transactions set forth in the "Chargeback Policies" chapter beginning on page 280.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.8 Issuer Originated Payments

Issuer Originated Payments (IOPs) are Transactions initiated by Cardmembers, using a payment solution provided by their Issuer to send funds to pay Service Establishments (S/Es).

AEGNS supports Merchant-Presented Quick Response (MPQR) as a type of IOP.

2.5.8.1 General Requirements for Issuer Originated Payments

Issuers and Acquirers may participate in the development and deployment of IOPs, subject to AEGNS approval.

Except as otherwise agreed to by AEGNS in its sole discretion, each Participant must adhere to the following requirements to enable IOPs:

- Execute an agreement with AEGNS for each IOP deployment.
- Integrate with AEGNS Application Programming Interface (API) messages for IOP deployment.
- Adhere to AML/ATF program requirements established in Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30.
- Adhere to marketing and branding requirements established in Section 2.9.19, "Marketing, Advertising, and Public Relations," on page 108.
- Adhere to Data Security requirements established in Section 2.4, "Participant Data Security Policy," on page 38.
- Ensure there are procedures and controls in place for monitoring and reporting fraud data on IOP Transactions to meet requirements set forth in Section 8.7, "Issuer Fraud Reporting," on page 382, as well as Section 8.9, "AEGNS Acquirer and S/E Risk Management," on page 383.
- Support value "8" in Position 6 in the Point of Service Data Code field to identify IOP Transactions.

AEGNS strongly recommends Participants monitor and track IOP Transaction volumes, and consider implementing fraud-mitigation measures such as setting Transaction parameters.

2.5.8.2 Merchant-Presented Quick Response

MPQR is an IOP Transaction that allows Cardmembers to initiate Transactions using an Issuer application on a Mobile Device to capture a Merchant-Presented QR Code.

Participants must comply with the standards and requirements detailed in, but not limited to, the most current version of the following documents, as applicable:

- Merchant-Presented QR Code Specification, which adheres to the EMVCo QR Code Specification for Payment Systems: Merchant-Presented Mode.
- *Merchant-Presented QR Code Implementation Guide*.

Participants must also adhere to any applicable local laws and regulations on QR Code standards.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.5.8.2.1 Authorization Processing for MPQR

MPQR Transactions are subject to special processing rules. Subsequent to the Cardmember initiating the Transaction using an Issuer application on a Mobile Device to capture a Merchant-Presented QR Code:

The Issuer will create and send an API message to AEGNS.

AEGNS then creates the POS Authorization Request (1100) message on receipt of the Issuer API message.

The Issuer will respond with a POS Authorization Response (1110) message, and AEGNS will send an API message to the Acquirer to notify them of this Transaction.

The Acquirer can accept or decline this Transaction.

If the Transaction is accepted, the Acquirer will notify the S/E and send an acceptance API message to AEGNS. AEGNS will send an API message to the Issuer that the Transaction is successful.

If the Transaction is declined, the Acquirer will notify the S/E and send a decline API message to AEGNS. AEGNS will then send a POS Authorization Reversal Advice (1420) message to the Issuer.

Issuers must adhere to Authorization-related policies in the "Authorizations" chapter beginning on page 245.

Acquirers must adhere to Authorization-related policies in the "Authorizations" chapter beginning on page 245, except for the following: Section 5.5, "Acquirer Authorization Requirements," on page 253, Section 5.6, "POS Authorization Requests," on page 253, Section 5.9, "Network Floor Limits," on page 261, Section 5.11, "ATM Authorizations," on page 266, and any other sections of the "Authorizations" chapter beginning on page 245 that pertain to POS or Offline Authorizations.

2.5.8.2.2 Acquirer Requirements for MPQR

Acquirers must ensure:

- A Transaction notification is sent to the S/E to inform them the Transaction was successful or unsuccessful.
- There are procedures in place for S/Es to process refunds and reversals for MPQR Transactions. See *Merchant-Presented QR Code Implementation Guide* for more information. S/Es processing Credit ROCs for MPQR Transactions are exempt from the requirements set forth in Section 4.2.22.1, "Completing Credit ROCs," on page 237.
- Acceptance marks at S/E locations are compliant with AEGNS branding and style guidelines detailed in *QR Code Communication Guidelines*, available on Knowledge Base.
- Their S/Es follow the requirements in Section 2.5.8.2.3, "S/E Acceptance Procedures for MPQR," on page 73.
- The POS First Presentment (1240) message includes value "8" in Position 6 and value "3" in Position 7 of the Point of Service Data Code field.

2.5.8.2.3 S/E Acceptance Procedures for MPQR

S/Es accepting MPQR are exempt from the requirements set forth in Section 4.2.7, "In-Person Charges," on page 216, Section 4.2.20.4, "No Signature/No PIN Program," on page 232, and Section 4.2.10, "Card Not Present Charges," on page 221, and must instead meet the requirements below.

Acquirers must ensure their S/Es meet the following requirements:

- The S/E must ensure its Merchant-Presented QR Code is not altered or tampered with.
- The S/E must receive a notification from the Acquirer that the Transaction has been approved and check the Transaction amount is correct before providing the Goods or Services.
- If the S/E does not receive the notification from the Acquirer, the S/E should contact the Acquirer to confirm the status of the MPQR Transaction.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- If suspicious of a Cardmember or notification from the Acquirer, S/Es are instructed to contact their Acquirer.
- AEGNS strongly recommends S/Es retain records of MPQR Transactions (e.g., notification from the Acquirer, invoice, or other Documentation of the Transaction).
- For MPQR Transactions made using the Card Not Present environment, S/Es are responsible for the actions of their delivery agents; therefore, S/Es are advised not to allow shipping address changes or interceptions to occur during the delivery. Whenever possible, the S/E should deliver merchandise to the matched Cardmember's address information and obtain a signature of the Person accepting the delivery.

2.5.8.2.4 Issuer Requirements for MPQR

To deploy MPQR, Issuers must:

- Complete an AEGNS Security Risk Assessment for their application, which initiates MPQR Transactions.
- Ensure their application adheres to the Data Security requirements established in Section 2.4, "Participant Data Security Policy," on page 38.
- Ensure their application is in accordance with AEGNS branding and style guidelines detailed in the *QR Code Communication Guidelines*, available on Knowledge Base.
- Adhere to local legal and regulatory requirements for MPQR.
- Use at least one AEGNS-approved CVM for MPQR Transactions as listed in Section 5.10.2, "Cardholder Verification Methods," on page 263 and Table 5-3, "Cardholder Verification Methods," on page 263.

  Note: If an Issuer chooses to use Mobile Passcode as a CVM for MPQR Transactions, it must ensure, prior to enablement of an Issuer MPQR application on a Cardmember's Mobile Device, the Mobile Passcode is not pre-set to the same value as that of the PIN issued for the Card.
- Support value "8" in Position 6 and value "3" in Position 7 in the Point of Service Data Code field of the POS Authorization Request (1100) message.

2.5.8.2.5 Chargeback Policies for MPQR

Specific Chargeback rights are afforded to Issuers when presented with MPQR Transactions that meet the criteria set forth in the "Chargeback Policies" chapter beginning on page 280.

2.6 Indirect Acceptors

Indirect Acceptors are a payment intermediary that contracts with an Acquirer to facilitate payments to third-party End Beneficiaries. The Indirect Acceptor accepts the Card, but does not send Card information to the End Beneficiary.

An End Beneficiary may separately be an S/E that directly accepts the Card. For example, a retailer may accept the Card (as an S/E) and also accept payment through one or more Indirect Acceptors (as an End Beneficiary).

Indirect Acceptors may operate through one or more different business models including:

- Bill Payment Provider: An S/E that is engaged by Cardmembers to pay a bill on their behalf. Bill Payment Providers charge the Cardmembers' Account and pay the End Beneficiary identified in the bill using another method, such as bank transfer, check, or wire.
- Installment Payment Provider: An S/E offering Cardmembers the ability to pay for purchases made at an End Beneficiary in installments over a fixed period.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Marketplace: an S/E that offers their prominently branded platform (website or mobile application), for Cardmembers to browse and purchase from multiple End Beneficiaries. Cardmembers pay for their purchases on the same platform.
- Peer-to-Peer Payment (P2P): A service offered through a payment application that enables a transfer of funds to and from its registered users.
- This does not include a transfer of funds with the intention of purchasing Goods or Services.
- Staged Digital Wallet: An S/E with a payment platform that allows Cardmembers to use a Card to fund a purchase in real time to an End Beneficiary.

Participants should refer to Section 7.9, "Chargeback Policy Rules," on page 304 to understand the Chargeback policies that apply to Indirect Acceptors.

Participants that fail to comply with the requirements in accordance with this section may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.6.1 Acquirer Requirements for Indirect Acceptors

Acquirers that contract with Indirect Acceptors are liable for all acts, omissions, and other adverse conditions caused by the Indirect Acceptors and their respective End Beneficiaries. As a result, the Acquirer must, at all times, be responsible for and manage, direct, and control all aspects of its Indirect Acceptor activities. Acquirers must also enforce all program management and operating policies applicable to Indirect Acceptors and End Beneficiaries in accordance with this Section 2.6.1, "Acquirer Requirements for Indirect Acceptors," on page 75, including enforcing the relevant policies based on the business model of the Transaction.

Prior to entering into an agreement with an Indirect Acceptor, the Acquirer must assess and determine that the Indirect Acceptor has adequate resources, financial and otherwise, to meet their obligations and deliver the services in accordance with applicable law and AEGNS' *Business and Operational Policies* and Network Specifications manuals.

Indirect Acceptors are considered S/Es and therefore subject to all requirements and obligations that apply to S/Es. Additionally, AEGNS reserves the right to designate an S/E as an Indirect Acceptor.

Indirect Acceptors are classified as a restricted industry and Acquirers must comply with the requirements set out in Section 2.9.4.2, "Restricted Industries," on page 95.

Acquirers must require that their Indirect Acceptors:

- Comply with Section 5.6.2, "Card Not Present Authorization Requests," on page 254.
- Comply with the requirements in Section 4.2.12, "Merchant-Initiated Transactions," on page 223 when processing non-Cardmember-Initiated Transactions.
- Obtain and maintain all required licenses and approvals necessary to conduct business.
- Not engage in American Express-related business with End Beneficiaries in prohibited or restricted industries. Refer to Section 2.9.4, "Prohibited and Restricted Industry Requirements," on page 94.

2.6.1.1 Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements

Acquirers must, for their Indirect Acceptors, meet the Anti-Money Laundering (AML), Anti-Terrorist Financing (ATF), and sanction screening requirements established in Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30. In addition, for all Indirect Acceptor models, except Stored Value Digital Facilities and Marketplaces, the Acquirer or their Indirect Acceptor must screen End Beneficiaries as customers, following the requirements in Section 2.3.2, "Customer Screening Program," on page 32.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.6.1.2 Right to Request Information

AEGNS may request that Acquirers provide information about their Indirect Acceptors and respective End Beneficiaries when needed to validate compliance. When requested, Acquirers must provide AEGNS with information about Indirect Acceptors and their End Beneficiaries no later than thirty (30) days, or as otherwise specified, after such request.

Additionally, upon request of AEGNS, the Acquirer must provide an Attestation of Compliance with the general requirements as set out in Section 2.6.1, "Acquirer Requirements for Indirect Acceptors," on page 75.

2.6.1.3 Data Element Requirements

Indirect Acceptor Transactions submitted to AEGNS by Acquirers must contain the mandatory data elements as defined in the Network Specifications manuals. Refer to the Network Specifications manuals for more information.

Acquirers must ensure that Indirect Acceptors submit accurate data and conduct periodic checks to ensure accuracy.

Acquirers must adhere to the following requirements when populating the Merchant Category Code field in both the Authorization Request and First Presentment messages:

Table 2-9. Indirect Acceptor Merchant Category Code Requirements

Transaction Type	Merchant Category Code (MCC)
Bill Payment Provider	The appropriate Merchant Category Code for each End Beneficiary
Installment Payment Provider	MCC 5999 - Miscellaneous and Specialty Retail
Marketplace	The appropriate Merchant Category Code that best describes the majority Goods and Services of the Marketplace
Peer-to-Peer Payment (P2P)	MCC 6538 - P2P Payments
Stored Value Digital Facility	MCC 6540 - Stored Value/Gift Card Purchase/Load

Refer to the *Codes Reference Guide* for more information.

2.6.1.4 Additional Requirements for Bill Payment Providers

Acquirers must require that their Bill Payment Providers:

- Submit each payment to be individually Authorized and Settled, and do not aggregate Transactions.
- Facilitate payments only to End Beneficiaries that are businesses, with the exception of rental payments.
- Disclose to the Cardmember that the Bill Payment Provider is the Merchant and is providing a financial service to the Cardmember by paying the End Beneficiary on the Cardmember's behalf.
- Facilitate payments only to End Beneficiaries that are located in the same country as the Bill Payment Provider, except for EEA & UK Bill Payment Providers which may facilitate payments to End Beneficiaries that are located in other EEA & UK countries.
- When facilitating payments on behalf of consumers, only pay End Beneficiaries that are in the industries listed in Table 2-10, "Allowed Industries for Bill Payment Providers Facilitating Consumer Payments," on page 77.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- When facilitating payments on behalf of businesses, must not pay End Beneficiaries that are in the following industries:
  - Airline/Charter/Air Carrier
  - Car Rental Agencies
  - Lodging (Hotels, Motels, Resorts, Central Reservations)
  - Cruise lines (including on-board shops)

Table 2-10. Allowed Industries for Bill Payment Providers Facilitating Consumer Payments

Code	Description
4814	Telecommunications Services, including Local and Long Distance Calls, Credit Card Calls, Calls Through Use of Magnetic-Stripe-Reading Telephones, and Fax Services
4899	Cable and Other Pay Television Services
4900	Utilities - Electric, Gas, Water, and Sanitary
6300	Insurance Sales, Underwriting, and Premiums
6513	Real Estate Agents and Managers - Rentals
7523	Parking Lots and Garages
7911	Dance Halls, Studios, and Schools
7997	Membership Clubs (Sports, Recreation, Athletic), Country Clubs, and Private Golf Courses
8011	Doctors and Physicians - Not Elsewhere Classified
8062	Hospitals
8099	Medical Services and Health Practitioners - Not Elsewhere Classified
8211	Elementary and Secondary Schools
8220	Colleges, Secondary Schools, Universities, Professional Schools, and Junior Colleges
8241	Correspondence Schools
8244	Business and Secretarial Schools
8249	Trade and Vocational Schools
8299	Schools and Educational Services - Not Elsewhere Classified
8351	Child Care Services
9211	Court Costs, including Alimony and Child Support
9222	Fitness
9311	Tax Payments
9399	Government Services - Not Elsewhere Classified

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.6.1.5 Additional Requirements for Installment Payment Providers

Acquirers must require their Installment Payment Providers:

- Do not charge the Cardmember interest, or any other non-discretionary fees, other than late payment fees.
- Disclose material terms of the installment agreement to the Cardmember including, but not limited to, the amount, frequency of the installment, and any late payment fees.
- Provide details to Cardmembers via mobile application or website about each installment Transaction, including:
  - Description of each individual purchase, including the name of the End Beneficiary
  - Date and value of each individual purchase
  - Date and value of each installment charge for that individual purchase
  - Number of installments paid and number of installments remaining in the series (e.g., "1 of 4")
- Submit an Authorization Request for each individual installment at the time the installment is due, for the value of the installment and not the full purchase amount.
- Do not charge related future installments if a purchase is disputed, and only resume installments if the dispute is resolved in the Acquirer's favor.
- Facilitate payments only to End Beneficiaries that are located in the same country as the Installment Payment Provider, except for EEA & UK Installment Payment Providers which may facilitate payments to End Beneficiaries that are located in other EEA & UK countries.

Note: Installments charged by Installment Payment Providers are not considered Recurring Billing Transactions.

2.6.1.6 Additional Requirements for Marketplaces

Acquirers must require their Marketplaces:

- Have legally binding terms with the End Beneficiary.
- Provide details to Cardmembers about each Transaction, including:
  - Description of each individual purchase, including the name of the End Beneficiary
  - Date and value of each individual purchase

2.7 Service Provider

The Service Provider policy is designed to mitigate operational risk and ensure Service Providers performing the services defined in Section 2.7.1.1, "Service Provider Categories and Service Types," on page 79 and conducting business with Participants are PCI DSS compliant.

If a Participant uses a Service Provider to provide any of the service types listed in Section 2.7.1.1, "Service Provider Categories and Service Types," on page 79, the Participant may be required to:

- Attest to the services provided by the Service Provider, and
- Confirm directly to AEGNS each such Service Provider's compliance to the PCI DSS as detailed in Section 2.4, "Participant Data Security Policy," on page 38.

Participants must not engage the services of Service Providers providing the services listed in Section 2.7.1.1, "Service Provider Categories and Service Types," on page 79 unless the Participant has confirmed to AEGNS that such Service Providers are PCI DSS compliant.

AEGNS is not responsible for the acts or omissions of any Service Provider, nor for any delay or failure to enforce the rules outlined herein.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.7.1 General Requirements

This section summarizes the general policy requirements that Participants must meet for each Service Provider whose services they have engaged:

- Perform due diligence to ensure that any such Service Provider is financially responsible, is capable of performing the services as described, and has not had any serious derogatory reports lodged against it.
- Obtain a document evidencing the Service Provider's status as PCI-compliant.
- Have a written contract with each of its Service Providers which binds them to observe the AEGNS DSP or its equivalent.
- Maintain a file on each Service Provider, which includes information on the due diligence performed before engagement and on an ongoing basis.
- Provide AEGNS, upon request, any Documentation related to the services provided by the Service Provider.
- Upon request, provide AEGNS the list and contact details of all Service Providers that provide services in the processing, storage, transmission, and/or switching of Cardholder Data and/or Sensitive Authentication Data, and classify such Service Providers as Level 1, Level 2, Level 3, or Level 4 as defined in Table 2-4, "S/E and Service Provider Compliance Validation Requirements," on page 42.
- Ensure Service Providers engaged in the service categories and service types listed in Section 2.7.1.1, "Service Provider Categories and Service Types," on page 79, are PCI DSS compliant for each unique service category and service type.
- Require and monitor that the Service Provider meets and complies with the requirements of the DSP as detailed in Section 2.4, "Participant Data Security Policy," on page 38.
- Participants must monitor on an ongoing basis that the Service Provider performs only the type of services it is contracted to perform.

2.7.1.1 Service Provider Categories and Service Types

The categories of Service Providers outlined below are examples of entities that store, process, or transmit Cardholder Data and/or Sensitive Authentication Data.

1. Service Providers performing payment processing-related services including, but not limited to:
   a. Authorizations
   b. Clearing and Settlement
   c. Payment gateways
   d. Payment switching
   e. Payment Facilitators (only applicable to Payment Facilitators that meet requirements of a Service Provider)
   f. TSPs
2. Service Providers performing data preparation-related services including, but not limited to:
   a. Billing/statementing
   b. Billing disputes management

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3. Service Providers performing fraud prevention and control-related services including, but not limited to:
    a. Risk analysis
    b. Fraud screening
    c. Fraud prevention
4. Any other Service Provider that is involved in the processing, storage, transmission, and/or switching of Account Data, Authorization Data. Transaction Data, Cardholder Data, and/or Sensitive Authentication Data, such as Authorized Processors, third-party processors, vendors, Mobile Entities (or their agents, representatives, or subcontractors).

Participants are solely responsible for performing the necessary due diligence to ensure that their Service Providers have the necessary qualifications and credentials to be included in the indicated service category.

AEGNS reserves the right to update the categories and service types listed in this section at its discretion.

2.7.1.2 Non-Compliance

If a Participant fails to comply with any requirements detailed in this policy, including the compliance validation requirements with the AEGNS DSP as detailed in Section 2.4, "Participant Data Security Policy," on page 38, the Participant may be subject to non-compliance fees as outlined in Section 10.7.1, "General Non-Compliance Fees," on page 411.

AEGNS reserves the right, at its sole discretion, to request from Participants information validating any of the compliance requirements stated in this policy. This information may be required to be submitted via a secure Web portal, secure fax, or email.

Participants are solely responsible for monitoring the PCI DSS compliance status of Service Providers whose services they have engaged.

2.8 Authorized Processors

In the case of Issuers, Authorized Processors may provide services that include, but are not limited to:

- Solicitation of Card applications
- Processing of Card applications
- Approval of Cardmembers
- Customer service activities
- Credit assessment of Cardmembers
- Billing and collection activities
- Implementation of additional benefits
- Statementing services

Issuers must not delegate to any Authorized Processor, directly or indirectly, the issuance of Cards or the ownership or management of Card receivables.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

In the case of Acquirers, Authorized Processors may provide services that include, but are not limited to:

- Authorization
- Clearing and Settlement
- S/E statementing
- Chargeback processing

Acquirers must not delegate to any Authorized Processors, directly or indirectly, any services that would permit an Authorized Processor to be a party to an S/E contract, or determine S/E discount rates.

2.8.1 Use of Authorized Processors

Participants may outsource to Authorized Processors any processing functions associated with their Card Issuing business or Acquiring business, with the prior written consent of AEGNS. Acquirers and Issuers wishing to use an Authorized Processor shall submit a proposal to AEGNS identifying their intended use of an Authorized Processor and detailing the specific functions to be performed. If AEGNS approves the use of the Authorized Processor, Participants shall be responsible and liable to AEGNS for the performance and all acts and omissions of such Authorized Processor. A Participant using Authorized Processors shall ensure that its contractual arrangements with such Authorized Processors contain adequate provisions to ensure that Authorized Processors:

- Perform in accordance with the terms and conditions of AEGNS Certification, the Participant Agreement, and all applicable law (including, but not limited to, data protection laws) at all times, and
- Implement security measures to prevent misuse of or unauthorized access to any American Express information (as defined in the Participant Agreement), Cardholder or S/E Data or lists, or other Cardmember or S/E Information, and
- Maintain an effective Anti-Money Laundering and Anti-Terrorist Financing program, to prevent the use of their operations for criminal purposes, and
- Comply with the Data Security Policy as outlined in Section 2.4, "Participant Data Security Policy," on page 38, and
- Execute documents as requested by AEGNS in connection with Certification, and
- Allow for AEGNS Audits as outlined in Section 2.2.17, "Audit Rights," on page 26, and
- Maintain the confidentiality of all American Express confidential information as outlined in Section 2.8.2, "Processor's Confidentiality Obligations," on page 82 below.

Authorized Processors must be certified by AEGNS as capable of providing services to each Issuer or Acquirer in accordance with Network requirements. Participants are fully responsible for any and all acts and omissions on the part of an Authorized Processor. Participants are responsible for ensuring that their Authorized Processor is on the current release of the AEGN. The Authorized Processor is responsible for data transfer to and from the Participant.

Participants are responsible for notifying AEGNS of the termination of their relationship with an Authorized Processor. Participants are responsible for making alternative arrangements, if necessary, to ensure compliance with the Participant Agreement and all AEGNS requirements.

All fees and costs incurred by a Participant and/or an Authorized Processor to perform Participant activities and to attain Certification from AEGNS are the sole responsibility and liability of the Participant.

AEGNS may provide a Participant a list of previously certified Authorized Processors. Inclusion of an Authorized Processor on such a list, or Certification of an Authorized Processor by an American Express Entity or AEGNS does not constitute a guaranty or warranty by any American Express Entity of the performance of any Authorized Processor and does not relieve the Participant of its responsibility and liability for any Authorized Processors the Participant elects to use. AEGNS and American Express Entities have no liability or responsibility for Authorized Processors. Participants are solely and fully responsible and liable for

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

the performance of all Authorized Processors which they use and bear all risks with respect to such Authorized Processors' performance, and are responsible for verifying that such Authorized Processors' performance continues to comply with all Network requirements and applicable law.

Any failure to perform by an Authorized Processor used by a Participant shall not relieve that Participant of its obligations under its Participant Agreement or its obligation to comply with AEGN requirements.

2.8.2 Processor's Confidentiality Obligations

Participants may provide Authorized Processors with access to confidential information of American Express Entities relating to the Network (including Network Specifications manuals, *Codes Reference Guide, Business and Operational Policies* manual, and *Network Participant Updates*) only to the extent that Authorized Processors need such access in order to provide services to Participants in accordance with their Participant Agreements and AEGNS manuals. Authorized Processors shall limit access to such Confidential Information to their employees who have a "need to know" for the purpose of performing such services for a Participant. Authorized Processors shall use such Confidential Information for the sole purpose of performing such services and are prohibited from disclosing or permitting the disclosure of such Confidential Information to any third party.

Authorized Processors are required to establish firewalls to maintain the confidentiality and separation of each Participant's confidential information. If an Authorized Processor performs processing or other services for any cards/merchants other than Cards/Merchants issued or acquired on the AEGN, the Authorized Processor shall ensure that:

- It does not use any trade secrets or Confidential Information of any American Express Entity or relating to the Network in performance of services for such other cards, or in any other activities; and,
- It does not use Confidential Information or trade secrets of any other card network in performing services for a Participant with respect to its business
- It does not disclose the information of one (1) Issuer on the American Express Network to another Issuer

If a Participant terminates its relationship with an Authorized Processor, it shall require the Authorized Processor to promptly return to the Participant all information relating to American Express Entities and/or AEGNS.

2.8.3 Compliance

Participants are responsible for ensuring that Authorized Processors comply with the foregoing requirements and are liable for any breach by Authorized Processors.

In the event of a breach by an Authorized Processor of this section, American Express Entities shall be entitled, in addition to any other rights and remedies and money damages that may be available, to specific performance and injunctive relief and any other appropriate equitable remedies for any such breach without proof of actual injury. Participants must ensure their agreements with Authorized Processors include a provision that the Authorized Processor must report all instances of a Data Compromise immediately to the Participant, and in no case later than seventy-two (72) hours after discovery of the incident. Participants must notify the Network immediately, and in no case later than seventy-two (72) hours, after discovery of a Data Compromise at an Authorized Processor. See Section 2.4.9, "Requirements for Notification of Data Compromise," on page 47 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9 Requirements for Conducting Merchant Acquiring Business

This section provides policies and rules specific to Acquirers.

Each Acquirer is required to (i) purchase all Charges made by Cardmembers on any Card and submitted to such Acquirer by its S/Es (ii) pay for the same in accordance with the schedule of payments set forth in its S/E agreements with such S/Es. Charges incurred by Cardmembers, must be submitted to Clearing Centers at the times and in the formats designated by AEGNS. Acquirers shall allow Charges to be submitted by S/Es, and shall pay for Charges submitted by such S/Es, only in the Authorized Currency.

Each Acquirer must be a party to all of its S/E agreements. The authority to act as an Acquirer and be the named contractual party on the relevant agreement cannot be transferred, outsourced or delegated.

Acquirers must ensure that all agreements, disclosures, communications, and solicitations comply with applicable laws and regulations and this AEGNS manual, including, without limitation, Section 2.9.3.3, "Compliant S/E Agreement Design," on page 87.

Subject to this AEGNS manual and the Issuer's and Acquirer's rights to be reimbursed pursuant to the Chargeback policy, each Acquirer alone bears all financial risk (for example, fraud risk) arising from or associated with its Merchant Acquiring Business.

Acquirers shall provide each of their S/Es with adequate operating materials and equipment (including the means to obtain Authorizations for Charges in the most expeditious manner), instructions on the procedures for honoring Cards and processing record of charge forms, and details as to the Acquirer's different payment options. Acquirers shall ensure that all S/Es display at least one (1) decal denoting acceptance of American Express® Cards on parity terms with all other general purpose card networks.

In carrying out its S/E acquisition and servicing duties, an Acquirer may require an S/E to own a bank account in the Territory but shall not require existing or prospective S/Es to establish a banking relationship with such Acquirer or any other specific banking institution, or to service S/Es that have not established such a banking relationship differently in any way from those that have.

Acquirers must follow the neutrality principles listed in "Exhibit 19. Neutrality Principles for Conducting Merchant Acquiring Business" on page 489with regard to the manner in which S/E offers, promotions and network capabilities will be made available to Issuers and their Cardmembers.

2.9.1 Acquirer-Related Certification

Prior to engaging in the Merchant Acquiring Business, Acquirers must complete the Certification process described in Section 2.2.6, "Network Infrastructure Access and Certification," on page 14 and Section 2.9.1, "Acquirer-Related Certification," on page 83. AEGNS will provide each Acquirer with the support described in Section 2.2.7.1, "AEGNS Assistance Prior to Launch," on page 14 prior to the enablement of an Acquirer's first S/E on the Network.

Acquirers shall strive toward achieving online electronic authorization and capture of Charges on as widespread a basis as possible.

In order to conduct business on the AEGN, Acquirers must specifically comply with, and certify compliance with the following requirements:

- Send and receive AEGNS-compliant Authorization messages and transmit Issuers' decisions (approve/deny/refer) to their S/Es' POS terminals.
- Receive and submit AEGNS-compliant Clearing and Settlement files, handle Network record types correctly, outclear First Presentments, Second Presentments and request fulfillments, inclear Retrieval Requests, First and Final Chargebacks, as well as acknowledging receipt of incleared files.
- Submit AEGNS-compliant data collection files, as defined in Section 2.9.2.2, "Acquirer File Submission Requirements," on page 85 and in the Network Specifications manuals.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- AEGNS' policies related to Anti-Money Laundering (AML), Anti-Terrorist Financing, and Customer Screening Programs. Refer to Section 2.10.4, "Use of Cardmember Information," on page 113 for details.
- Acquirers of S/Es in industries listed in Table 2-11, "Restricted Industries Requirements," on page 95 are required to complete a Brand Protection Assessment (refer to Section 2.9.5, "Brand Protection," on page 97 for related requirements).

When considering making an operational or systems change to its Merchant Acquiring Business, an Acquirer must contact its AEGNS representative to ensure compliance with AEGNS policy. Acquirers shall bear the cost of Certification of their Merchant Acquiring Business (including, without limitation, their Authorized Processors) as determined by AEGNS. Regardless of whether Certification is conducted by AEGNS or its designee, Acquirers shall be fully liable for their failure to perform, or the failure of any of their agents and processors (including without limitation, Authorized Processors and their agents).

2.9.1.1 POS Certification Requirements

In order to conduct business on the Network and ensure payment Transaction interoperability, AEGNS requires that new or replaced Chip Card-enabled POS devices, attachments, and peripherals must successfully complete an end-to-end Certification and be approved prior to deployment. For more information on the end-to-end POS device Certification process, see the *POS Device Certification Process Guide* available on Knowledge Base. Use the Search function to find this document.

AEGNS also requires end-to-end Mobile POS (mPOS) Certification for mPOS devices prior to deployment.

Prior to obtaining AEGNS end-to-end Certification, devices must meet the following requirements:

- Have a valid EMVCo approval for contact and Contactless devices (excludes software-based mPOS).
- Comply with the PCI POS device-related requirements listed in Section 2.4.3, "Acquirer Data Security Compliance Validation Requirements," on page 41.
- Meet the requirements detailed in Section 2.9.17.4, "Expresspay-Enabled POS Devices," on page 105, if applicable. POS devices must also be capable of processing AEIPS and/or Expresspay-compliant Chip Card Transactions.

Acquirers, in designated countries, are required to certify their Chip and PIN-enabled POS devices to support Online PIN. Refer to Section 4.2.20.8, "POS Online PIN Certification and Enablement Program," on page 234 for details.

A POS device includes, but is not limited to:

- Stand-alone contact and Contactless devices
- mPOS
- Software payment applications

Devices without end-to-end Certification and approval which are causing Transaction disruptions will be required to undergo the Certification and approval process as stated above.

Participants who do not comply with the Certification and approval requirements of this section will be responsible for all costs and liabilities incurred by AEGNS. AEGNS reserves the right, at its sole discretion, to request from Participants information validating any of the requirements stated in this policy. Non-compliant Participants may be subject to fees as stated in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

For more information on POS device Certifications and approvals, contact your AEGNS representative.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.2 Reporting to AEGNS

2.9.2.1 Annual Plan Disclosure

To anticipate future load capacity, effectively administer the Network, and ensure protection of the American Express Brand, AEGNS must be made aware of Acquirer plans that could affect the performance of the AEGN.

Acquirers, at their sole expense, shall have the responsibility for preparing a yearly plan for their S/E Acquiring business and shall submit such plan for AEGNS' review by the first of August of the preceding year. AEGNS shall be allowed to review such plan in advance for purposes of assessing what effect the implementation of such a plan will have on the AEGN and for ensuring that all advertising and marketing aspects of the plan are consistent with guidelines for the protection of the American Express Brand. The plan, after review by AEGNS, will be effective for the immediately succeeding calendar year.

AEGNS must be informed immediately of any revision or re-forecast of such plan which may occur during the plan year.

2.9.2.2 Acquirer File Submission Requirements

AEGNS requires that Acquirers submit the following files to the Network. The submission frequency for each message is defined below. Refer to the Network Specifications manuals for more information regarding these messages.

2.9.2.2.1 S/E Demographics Detail Data (9640) Message Submission Requirements

All Acquirers are required to submit the S/E Demographics data via the S/E Demographics (9640) message at the time there are changes to their S/E portfolio. Changes to S/E demographics are defined as:

- New S/Es added
- Cancelled S/Es
- Changes to existing S/E information (e.g., address, changes to High Risk Indicators, and status)
- New, Cancelled, and Changes to Multinational Accounts (MNAs) as defined in Section 2.9.3.3.1, "Multinational Accounts (MNAs)," on page 88

If there are no changes to S/E demographic data within a given month, the Acquirer must send a Data Collection File Header (9844) and a Data Collection File Trailer (9845) by the 5th day of the following month. This action will indicate to the Network that no changes to an Acquirer's S/E portfolio have taken place.

2.9.2.2.2 On-Us POS and ATM (1340) Message Submission Requirements

All Participants who process On-Us Transactions must submit a daily On-Us (1340) file to the Network that includes all American Express Transactions processed outside of the Network. These Transactions include all POS and ATM First and Second Presentments and First and Final Chargebacks.

For purposes of this reporting requirement, a Transaction that takes place by Cardmembers of a Participant that is both an Issuer and an Acquirer at a Multinational Account (MNA) in the Territory will be considered an "On-Us" Transaction, which the Acquirer will be required to include in its daily On-Us (1340) file under this Section 2.9.2.2.2.

2.9.2.3 Acquirer Data Collection File Submission Requirements

Participants must provide AEGNS with an attestation of accuracy for data collection files on an annual basis. The attestation will also request Acquirers to confirm that:

1. The speed of pay has been accurately applied to MNA accounts in a timely manner; and
2. Additional fees are not charged to MNAs other than the ones communicated by American Express in reference to Section 2.9.3.3.1, "Multinational Accounts (MNAs)," on page 88.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Acquirers will be required to complete and submit to AEGNS an attestation of accuracy for the data in data collection files provided to the Network and for the MNA account terms applied during the prior year. The attestation submission period for a given Participant will be determined by AEGNS and communicated to the Participant together with instructions for completing the attestation.

The attestation must be executed by an individual (such as Vice President for Finance, or another designee authorized by the Chief Financial Officer or Chief Executive Officer of the Participant and acceptable to AEGNS) with the authority to speak for and bind the Participant to the requirements set forth in this section.

Acquirers must ensure the data submitted in their data collection files and terms applied to the MNA accounts are accurate and complete.

Acquirers that do not comply with this attestation requirement, or fail to submit accurate data or apply AEGNS communicated terms to MNA accounts, respectively, may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.9.3 S/E Qualifications and Agreement Requirements

For all S/Es, the Acquirer must follow the application elements, risk evaluation, and agreement design described below.

2.9.3.1 S/E Application Elements

Acquirer's S/E application must include the following data that shall be made available to AEGNS upon request:

- S/E corporate name
- S/E name (DBA name)
- Address of business
- Tax ID number(s) (where available)
- Incorporation status
- Merchant Category Code (MCC)

2.9.3.2 S/E Acquisition Verification Process

An Acquirer shall perform the following minimum risk investigation and evaluation process on all new S/Es to ensure all S/Es meet minimum standards:

- Verify that the S/E is in the type of business it claims to be conducting and is financially sound.
- Perform screening of the S/E in accordance with Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30.
- Ensure that the S/E is domiciled in the country in which it is being affiliated.
- Conduct a physical site visit or phone/address/name match that confirms that the S/E has a valid business establishment.
- Determine if the S/E, regardless of industry, conducts business using a website.
- Record the S/E's URL (Uniform Resource Locator, i.e., website address (www.address.com)).
- Collect advertising copy and, wherever possible, obtain sample merchandise from S/Es conducting mail, telephone, or Internet Transactions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.3.3 Compliant S/E Agreement Design

Although an Acquirer may design its own S/E agreement in compliance with applicable law, basic terms to be included in an AEGN-compliant agreement except as otherwise required by applicable law are listed below:

- Every S/E must honor all Cards equally with all other cards the S/E accepts.
- S/E must not state or publish or otherwise indicate preference for other cards over the Card.
- S/E must represent and warrant that its policy is not to prefer any other card over the Card.
- S/E must not impose additional conditions or restrictions on use of Cards that are not imposed on other cards the S/E accepts.
- S/E may not establish minimum or maximum Transaction amounts as a condition for accepting Cards that do not apply equally to other card payment networks.
- An S/E may allow discount pricing for cash purchases.
- S/E may not require Cardmembers to provide personal information such as telephone number or address as a condition for accepting the Card, except as required for Card Not Present Charges. See Section 4.2.10, "Card Not Present Charges," on page 221 for more information. An S/E may only request identification from the Cardmember when:
  - An Issuer requests validation of ID during the Authorization process, or
  - If the back of the Card is not signed.
- S/E may not require Cardmembers to provide a photocopy of the Card.
- Every S/E must include all taxes required by local law that apply to purchases with the Card. These required taxes must be included in the Transaction amount.
- The Acquirer must hold any reserve Account in the name of the S/E.
- Acquirers may not submit Transactions for processing from S/Es that have been cancelled for derogatory reasons.
- Acquirers must not allow S/Es to submit Transactions that were conducted in prohibited industries. Refer to Section 2.9.4.1, "Prohibited Industries," on page 94 for additional information.
- Unless specifically authorized as a Cash Disbursement Provider, no S/E may provide cash upon presentment of the Card.
- S/E may not create a Transaction for a Cardmember who is attempting to refinance a bad check or a past due amount.
- S/Es must not submit Transactions on behalf of other S/Es.
- Acquirers must include requirements in the S/E agreement that will enable the Acquirer to comply with the "Chargeback Policies" chapter beginning on page 280.
- Acquirers must provide its standard S/E agreement to AEGNS for review for consistency with these requirements and the American Express Brand.
- Acquirers have sole responsibility for setting pricing for S/Es (with the exception of MNAs).
- S/Es are required to obtain a valid Authorization, prior to submission for payment, on all Transactions in excess of the Network Floor Limit.
- An S/E must not split a Transaction with the intent of avoiding a single Authorization for the full amount of the purchase.
- Acquirers must ensure that their S/E agreements include a requirement that the S/E must comply with the current PCI Data Security Standard.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Acquirers must ensure that their S/E agreements include a provision that the S/E must report all instances of a Data Compromise immediately to the Acquirer, and in no case later than seventy-two (72) hours after discovery of the incident.
- Acquirers must ensure that their S/E agreements include a provision which would allow the agreement to be assigned to an American Express Entity or its designee.
- Acquirers must ensure that their S/E agreements include a provision that authorizes data from transactions at such S/Es to be shared with American Express Entities.
- S/Es must not engage in activities or practices that are deceptive or misleading or that could reflect unfavorably upon the good name, goodwill, reputation, or image of American Express or any American Express Entity, or that in any way are contrary to applicable law.
- If an Acquirer introduces changes to its S/E agreement, it shall notify impacted S/Es of such modifications, clearly and transparently, with reasonable anticipation, and in accordance with applicable law and good industry practice.
- If AEGNS has reasonable grounds to believe that an S/E is engaged in fraudulent, unlawful, or similarly objectionable activity that could create legal or financial risk to the Network or reflect unfavorably on the American Express Brand, AEGNS may require the Acquirer to cancel its agreement with that S/E.
- S/E agreements used by Acquirers must contain provisions addressing choice of law and jurisdiction in case of dispute.

2.9.3.3.1 Multinational Accounts (MNAs)

MNAs require coordinated servicing and relationship management on a global or regional basis. As such, local Acquirers are responsible for providing full servicing of MNAs in their Territories on behalf of American Express Entities and shall follow all instructions from AEGNS in respect to MNAs. Discount rates, speed of pay, and other terms applicable to MNAs are negotiated by American Express, and updates must be made across all MNA locations, including those located in each Acquirer's Territory. AEGNS will notify local Acquirers of any such updates, and local Acquirers are required to action these notifications within ten (10) days of receipt. Local Acquirers are required to provide information relating to MNAs as requested by AEGNS, including requirements defined in Section 2.9.2.2, "Acquirer File Submission Requirements," on page 85.

The servicing of MNAs for which local Acquirers are responsible in their Territories includes, but is not limited to:

- Requesting and receiving authorizations for Charges on any Cards at such MNAs
- Submitting the Charges for First Presentment
- Paying for Charges in accordance with the contracts between the applicable MNA and American Express
- Receiving and managing Transaction data on such Charges
- Managing disputes and processing Chargebacks
- Monitoring, researching, and reporting of suspicious activity, as described in Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30
- Monitoring for activity indicative of fraud and taking appropriate action, as described in Section 8.9.3, "S/E Risk Management," on page 388
- Implementing account opening procedures, including Know Your Customer (KYC) and sanctions screening procedures, as described in Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30 or as otherwise directed by AEGNS

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

In consideration of their servicing of MNAs, local Acquirers shall receive the Merchant Discount for Charges on Cards at MNAs in their markets (subject to AEGNS' entitlement to be paid a portion of the Merchant Discount, as applicable, pursuant to the Participant Agreement between the local Acquirer and AEGNS). Accordingly, local Acquirers bear responsibility (and must provision) for any obligations on such Charges that arise under the Clearing, Settlement, and Funds Exchange processes set out in the "Clearing and Settlement" chapter beginning on page 269 and under the Chargeback policies set out in the "Chargeback Policies" chapter beginning on page 280 and shall fund any obligations that may arise thereunder with respect to such Charges.

To fulfill AEGNS requirements under its Participant Agreements to designate MNAs in writing, AEGNS will update American Express' global list of MNAs and Foreign International Establishments (FIEs) and post the updated list on Knowledge Base on a biannual basis in April and October. Use the Search function to find the MNA/FIE List. The most current list posted on Knowledge Base will supersede the original MNA/FIE list attached to the Participant Agreement. Please contact your AEGNS representative if you have questions about how the updated list applies to your market or region.

Note: Participants servicing MNAs in the European Economic Area (EEA) are hereby on notice that all instructions in respect of Payment Services and related activity provided to MNAs in the EEA by AEGNS are given on behalf of American Express Payment Europe S.L.

2.9.3.4 Acquirer Eligible Marketing Region

Acquirers may sign only S/Es within the Territory specified under the Participant Agreement, which is generally the country where the Acquirer is headquartered. An S/E's country of residence is the country where the S/E is located and registered to do business. S/E acquisitions within Army Post Offices (APOs) and Fleet Post Offices (FPOs) are negotiated on an individual basis through AEGNS.

Unless separately agreed by AEGNS, an Acquirer affiliating S/Es in more than one (1) country will be assigned a separate Acquiring Institution Number (AIN) for each country in which it acquires.

Acquirers generally may not advertise in any geographic territory other than the Territory specified in the Participant Agreement.

2.9.3.5 Payment Facilitator

This section outlines the policies and rules that apply to entities (third parties or S/Es) that operate as Payment Facilitators in either the Card Present or Card Not Present payment environment. Payment Facilitators are entities that contract with an Acquirer to provide Payment Services to Sponsored Merchants, enabling them to accept the Card. These Sponsored Merchants may or may not have a direct relationship with the Acquirer.

Acquirers that contract with Payment Facilitators are liable for all acts, omissions and other adverse conditions caused by the Payment Facilitators and their respective Sponsored Merchants. In the event that a Payment Facilitator is unable to fulfill their obligations to their Sponsored Merchants, the Acquirer will be responsible for Transaction processing and Settlement with Sponsored Merchant(s). The Acquirer will hold AEGNS harmless against any claims made by a Sponsored Merchant or its representatives that it has not received accurate, complete and timely Settlement from the Payment Facilitator. As a result, the Acquirer must at all times be responsible for and manage, direct, and control all aspects of its Payment Facilitator activities and enforce all program management and operating policies applicable to Payment Facilitators and Sponsored Merchants in accordance with Section 2.9.3.5 and other sections referenced in the *Business and Operational Policies* manual. AEGNS or its designee reserves the right to conduct audits of an Acquirer, its Payment Facilitators, and the Payment Facilitator's Sponsored Merchants at any time for the purpose of determining compliance with these Payment Facilitator rules and other applicable policies provided in the *Business and Operational Policies* manual.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.3.5.1 Payment Facilitator Qualifications

An Acquirer must execute a Payment Facilitator Agreement with a Payment Facilitator. This agreement must contain the requirements established in Section 2.9.3.5.4, "Payment Facilitator Agreement Requirements," on page 92. An Acquirer must ensure their Payment Facilitators adhere to all general policies and rules as provided in the *Business and Operational Policies* manual and the specific minimum requirements for Payment Facilitators described in this policy.

2.9.3.5.2 General Requirements for Acquirers, Payment Facilitators, and Sponsored Merchants

Acquirers must ensure that their Payment Facilitators and the Payment Facilitators' respective Sponsored Merchants comply with AEGNS requirements that include, but are not limited to the following:

- Payment Facilitators have been assessed and, based on the Acquirer's assessment, have adequate resources, financial and otherwise, to meet their obligations and deliver the services in accordance with applicable law and AEGNS' *Business and Operational Policies* and Network Specifications manuals prior to entering into a Payment Facilitator Agreement. Furthermore, Acquirers are required to conduct annual reviews of their Payment Facilitators to ensure compliance with the *Business and Operational Policies* and Network Specifications manuals.
- Payment Facilitators must enter into a Sponsored Merchant Agreement with each Sponsored Merchant. Payment Facilitators must enforce each Sponsored Merchant's compliance with the provisions of the Sponsored Merchant Agreement as outlined in Section 2.9.3.5.5, "Sponsored Merchant Agreement Requirements," on page 92, including the termination of Payment Services provided to Sponsored Merchants if they fail to comply with any of these provisions.
- Payment Facilitators must meet the anti-money laundering (AML) and anti-terrorist financing (ATF) program requirements established in Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30. Acquirers must also be prepared to provide copies of these documents to AEGNS within thirty (30) days, or as otherwise specified, of request from AEGNS.
- Payment Facilitators and their respective Sponsored Merchants must comply with the AEGNS Data Security Policy as set forth in Section 2.4, "Participant Data Security Policy," on page 38.
- Payment Facilitators and their Sponsored Merchants must at all times operate their business in a safe and sound manner and in compliance with applicable law, and must not directly or indirectly engage in or facilitate any action that does not comply with local laws or regulations.
- Payment Facilitators and their Sponsored Merchants must have all licenses and legal and regulatory permissions necessary to conduct business.
- Payment Facilitators and their Sponsored Merchants must not engage in illegal or potentially deceptive marketing practices or otherwise process Transactions that may adversely affect the American Express Brand, and otherwise must adhere to AEGNS' Brand Protection policy as provided in Section 2.9.5, "Brand Protection," on page 97.
- Payment Facilitators and their Sponsored Merchants must adhere to the policies for review and approval for Marketing and Branding requirements established in Section 2.9.19, "Marketing, Advertising, and Public Relations," on page 108.
- Acquirers must accept and process Transactions only from Payment Facilitators and Sponsored Merchants within the geographic territory or eligible marketing region specified under their Participant Agreement.
- Payment Facilitators must not contract with another Payment Facilitator as a Sponsored Merchant, nor allow Payment Facilitators to operate under another Payment Facilitator as a Sponsored Merchant.
- Payment Facilitators may contract with Marketplaces as a Sponsored Merchant.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Payment Facilitators and their Sponsored Merchants must comply with the requirements in Section 2.9.7, "S/E Website Information Display Guidelines," on page 101 and ensure, on an ongoing basis, that such websites do not contain any content or material that may cause harm to any individuals or damage to the American Express Brand.
- Neither the Payment Facilitators nor any of their respective Sponsored Merchants are in Prohibited Industries (as detailed in Section 2.9.4.1, "Prohibited Industries," on page 94) and/or engaging in American Express related business with any country on which the United States has imposed economic sanctions (as detailed in Section 2.3.6.1, "Prohibited Countries and Regions," on page 36).
- Payment Facilitators and Sponsored Merchants must ensure Transactions submitted to AEGNS comply with the Network Specifications manuals.
- Acquirers must monitor the activities of their Payment Facilitators and Sponsored Merchants to deter fraud and other wrongful activity, and to ensure that they are in full compliance with all other requirements as outlined in Section 2.9, "Requirements for Conducting Merchant Acquiring Business," on page 83 and provided in Section 2.9.3.5, "Payment Facilitator," on page 89.
- Acquirers must ensure that their Payment Facilitators and respective Sponsored Merchants operate in accordance with obligations and requirements provided in Section 8.10, "AEGNS Issuer and Cardmember Risk Management," on page 391.

Additionally, upon request of AEGNS, the Acquirer must provide an Attestation of Compliance with the general requirements as set out in this section.

2.9.3.5.3 Reporting Requirements for Payment Facilitators

AEGNS may request information about Payment Facilitators, which may include the data elements listed below:

- Acquirer ID Number
- Payment Facilitator Start Date
- Payment Facilitator Termination Date (when applicable)
- Payment Facilitator Status: new/renew/termination
- Payment Facilitator Doing Business As (DBA) name
- Payment Facilitator Legal Name
- Payment Facilitator Business function
- Payment Facilitator S/E#
- Payment Facilitator Contact information:
  - Legal address
  - Principal owner name
  - Business phone
  - Business address
  - Business URL

This list of data elements is not exhaustive. AEGNS may, in its sole discretion, request other data elements.

Acquirers must submit the information to AEGNS no later than thirty (30) days after such request, or as otherwise specified.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.3.5.4 Payment Facilitator Agreement Requirements

Although an Acquirer may design its own Payment Facilitator Agreement, this agreement must contain the principles and substance provided in the "Business Policies and Rules" chapter beginning on page 11, including, but not limited to, statements specifying:

- The Acquirer's right to immediately terminate a Payment Facilitator or Sponsored Merchant contract for good cause or fraudulent or other activity, or upon AEGNS request.
- Payment Facilitators are liable for all Settlement activity on behalf of their Sponsored Merchants, including Chargebacks and Credits. Payment Facilitators are also liable for all other acts, omissions, and Cardmember customer service-related issues caused by the Payment Facilitators' Sponsored Merchants.
- Payment Facilitators must perform due diligence and "Know Your Customer (KYC)" screening for each of its Sponsored Merchants, which must include a financial review and background check of their principal or controlling owner.
- Payment Facilitators must retain any records concerning the investigation of its Sponsored Merchants, and provide such records to the Acquirer and/or AEGN within thirty (30) days, or otherwise specified, of request from AEGN.
- Payment Facilitators must provide the names of owner(s) for each of their Sponsored Merchants on the Network through the Sponsored Merchant Reporting as outlined in Section 2.9.3.5.6, "Sponsored Merchant Reporting Requirements," on page 93.
- Payment Facilitators must ensure that their Sponsored Merchants comply with the AEGNS Data Security Policy as set forth in Section 2.4, "Participant Data Security Policy," on page 38.
- Payment Facilitators must remove American Express Licensed Marks from their website and wherever else they are displayed upon termination of the Payment Facilitator Agreement.

2.9.3.5.5 Sponsored Merchant Agreement Requirements

Although Payment Facilitators may design their own Sponsored Merchant Agreement, each Payment Facilitator must enter into a written agreement with each Sponsored Merchant, and such agreements must contain the principles and substance provided in Section 2.9.3, "S/E Qualifications and Agreement Requirements," on page 86. In addition, the agreement should include the following specific provisions:

Sponsored Merchants are required to comply with all applicable laws, rules and regulations relating to the conduct of the Sponsored Merchant's business.

A requirement that Payment Facilitators have the right to immediately terminate a Sponsored Merchant for good cause, or fraudulent or other activity, or upon request of the Acquirer or AEGNS.

The Sponsored Merchant must adhere to AEGN Card Acceptance and Authorization policies and procedures.

A provision to ensure Transactions submitted to AEGNS comply with the Network Specifications manuals.

Sponsored Merchants are responsible for being aware of and adhering to privacy and data protection laws and provide specific and adequate disclosures to Cardmembers of collection, use and processing of personal data.

Sponsored Merchants must comply with the AEGNS Data Security Policy provided in Section 2.4, "Participant Data Security Policy," on page 38.

A requirement to remove American Express Licensed Marks from the Sponsored Merchant website and any other locations under the control of the Sponsored Merchant, no later than thirty (30) days of termination of the Sponsored Merchant Agreement.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.3.5.6 Sponsored Merchant Reporting Requirements

AEGNS may request information about Sponsored Merchants operating through a Payment Facilitator registered on the Network. Such requests may include the data elements listed below:

- Payment Facilitator S/E Number
- Date Signed
- Date Terminated
- Status: New/Change/Cancelled
- Seller ID: An Acquirer assigned unique identifier of a Sponsored Merchant, e.g., up to twenty (20) byte combination of letters and/or numbers that uniquely identifies a Sponsored Merchant
- Sponsored Merchant Legal Name
- Doing Business As (DBA) name
- Street Address
- City
- State/Region
- Postal Code
- Country
- Website address (URL)
- Merchant Category Code (MCC)
- Sales count and amount
- Chargeback count and amount

This list of data elements is not exhaustive. AEGNS may, in its sole discretion, request other data elements. Acquirers must provide the data to AEGNS within thirty (30) days, or as otherwise specified, of such request. Detailed reporting and submission instructions will be included in the AEGNS request.

Acquirers must submit the information to AEGNS no later than thirty (30) days after such request, or as otherwise specified.

2.9.3.5.7 Data Elements Requirements

Transactions submitted to AEGNS by Payment Facilitators and Sponsored Merchants must contain the mandatory data elements as defined in the Network Specifications manuals. Refer to the Network Specifications manuals for more information.

2.9.3.5.8 Data Quality

Merchant Category Code (MCC), Merchant Name, and Transaction activity provide AEGN with information to support Risk Management, Compliance and Brand Protection policies.

In addition to the applicable sections in the Network Specifications manuals, Acquirers are required to:

- Ensure Payment Facilitators and Sponsored Merchants use the appropriate Merchant Category Code for each Sponsored Merchant in the Authorization Request and Presentment message, as specified in the Network Specifications manuals and *Codes Reference Guide.*
- Ensure the Sponsored Merchant characteristic and activity reporting provided to AEGNS is accurate.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.3.6 Terms Applicable to the European Union/European Economic Area and United Kingdom Only

Nothing in this Section 2.9.3, "S/E Qualifications and Agreement Requirements," shall prohibit Acquirers in the European Union/European Economic Area and United Kingdom (EU/EEA & UK) from concluding "passive" sales to an S/E within the EU/EEA & UK, subject to meeting operational requirements and agreeing commercial terms with American Express Entities (regarding which "passive" sales, for purposes of definition only, reference should be made to the guidelines in EU Regulation 330/2010).

2.9.4 Prohibited and Restricted Industry Requirements

All Acquirers on the Network must comply with the prohibited and restricted industry policy requirements detailed in this section.

2.9.4.1 Prohibited Industries

Acquirers shall not contract with businesses deemed prohibited according to the following list nor seek to alter the industry designation in order to circumvent the policies as set forth in this section. In addition, Acquirers must not allow S/Es to submit Transactions that were conducted in prohibited industries, as defined in this section.

Unless otherwise specified, all restrictions regarding prohibited industries apply to conventional businesses having physical buildings and facilities, as well as businesses operating remotely (i.e., Internet S/Es).

The following are designated as prohibited industries:

- Illegal businesses and activities according to the laws and regulations governing the S/E
- Check Cashing/Check Guarantee businesses
- Credit Restoration Services
- Multi-level marketing (including pyramid selling, excludes national and multinational Accounts)
- Prostitution (including S/Es involved in prostitution such as unlicensed massage parlors and escort services)
- Internet adult digital content
- Individuals and organizations that the U.S. government identifies as supporting terrorism and which are listed on the Internet at: www.treasury.gov/offices/enforcement/ofac/sdn/index.shtml
- Sale of Infringing Products

AEGNS monitors Network activity related to the policies detailed in this section. Acquirers that do not comply with these requirements are subject to non-compliance fees. Refer to Section 2.9.5.2, "Reporting Violations," on page 98 for details on reporting violations and applicable non-compliance fees.

AEGNS may require an Acquirer to terminate Card acceptance with an S/E that meets any of the prohibited industry criteria listed above.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.4.2 Restricted Industries

Restricted industries are those industries listed in Table 2-11, "Restricted Industries Requirements," on page 95 which are subject to additional compliance requirements.

Table 2-11. Restricted Industries Requirements

Industry Category	MCC[1]	Written Approval[2]	S/E Registration[3]	Brand Protection Assessment[4]
Digital file hosting (Cyberlockers)	N/A			✓
Telemarketing – travel-related arrangements	5962			✓
Direct marketing – outbound	5966			✓
Direct marketing – inbound	5967			✓
Direct marketing – not elsewhere classified	5969			✓
Virtual Currencies – distribution and/or cashing out[5]	N/A	✓	✓	✓
Pharmacies that intend to submit Card Not Present Transactions[6, 7]	5122 5912		✓	✓
Tobacco and smokeless tobacco retailers that intend to submit Card Not Present Transactions	5993		✓	✓
Miscellaneous and specialty retail not elsewhere classified	5999			✓
Indirect Acceptors (excluding P2P)	N/A			✓
Peer-to-Peer Payments (P2)	6538	✓	✓	✓
Government-licensed online casinos (online gambling) - U.S. S/Es only[8]	7801	✓	✓	✓
Government-licensed horse/dog racing - U.S. S/Es only[8]	7802	✓	✓	✓
Gambling - includes casino chips, gambling services, Internet gambling sites, bingo, and off-track betting and wagers at race tracks[6]	7995	✓	✓	✓
Lotteries - Card Not Present sales of lottery tickets[6]	7995	✓	✓	✓
Lotteries – onsite sales of lottery tickets at state and national government-owned authorized retailers (Card Present)[6]	7995 7800		✓	✓
Payment Facilitators	N/A			✓
Collection Agencies (receivable on Card)	7322	✓	✓	✓

1. Merchant Category Codes (MCCs) should not be used as the sole indicator of an S/E's business or industry type. While Brand Protection policies focus on the industries listed above, the policies extend to all industries, S/Es, Sponsored Merchants, and Payment Facilitators on the AEGN. The above information may be amended at any time at the discretion of AEGNS.
2. Participants wishing to acquire S/Es conducting business in these industries must obtain prior written approval from AEGNS. Participants must notify AEGNS of any changes related to information provided or condition given for any such approval. Contact your AEGNS representative for details.
3. These S/Es must be registered with AEGNS prior to transacting on the Network, and confirm registration details annually thereafter upon request from AEGNS. Refer to the *Brand Protection Guide for Acquirers*, available on Knowledge Base, for additional information and instructions related to S/E registration.
4. Acquirers are required to complete a Brand Protection Assessment if they decide to acquire S/Es in these industries. See Section 2.9.5, "Brand Protection," on page 97 for details.
5. Partner Loyalty Reward and/or Affinity Programs are excluded from this restriction.
6. Payment Facilitators that submit Transactions on behalf of an S/E engaged in a restricted industry must adhere to the requirements outlined in this table.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7. Nationally accredited online pharmacies are excluded from the S/E registration requirement, subject to approval by AEGNS. A nationally accredited online pharmacy is one that complies with the licensing and survey requirements of both the buyer's and seller's jurisdiction, as endorsed by an officially recognized national entity that is accepted as authoritative, such as VIPPS (Verified Internet Pharmacy Practice Site) in the U.S. These pharmacies must meet nationally endorsed standards of pharmacy practice, privacy, authentication, and security of prescriptions as well as strict quality assurance policies.
8. These Merchant Category Codes (MCCs) are restricted for use only with S/Es in the United States.

Card Not Present Transactions will be identified by Point of Service Data Code(s) in the POS Authorization Request (1100) and/or POS First Presentment (1240) messages. Refer to the *Brand Protection Guide for Acquirers*, available on Knowledge Base, for additional information and instructions related to S/E registration. For a detailed description of MCCs, refer to the *Codes Reference Guide* available on Knowledge Base. Use the Search function to find these documents.

2.9.4.3 General Requirements for Acquirers, Lotteries, and Gambling S/Es

Acquirers, Lotteries, and Gambling S/Es are required to adhere to the following requirements including, but not limited to:

- Legal Authority and Legal Opinion - Ensure gambling Transactions are permissible under applicable law. Acquirer must provide evidence of S/E's license and effective controls. A reasoned legal opinion, addressed to the Acquirer from a reputable law firm with expertise in the subject matter, may be requested.
- Written Approval Required - Acquirers that decide to acquire Gambling S/Es must obtain prior written approval from AEGNS. Acquirer must notify AEGNS of any changes related to information provided or condition given for any such approval.
- S/E Registration - Acquirers must register all Gambling S/Es with AEGNS before transacting on the American Express Global Network, and confirm registration details annually thereafter upon request from AEGNS.
- Anti-Money Laundering - Maintain an effective Anti-Money Laundering (AML) monitoring program. Refer to Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30 for more information.
- Merchant Category Code (MCC) - Gambling S/Es must be identified with MCCs 7801, 7802, or 7995. Card Not Present sales of lottery tickets must be identified with MCC 7995.
- Brand Protection Assessment - Acquirers must complete a Brand Protection Assessment when acquiring Gambling S/Es. Refer to Section 2.9.5.6, "Brand Protection Assessment," on page 99 for more information.
- Risk Controls - Acquirers must incorporate risk controls within submission monitoring as requested by AEGNS.
- Winnings - Winnings cannot be credited back to a Card.
- High Risk S/E List - Gambling S/Es must be added to the High Risk S/E (HRSE) list.
- AEIPS and Expresspay Transactions - For Card Present Transactions, Gambling S/Es must process as AEIPS and Expresspay Transactions only.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Enhanced Controls - For Card Not Present Transactions:
  - Gambling S/Es must utilize SafeKey.
  - Gambling S/Es must utilize Geolocation Compliance to ensure online Transactions are restricted to within the geographic area approved by AEGNS.
  - Acquirers must make sure their Gambling S/Es maintain systems that are reasonably designed to ensure their gambling business remains within lawful limits, including, but not limited to, Geolocation Compliance and controls for age verification.
  - Acquirers must provide to AEGNS Certification of testing conducted by an independent third party, or an alternative form of proof commonly accepted in the industry in each jurisdiction where the Gambling S/E operates, that demonstrates the Gambling S/E's Geolocation Compliance effectiveness to ensure the processing of lawful Transactions. Any form of proof provided to AEGNS must at a minimum, (i) meet requirements under applicable law for conducting the Gambling S/E's business and (ii) demonstrate to AEGNS' satisfaction that the Gambling S/E's systems are reasonably designed to ensure that its gambling business will remain within lawful limits prescribed by applicable law, including with respect to age and location verification.

    Note: Gambling Transactions on Corporate Cards, OPEN Cards, Prepaid, and Commercial Cards are not allowed.

Note: State and national government-owned authorized onsite lotteries retailers registered as MCC 7995/7800 may not be required to comply with all of the requirements outlined above.

Acquirers that fail to comply with the requirements relating to Gambling S/Es detailed above will be subject to the Brand Protection Non-Compliance Fees as described in Table 10-23, "Brand Protection Non-Compliance Fees," on page 412. AEGNS reserves the right to request from Participants, at its own discretion, Documentation confirming their Gambling S/E's business is compliant with the general requirements described in this section.

2.9.5 Brand Protection

Brand Protection encompasses policies and procedures designed to protect the American Express Brand and Participants against exposure to regulatory, financial and brand risks associated with Illegal or Brand Damaging Activity.

2.9.5.1 Illegal or Brand Damaging Activity

An increase in Card Not Present Transactions, a range of illegal products, and deceptive marketing practices expose American Express and Participants to regulatory, financial, litigation and brand risk. Threats come from a variety of sources including, but not limited to:

- The sales of Infringing Products
- Unlawful sales of pharmaceutical products
- Unlawful sales of tobacco and electronic smokeless tobacco products
- Prohibited gambling activities
- S/Es engaged in activities or practices that are deceptive or misleading or that reflect unfavorably upon the good name, goodwill, reputation or image of American Express or any American Express Entity, or that in any way are contrary to applicable law
- Transactions related to child pornography, bestiality, or rape

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

At any time AEGNS may determine that a particular S/E activity or industry is an Illegal or Brand Damaging Activity. In such cases Acquirers will be notified and given a reasonable amount of time to manage the policy change. During this time Acquirers will not be subject to Brand Protection non-compliance fees that may arise from violations associated with the S/Es targeted by the change.

Acquirers are required to ensure their S/Es, Sponsored Merchants and Payment Facilitators accepting or processing American Express Cards are not participating in Illegal or Brand-damaging activity as determined by AEGNS, which includes advertising or an intention to sell illegal or Brand-damaging Goods where there is association with the American Express Brand or where the American Express Blue Box logo is displayed. All Transactions must be legal in both the seller's and buyer's jurisdictions.

Acquirers are also required to:

- Register S/Es in accordance with Section 2.9.4.2, "Restricted Industries," on page 95.
- Report violations to AEGNS in accordance with Section 2.9.5.2, "Reporting Violations," on page 98.
- Investigate potential violations at the request of AEGNS in accordance with Section 2.9.5.3, "Investigations," on page 99.
- Correct all violations, regardless of how they were identified and regardless of whether an investigation was requested by AEGNS or not, in accordance with Section 2.9.5.4, "Correcting Violations," on page 99.
- Verify compliance of an S/E's business at the request of AEGNS, in accordance with Section 2.9.5.5, "Verification of Compliance," on page 99.

Acquirers should refer to the *Brand Protection Guide for Acquirers* available on Knowledge Base for additional information related to Brand Protection policies and processes. Use the Search function to locate these documents.

2.9.5.2 Reporting Violations

Acquirers are required to report violations to AEGNS in writing related to Illegal or Brand Damaging Activity. Violations must be reported as soon as possible but in no case later than seventy-two (72) hours after discovery. For additional instruction on how to report violations please refer to the *Brand Protection Guide for Acquirers* on Knowledge Base.

Brand Protection non-compliance fees for violations related to Illegal or Brand Damaging Activity will be waived if the Acquirer reports the violations to AEGNS in writing before AEGNS notifies the Acquirer of the violation, so long as the violation is then corrected according to policies herein.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.5.3 Investigations

At the request of AEGNS, an Acquirer must investigate the activity of an S/E and provide all requested information to AEGNS as soon as possible, but in no case later than the time period stated in the following table:

Table 2-12. Investigation Time Periods

Violation	Investigation Time Period
Sale of Infringing Products	Thirty (30) Business Days
Illegal or Brand Damaging Activity related to child pornography	Three (3) Business Days
All other cases involving Illegal or Brand Damaging Activity	Ten (10) Business Days

Note: The time periods in the table above may be amended at any time, at the sole discretion of AEGNS. AEGNS may grant an extension allowing an Acquirer more time to perform an investigation.

In all cases, AEGNS will decide, based on the Acquirer's investigation report and any other relevant information, whether to take no action, to require further investigation, or to require suspension or termination of the S/E.

2.9.5.4 Correcting Violations

Acquirers are required to correct violations related to Illegal or Brand Damaging Activity as soon as possible, but in no case later than ten (10) Business Days from the date the violation is confirmed (three (3) Business Days for cases involving child pornography). These timeframes may be amended at any time at the sole discretion of AEGNS. Correction may include a requirement by AEGNS for the Acquirer to cancel the S/E account immediately.

2.9.5.5 Verification of Compliance

Acquirers may be required to provide verification that an S/E's, Payment Facilitator's, or Sponsored Merchant's business is compliant with applicable laws and regulations. Examples include, but are not limited to, an attestation from the S/E, Payment Facilitator, or Sponsored Merchant, a Certification or accreditation by a recognized third party or an independent written opinion from legal counsel, that the S/E's, Payment Facilitator's, or Sponsored Merchant's activity complies with all applicable laws and regulations.

2.9.5.6 Brand Protection Assessment

Acquirers must have adequate policies, procedures and controls in place to mitigate risks of acquiring S/Es that participate in Illegal or Brand Damaging Activity. The Brand Protection Assessment enables AEGNS to assess the capability of an Acquirer to mitigate such risks and identifies potential deficiencies in an Acquirer's acquiring policies, procedures and controls. Acquirers are required to work with AEGNS to remediate any deficiencies that may be uncovered by the Brand Protection Assessment.

A Brand Protection Assessment includes:

1. Completion of a Brand Protection Assessment questionnaire.
2. Correction of any deficiencies as determined by AEGNS. The status of any remediation activities must be provided to AEGNS upon request.
3. Written confirmation from AEGNS that the Brand Protection Assessment has been completed, deficiencies have been corrected to the satisfaction of AEGNS and the Acquirer is approved, subject to all other requirements of the *Business and Operational Policies* manual, to acquire S/Es in industries or participating in activities listed in Table 2-11, "Restricted Industries Requirements," on page 95.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

AEGNS will provide the questionnaire to Acquirers when the request is made to begin a Brand Protection Assessment. The assessment is subject to a processing fee (see Section 10.7.2.1, "Brand Protection Assessment Fees," on page 412). Acquirers will be given a minimum of three (3) months to complete and return a Brand Protection Assessment questionnaire from the date AEGNS requests its completion. Acquirers that fail to complete a Brand Protection Assessment within the timeframes specified in a request by AEGNS will be subject to Brand Protection non-compliance fees.

Acquirers are required to complete a Brand Protection Assessment if they satisfy one (1) or more of the following conditions:

- The Acquirer signs S/Es who operate in industries or participate in activities listed in Section 2.9.4.2, "Restricted Industries," on page 95.
- The Acquirer is identified as acquiring an S/E that participates in Illegal or Brand Damaging Activity.
- The Acquirer currently has no S/Es operating in industries or participating in activities listed in Section 2.9.4.2, "Restricted Industries," on page 95, but wishes to sign such S/Es in the future. The Acquirer must complete the Brand Protection Assessment prior to signing said S/Es.

After completing an initial Brand Protection Assessment, an Acquirer may be required to complete a supplemental Brand Protection Assessment periodically thereafter, but in no case more frequently than annually, in order to ensure ongoing adherence to AEGNS policies. At the sole discretion of AEGNS, an Acquirer may be required to complete a supplemental Brand Protection Assessment if the Acquirer is exposed to an increased level of risk, on the basis of factors including, but not limited to, a change in regulation or business model, or if the Acquirer has acquired an S/E that participates in a restricted industry or in Illegal or Brand Damaging Activity.

See Section 10.7.2.1, "Brand Protection Assessment Fees," on page 412 for information on Brand Protection Assessment processing fees.

2.9.5.7 Data Quality

MCCs, Point of Service Data Codes and On-Us data provide the AEGN with information that helps support Brand Protection policies. Acquirers are required to ensure:

- S/Es are assigned the correct MCC (see *Codes Reference Guide* for additional information).
- Point of Service Data Code conforms to the current Network Specifications manuals.
- On-Us data is both accurate and complete. See Section 2.9.2.2, "Acquirer File Submission Requirements," on page 85 for additional information.

Violations related to MCCs or Point of Service Data Codes which involve S/Es who operate in industries or participate in activities listed in Section 2.9.4.2, "Restricted Industries," on page 95, and On-Us data violations must be corrected within thirty (30) Business Days of notification from AEGNS to the Acquirer in order to avoid non-compliance fees (see Table 10-23, "Brand Protection Non-Compliance Fees," on page 412).

An Acquirer found to be submitting inaccurate or incomplete data to the AEGN in an attempt to circumvent Brand Protection policies will be subject to Brand Protection non-compliance fees.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.6 Unique S/E Number

Except as otherwise agreed in the Participant Agreement, only a single 10-digit S/E number range shall be made available to each Acquirer.

In addition:

- If the S/E has more than one (1) location, the Acquirer may either assign a separate S/E number for each location or a single S/E Number for multiple locations.
- The S/E number assigned must be within the range of S/E numbers the Acquirer was provided during implementation. This will either be a 3-digit or 6-digit range depending on the market.
- Acquirers must submit the S/E number assigned to the location(s) on every POS Authorization Request (1100) message and every Presentment. An S/E may choose to process centralized authorizations and/or centralized submissions. Acquirers must ensure that the S/E number representing the actual S/E location is defined as part of the hierarchy for the central S/E number used on Transactions.
- The S/E number assigned must conform to the Network Specifications manuals (e.g., Mod 10).

AEGNS reserves the right to add to the High Risk S/E list any S/E Number(s) used by Acquirers in a way that is not compliant with this policy.

Acquirers found to be out of compliance with this policy may be subject to non-compliance fees. See Section 10.7.1, "General Non-Compliance Fees," on page 411 for more information.

2.9.7 S/E Website Information Display Guidelines

Acquirers must ensure that S/Es adhere to the following website information display guidelines. The S/E website must display the following:

- An accurate description of Goods/Services offered, including the currency type for the Transaction (e.g., U.S. Dollars, Canadian Dollars)
- An email address and a telephone number for customer service disputes
- The S/E's return/refund policy
- A description of the S/E's delivery policy (e.g., No COD, No overnight)
- A description of the S/E's security practices (e.g., information highlighting security practices the S/E uses to secure Transactions conducted on the Internet)
- A statement of known export restrictions, tariffs, and any other regulations
- The name of the country in which the S/E is located
- A privacy statement regarding the type of personal information collected and how the information is used. Additionally, S/Es must provide to consumers the option to decline being included in marketing campaigns or having their personal information included on lists sold to third parties. S/Es may use the following privacy statement, provided that their practices comply with this statement:
  At [S/E name] we are committed to protecting the privacy of all our customers. We collect only customer information that is needed and we inform all customers how we use it. On a regular basis, we give customers choices about how their data will be used including the option to decide whether or not they wish to have their names removed from lists used for marketing campaigns. All customer information is stored securely and access to it is limited to those employees who specifically need it to conduct their business responsibilities. All [S/E name] employees and business partners are responsible for upholding our privacy principles.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.8 S/E Monitoring

Refer to Section 8.9.3, "S/E Risk Management," on page 388 and Section 2.9.5, "Brand Protection," on page 97 for additional information.

2.9.9 S/E Floor Limits

AEGNS has established Network Floor Limits, however, it is the Acquirer's prerogative to set individual Floor Limits for S/Es. By setting an S/E's Floor Limit above the Network Floor Limit amount for that S/E category, the Acquirer assumes the financial risk of allowing unauthorized Transactions that exceed the Network Floor Limits. Specific Chargeback rights are afforded Issuers when presented with Transactions that meet the criteria set forth in Chapter 7 "Chargeback Policies" beginning on page 280.

2.9.10 S/E Classifications

AEGNS publishes a separate listing of Merchant Category Codes (MCC) in the *Codes Reference Guide* to be used by Acquirers when classifying S/Es. The MCCs are used to determine the Floor Limits for S/Es and are useful to the Issuer when determining the risk associated with authorizing Transactions at the S/E. The Acquirer must ensure that the correct MCCs are assigned to S/Es and that the correct MCC is submitted on each Authorization Request and outclearing. Acquirers shall not present for payment any Transactions from any S/Es doing business in any prohibited industry. An Acquirer found assigning an incorrect MCC to an S/E in order to circumvent this requirement must cancel the S/E. Refer to Section 2.9.4.1, "Prohibited Industries," on page 94 for a list of prohibited industries.

2.9.11 S/E Card Acceptance Process

Acquirers are responsible for ensuring that S/Es conform to Card acceptance procedures as defined in:

- Section 2.9.3, "S/E Qualifications and Agreement Requirements," on page 86
- Section 4.2, "S/E Card Acceptance Procedures," on page 214, and
- Section 4.6, "ATM Requirements," on page 241.

Failure to do so may result in Transactions that are subject to Chargeback rights as defined in the "Chargeback Policies" chapter beginning on page 280.

Acquirers may be required to accept Fraud Full Recourse Chargebacks and/or suspend doing business with S/Es where excessive numbers of fraudulent Transactions have taken place or where Card Accounts are being compromised.

The S/E must use the appropriate Point of Service Data Code indicating the Transaction was processed via the Internet. Refer to Point of Service Data Codes in the *Codes Reference Guide.*

2.9.12 Acquirer Transaction Processing Requirements

All ROCs must be submitted by the Acquirer to the AEGN for clearing no later than thirty (30) days from the Transaction Date of the ROC. Submitting a ROC more than thirty (30) days after the Transaction Date may subject the Transaction to Chargeback.

Further, Acquirers must comply with all AEGNS requests to supply Clearing Centers with specific items of transaction data on all Charges at their S/Es (including requests for enhanced data capture in connection with Commercial Cards) at the times and in the formats designated by AEGNS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.13 Requirements for Acquirers of Cash Disbursements

Cash Disbursements are manual disbursements of cash to Cardmembers by an individual at a Cash Disbursement Provider in the Provider's local currency. Cash Disbursement Transactions are identified by Merchant Category Code (MCC) 6010 - Financial Institutions, Manual Cash Disbursements.

Acquirers of Cash Disbursement Transactions along with their Cash Disbursement Providers are subject to all of the requirements for Acquirers and S/Es as described in Section 2.3.3, "Additional Anti-Money Laundering (AML) Requirements for Cash Disbursements," on page 33 and Section 2.9, "Requirements for Conducting Merchant Acquiring Business," on page 83.

Acquirers of Cash Disbursement Transactions are required to monitor and report Cash Disbursement Transactions at their Cash Disbursement Provider locations in accordance with AEGNS requirements and as prescribed by local law. Refer to Section 2.10.4, "Use of Cardmember Information," on page 113.

2.9.13.1 Point of Sale Device Requirement for Cash Disbursement

As an added security measure for Issuers, Acquirers of Cash Disbursement Transactions must ensure that Point of Sale (POS) devices deployed to facilitate these Transactions are programmed to always prompt for the PCSC and to submit it as part of the Authorization Request.

2.9.14 Stored Value Digital Facility Acquirer Requirements

A Stored Value Digital Facility (SVDF) is an S/E-offered feature that allows funds to be loaded into a digital wallet for subsequent payments, including purchases of Goods and Services, at single or multiple payment acceptors.

SVDFs that facilitate purchases at multiple different End Beneficiaries are Indirect Acceptors and as such are required to comply with the requirements established in Section 2.6, "Indirect Acceptors," on page 74.

Acquirers must ensure that S/E agreements (with S/Es that offer SVDF) include requirements that the S/E must comply with local laws or regulations for SVDF, including, but not limited to, registration, licensing, or requirements to hold funds in reserve. Acquirers that do not comply with this S/E agreement requirement may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.9.15 Internet Transaction Descriptor Information

Acquirers are required to include a meaningful description of Internet S/Es' products or services when outclearing Presentments to the AEGN. This will help reduce the incidents of customer service inquiries and Chargebacks.

2.9.16 Record of Charge Archival Storage

The Acquirer must maintain (or mandate that S/Es maintain) ROCs for all Transactions which are submitted by S/Es and presented to the AEGN for payment. The Acquirer or their S/E must retain the original or electronically store ROCs for all Transactions. The ROC and other supporting Documentation for any Transaction must be supplied to the Issuer upon receipt of a Retrieval Request Notification (1642) message from the Issuer. The ROC and other supporting Documentation must be available to the Issuer for a period of at least one (1) year (or as required by local law) following the Network Processing Date of the Transaction.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.17 Chip Card Requirements

American Express supports two (2) types of Chip Card terminal applications. These applications must be certified by the AEGN to comply with either or both of the following specifications:

- AEIPS Terminal Technical Manual
- Expresspay Terminal Specifications

Implementation of AEIPS and/or Expresspay-compliant card readers/POS devices is at the sole discretion of Acquirers. However, Acquirers choosing to proceed with implementation of a Chip Card program, must adhere to the following requirements:

- The Acquirer must be approved by AEGNS for Chip Card enablement.
- POS devices must be certified as AEIPS and/or Expresspay-compliant.
- Acquirers must ensure that Chip Card-enabled POS devices are in compliance with industry POS security standards (e.g., current PCI requirements and guidelines for PIN entry devices that can be accessed at www.pcisecuritystandards.org).
- The POS devices must capture and pass AEIPS and/or Expresspay data in the POS Authorization Request (1100) message. Refer to the Network Specifications manuals for more information.
- For AEIPS and EMV Mode Expresspay Transactions, the First Presentment must include a Chip Card Addendum ((9240) message - Addenda Type Code Type 07). Refer to the Network Specifications manuals for more information.
- For AEIPS and EMV Mode Expresspay Transactions, the Transaction Certificate must be included as supporting Documentation with all Arbitration Filings submitted by the Acquirer with AEGNS.

Refer to Section 7.12, "Arbitration and Compliance," on page 366 for additional information.

Acquirers choosing to proceed with implementation of Expresspay Mobile should refer to the latest Expresspay Terminal Specifications and Network Specifications manuals available on Knowledge Base or contact their AEGNS representative for more information.

2.9.17.1 Certification Authority Public Key (CAPK) Management for Acquirers

- Acquirers must ensure that terminals provide space for six (6) Certification Authority Public Keys (CAPKs).
- Acquirers must ensure that AEGNS CAPKs are loaded in all POS devices that support Offline Data Authentication by the required date for Acquirers to load these public keys. Refer to Table 2-13, "CAPK Management Life Cycle," on page 104.
- Acquirers are required to remove the CAPK lengths from service in all active terminals by the required removal date. Refer to Table 2-13, "CAPK Management Life Cycle," on page 104.
- Acquirers must ensure that when an expiry date for a given CAPK length is extended by American Express, all S/Es are able to process the CAPK length up until the new expiry date.

Table 2-13. CAPK Management Life Cycle

CAPK Length	Expiry Date	Required Date for Acquirers to Load	Earliest Date for Issuers to Use	Required Removal Date at Terminals
1152	31 December 2017	31 December 2005	1 March 2006	30 June 2018
1408	31 December 2024	31 December 2006	1 January 2007	Six (6) months after expiry date
1984	31 December 2027[1]	31 December 2006	1 January 2007	Six (6) months after expiry date

1. The earliest date this CAPK will expire.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.17.2 AEIPS Terminal Requirements for the EU/EEA & UK

Acquirers must ensure all POS devices (including mPOS and CATs) are AEIPS Chip and PIN-enabled, except for unattended terminals, such as CATs, used for the purpose of paying transport fares or parking fees.

2.9.17.3 PIN Bypass Requirements for Acquirers

PIN Bypass occurs when a chip/PIN card meets (interfaces with) a chip/PIN terminal during a Transaction. The Card chip has been read but the PIN has not been verified because the cashier or Cardmember has taken a step to bypass PIN entry.

Acquirers that choose to support PIN Bypass must provide the appropriate values in the Point of Service Data Code (Bit 22) when sending the POS Authorization Request (1100) message to indicate that an Integrated Circuit Card (ICC) with PIN capability was used to initiate the Transaction but that no PIN was used to authenticate the Cardmember. This information, together with the required Terminal Verification Results (TVR), located within Bit 55 in the POS Authorization Request (1100) message, will enable Issuers to identify a PIN Bypass Transaction. Acquirers and S/Es must not alter the TVR after cryptogram generation. Refer to the *Codes Reference Guide* for more information about valid Point of Service Data Code values.

For additional information on PIN Bypass Transaction identification, please refer to the *AEIPS Terminal Technical Manual*, the AEIPS Chip Card Specifications, and the *American Express Automated Fuel Dispenser Guide (US Region)* on Knowledge Base.

2.9.17.4 Expresspay-Enabled POS Devices

Acquirers that deploy Expresspay-enabled POS Devices programmed to read Contactless Cards must adhere to the following requirements:

- Expresspay-enabled POS Devices must display the following EMVCo core visual component indicating Contactless acceptance at the POS: (www.emvco.com):



- All Expresspay-enabled POS Devices must also display a Blue Box logo:



- Acquirers must obtain AEGNS' approval prior to setting up S/Es that operate Expresspay-enabled Transit Access Terminals (TATs).
- Acquirers must ensure that new and replaced devices capable of processing Expresspay Transactions have been certified to the latest version of the Expresspay Terminal Specifications, available on Knowledge Base. Refer to the *Expresspay EMV Implementation Guide Bulletin* for dates, available on Knowledge Base.
- Acquirers must meet the requirements detailed in Section 2.9.1.1, "POS Certification Requirements," on page 84.
- Acquirers in designated countries must ensure that POS devices transition to the acceptance of both AEIPS and Expresspay. Refer to Section 2.9.17.5, "AEIPS and Expresspay Enablement Program for Acquirers," for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Acquirers within the EU/EEA & UK must ensure that:

- All Expresspay-enabled POS Devices (including Mobile Point of Sale (mPOS) and Customer Activated Terminals (CATs)) support Strong Customer Authentication (SCA) requirements, including the ability to prompt for Two Factor Authentication (2FA) upon request. Unattended terminals, such as CATs, used for the purpose of paying transport fares or parking fees, are excluded from this requirement.
- All unattended terminals, such as CATs, used for the purpose of paying transport fares or parking fees, must be identifiable as exempt to the Card when it is presented, effective April 14, 2023. Refer to the following documents, available on Knowledge Base:
  - American Express Contactless Terminal Implementation Guide
  - Expresspay Terminal Specifications

Acquirers within the United States must ensure that all Expresspay-enabled POS Devices support EMV Mode.

2.9.17.5 AEIPS and Expresspay Enablement Program for Acquirers

Acquirers located in countries as specified in Table 2-14, "AEIPS and Expresspay Enablement Program - Acquirer Countries," on page 106 must comply with the following mandates at the dates specified:

- New and Replaced POS Devices - Acquirers must be capable of processing AEIPS and Expresspay Transactions. All new and replaced POS devices (including CATs) must be AEIPS and EMV Mode Expresspay-enabled at the date specified in Table 2-14.
- All POS Devices - All existing POS devices (including CATs) must be AEIPS and EMV Mode Expresspay-enabled at the date specified in Table 2-14.

Acquirers that fail to comply with these requirements, as determined by AEGNS, may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

Table 2-14. AEIPS and Expresspay Enablement Program - Acquirer Countries

Region	Country	Effective Date for New and Replaced POS Devices	Effective Date for All POS Devices
Latin America	All[1]	October 12, 2018	April 14, 2023
EMEA	Albania, Andorra, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Faroe Islands, Finland, France, Georgia, Germany, Gibraltar, Greece, Greenland, Hungary, Iceland, Ireland, Israel, Italy, Kazakhstan, Kyrgyzstan, Liechtenstein, Luxembourg, Macedonia (Formerly Yugoslav Republic of), Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Switzerland, Tajikistan, Turkey, Turkmenistan, Ukraine, United Kingdom, Uzbekistan, Vatican City State (Holy See)	April 15, 2016	December 31, 2019
	Estonia, Latvia, Lithuania, Sweden	January 1, 2017	January 1, 2020
	All Other EMEA	October 12, 2018	April 14, 2023
APAC	Australia, New Zealand	October 17, 2014	October 16, 2015
	All Other APAC	October 12, 2018	Not Applicable

1. Excludes Caribbean Countries.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Note: This policy requirement excludes ATMs.

Note: Expresspay-enabled POS Devices that do not have a contact EMV chip reader (for example, Transit Access Terminals) are exempt from the requirement of supporting AEIPS.

For more information on the Expresspay-enabled POS Devices or Certification requirements, contact your AEGNS representative.

2.9.18 American Express SafeKey Acquirer Requirements

SafeKey is an industry-standard Authentication tool that, when employed by Issuers, Cardmembers, Acquirers, and S/Es, provides greater security for Transactions. Acquirers must comply with the following requirements:

- AEGNS strongly recommends that all Acquirers support SafeKey.
- Acquirers in designated countries must support SafeKey in accordance with the following table:

Table 2-15. Acquirer SafeKey Support Requirements

Region	Country
APAC	Australia, Bangladesh, Cambodia, Hong Kong (Special Administrative Region of China), India, Indonesia, Macao (Special Administrative Region of China), Malaysia, New Zealand, Philippines, Republic of Korea (South Korea), Singapore, Taiwan (Province of China), Thailand, Vietnam
EMEA	European Union/European Economic Area (EU/EEA) and United Kingdom (UK)

SafeKey Certification

- Prior to enabling SafeKey for S/Es, Acquirers must complete Certification according to the SafeKey specifications as described in the American Express SafeKey Protocol Specifications. Refer to the Network Specifications manuals and the American Express SafeKey Acquirer - Merchant Implementation Guides for more information.
- Acquirer Certification for SafeKey is not version-specific. Requirements are documented in all versions of the SafeKey Implementation Guides.
- Acquirers and their S/Es must comply with all SafeKey-related requirements contained in the American Express SafeKey Protocol Specifications, the American Express SafeKey Acquirer - Merchant Implementation Guides, the *Business and Operational Policies* manual, Network Specifications manuals, and *American Express SafeKey Guidelines*.
- Acquirers must ensure the requirements relating to American Express SafeKey contained in the *Business and Operational Policies* manual and the Network Specifications manuals are included in the S/E agreement.

SafeKey S/E Requirements

- Acquirers must ensure that all of their S/Es are aware of the availability of SafeKey on the AEGN.
- Acquirers should ensure S/Es employ multiple fraud mitigation practices available for that market (e.g., PCSC, AAV) to be used in conjunction with SafeKey. Refer to Section 8.11, "Fraud Mitigation Practices," on page 397 for additional information.
- AEGNS recommends that Acquirers maintain a log for at least two (2) years of all Authentication Data.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Acquirers must ensure that the Transaction Authentication was Attempted or Fully Authenticated as provided by the SafeKey service during the Transaction Authentication. Additionally, the Electronic Commerce Indicator (ECI) value of 06 or 05 respectively, must match between the POS Authorization Request (1100) message and the POS First and Second Presentment (1240) message or, for Acquirers located in Japan, only the Authorization Request message.
- Acquirers must ensure that all S/Es that offer SafeKey functionality to Cardmembers display the following core visual component on their shopping cart site:



2.9.18.1 Reuse of SafeKey Authentication Data

In a SafeKey Transaction, an S/E may only re-use the original Authentication Data when a subsequent POS Authorization Request (1100) message is necessary on the original purchase. Original Authentication Data is valid for up to ninety (90) days from the Authentication date.

Authentication data must not be submitted in the Authorization Request for separate purchases. In the event of a Cardmember dispute, the Acquirer and S/E must be able to demonstrate that all Authorization Requests relate to the single, original authenticated purchase.

2.9.19 Marketing, Advertising, and Public Relations

Acquirers must adhere to the following policies for review and approval of marketing, advertising, and public relations materials. Acquirers are responsible for ensuring that S/Es adhere to the same requirements.

- The American Express Blue Box logo may only be reproduced and used as specified in the Marketing section on Knowledge Base.
- Acquirers and S/Es may not use any existing American Express sign offs or slogans (past or present) nor may Acquirers or S/Es mimic, ridicule, copy, or alter any past or present American Express sign off or slogan.
- Acquirers and S/Es may not place any American Express Licensed Mark on any product, service, or communications materials without the prior written approval of AEGNS. Communications materials, when designed, should place American Express Licensed Marks in a preferred position.

In addition, Acquirers must comply with the neutrality principles set out in "Exhibit 19. Neutrality Principles for Conducting Merchant Acquiring Business" on page 489 when promoting local S/E offers.

2.9.20 Transfer of S/E Portfolio

An Acquirer must not transfer an S/E portfolio, in whole or in part, to any third party (other than a subsidiary which is 100% owned by it) without the prior written consent of AEGNS. In the event that an Acquirer wishes to transfer an S/E portfolio to such 100%-owned subsidiary, it may do so upon sixty (60) days prior written notice, but only on the express conditions that:

- Such 100%-owned subsidiary must meet all the requirements set forth in the applicable Participant Agreement and in AEGNS manuals, and otherwise be capable of performing the obligations of the applicable Acquirer thereunder, and
- The Acquirer guarantees and shall remain liable for the full performance and payment by such subsidiary of any and all obligations under the applicable Participant Agreement. An Acquirer shall be permitted to transfer S/Es pursuant to this section no more frequently than once per year.

Any other entity to which an Acquirer wishes to transfer an S/E portfolio must meet AEGNS' requirements and enter into a Participant Agreement with an American Express Entity.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.9.21 No Factoring

Except as permitted under the Participant Agreement or otherwise permitted in writing by AEGNS, a Participant shall not factor any of its accounts receivable from an American Express Entity under the Participant Agreement or assign any interest therein as security for Participant obligations or otherwise permit any lien or security interest to attach to or remain on any such accounts receivable.

Note: This restriction is not intended to prevent a Participant, in its capacity as an Issuer, from securitizing its account receivables from Cardmembers, or from selling or assigning to outside collection agencies or attorneys such of its accounts receivable from Cardmembers that remain unpaid after all normal collection efforts have been made, but in no event that are less than ninety (90) days past due.

2.9.22 Cancelled S/E Policy

Acquirers are responsible for ensuring that Authorization Requests submitted by S/Es whose Card acceptance agreement has been cancelled by the Acquirer for derogatory reasons, as listed in Table 8-1, "Derogatory Status Reason Codes (Cancellation)," on page 387 in Section 8.9.2.5, "Cancelled S/Es (Derogatory)," on page 387, are rejected by the Acquirer's Authorization system. Authorization Request messages from such cancelled S/Es must not be sent to the AEGN. Penalties may be assessed for non-compliance. See Table 10-7, "Violations Subject to Fraud Non-Compliance Fee Schedule A," on page 404, and Table 10-6, "Fraud Non-Compliance Fee Schedule A," on page 403 for violation information. Acquirers are responsible for ensuring that Transactions initiated by such cancelled S/Es are not outcleared to the Network.

2.10 Requirements for Conducting Card Issuing Business

This section provides policies and rules specific to Issuers.

Prior to engaging in the Card Issuing Business, Issuers must complete the Certification process described in Section 2.2.6, "Network Infrastructure Access and Certification," on page 14 and Section 2.10.1, "Certification of Card Issuing Programs," on page 110. AEGNS will provide each Issuer with the support described in Section 2.2.7.1, "AEGNS Assistance Prior to Launch," on page 14 prior to the issuance of an Issuers first Card.

Each Issuer shall bear the cost of Certification of its Card Issuing Business (including, without limitation, its Authorized Processors) as determined by AEGNS. When considering making an operational or systems change to its Card Issuing Business, an Issuer must contact its AEGNS representative to ensure compliance with AEGNS policy. Regardless of whether Certification is conducted by AEGNS or its designee, Issuers shall be fully liable for their failure to perform, or the failure of any of their agents and processors (including without limitation, Authorized Processors and their agents).

Each Issuer must be party to all of its Cardmember Agreements. The authority to act as an Issuer and be the named contractual party on the relevant agreement cannot be transferred, outsourced or delegated. Issuers must ensure that all agreements, disclosures, communications, and solicitations comply with applicable laws and regulations and this AEGNS manual, including, without limitation, Section 3.9.1.6, "Cardmember Agreement/Solicitation Materials," on page 207.

Under no circumstances shall applications for American Express Cards, even if declined, be treated as an application for the issuance of another general purpose card network product; it being understood that Issuers are not prevented from issuing another general purpose card network product on the basis of an application specific to such general purpose card network product.

Subject to this AEGNS manual and the Issuer's rights to be reimbursed pursuant to the Chargeback policy, each Issuer alone bears all financial risk (including i.e., credit risk, fraud risk and counterfeit risk) arising from or associated with its Card Issuing Business.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.1 Certification of Card Issuing Programs

Certification means testing to verify that a process or service complies with AEGNS' standards. For certain items, Issuers will be required to perform the Certification process themselves and provide written evidence of Certification. For other items, Certification will be performed by AEGNS or its designee.

Issuers are required to submit certain aspects of their Card Issuing Business for Certification by AEGNS in order to maintain the quality, efficiency, and financial soundness of the Network, its Participants, and the American Express Brand image. If the Issuer wishes to use a third-party processor to perform any aspect of the Card processing, such processors must be certified as Authorized Processors as described in Section 2.8, "Authorized Processors," on page 80, capable of performing the processing services before they begin any such processing. Certification shall occur prior to the time the Issuer issues Cards and thereafter as deemed necessary by AEGNS upon changes in the Authorized Processor used by the Issuer, implementation of new systems and/or operating procedures and/or a decline in operating quality.

Issuers shall specifically comply with, and certify compliance with the following requirements:

- Issuers must ensure that the Primary Account Number (PAN) is encoded and visible on their Cards and/or programmed on an AEIPS-compliant chip (which includes the BIN) and that their Cards comply with the most recent version of the Network Specifications manuals, the Marketing section of Knowledge Base, the AEIPS Chip Card Specifications, and *AEIPS Terminal Technical Manual*.

  Note: The above requirement does not apply in the case of Cardless Accounts where a physical card is not issued for the Account.
- All activities related to Network connectivity in which data passes between the AEGN, Acquirers, Issuers, and/or their Authorized Processors as described in the Network Specifications manuals.
- Issuers must ensure that all computer systems and software used in their conduct of the Card Issuing Business have been tested and will be fully capable of providing accurate results.
- AEGNS' policies for maintaining confidentiality of Network information.
- AEGNS' policies related to Anti-Money Laundering (AML), Anti-Terrorist Financing and Customer Screening Programs. For details, see Section 2.10.4, "Use of Cardmember Information," on page 113.
- Any other activity deemed by AEGNS to require Certification.

2.10.1.1 Advanced Payment Product Certification Requirements

In order to conduct business on the Network and enable payment Transaction interoperability, AEGNS requires that Issuers of Advanced Payment Products successfully complete the end-to-end Issuer personalization Certification process for all such products. All Advanced Payment Products must have a valid and current Certification prior to deployment.

Advanced Payment Products include, but are not limited to:

- EMV products (Chip Cards)
- Expresspay products, wearables (dual interface Chip Cards), bracelets, key fobs, etc.
- Expresspay Mobile products
- HCE

For more information on the Issuer personalization Certification process and how to comply with the requirements, see the *Issuer Personalization Certification Guide* available on Knowledge Base.

Issuers are solely responsible for all costs and fees associated with the Issuer personalization Certification process, including without limitation, the fees described in Section 10.5.12, "Issuer Personalization Certification Testing," on page 409.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Issuers found not to be in compliance with any section of this policy may be subject to fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411, and will be required to complete the end-to-end Issuer personalization Certification process.

For more information on Issuer personalization Certification, contact your AEGNS representative.

2.10.1.2 Beta Test of Cards and Expresspay Mobile

A Beta Test is the process of testing the functionality of a system in a live operational environment, or if agreed by AEGNS, in an environment as close to full-scale production as possible to validate performance prior to product launch. AEGNS and the Issuer shall conduct a Beta Test before the Issuer begins any sales or marketing activity with respect to each type of Card, and prior to release of any change to the design of an existing Card to determine, to the satisfaction of AEGNS, that the proposed Cards comply with AEGNS requirements, can be accepted operationally by S/Es, and that Transactions incurred with such Cards can be properly authorized, submitted, processed, billed, and settled.

Upon successful completion of the Beta Test, and receipt and approval by AEGNS of a sample Card of the type to be issued, AEGNS will notify the Issuer that it may begin sales and marketing or release of such Cards.

The initial Beta Test and any subsequent Beta Test shall take no longer than sixty (60) days, except as necessary to address problems identified during a Beta Test.

Issuers and their Mobile Entities, including Service Providers as applicable, who participate in the enablement and deployment of Expresspay Mobile shall participate in a Beta Test with AEGNS prior to the product release. The results of the Beta Test must demonstrate, to the satisfaction of AEGNS, that the proposed Expresspay Mobile complies with AEGNS requirements, can be accepted operationally by S/Es, and that Transactions initiated with the Expresspay Mobile can complete the Transaction Life Cycle.

2.10.1.3 Launch Date

The Issuer shall use best efforts to ensure that the Launch Date for Cards or Expresspay Mobile shall be no later than forty-five (45) days from the end of the applicable Beta Test.

The initial Beta Test (the Beta Test for the first type of Card an Issuer proposes to issue under the Participant Agreement) will take place in a manner which will allow the Issuer to meet its launch date as set out in the Participant Agreement.

2.10.1.4 Card Security Requirements

2.10.1.4.1 Card Security Encoding Requirements

Issuers are required to encode a 5-digit Card Security Code (5CSC) on the magnetic stripe (Track 1 and Track 2). Issuers may choose to encode the Integrated Circuit Card Security Code (iCSC), instead of the 5CSC, on the magnetic stripe equivalent of AEIPS Chip Cards. For additional information, please contact your AEGNS representative.

2.10.1.4.2 Card Security Code (CSC) Validation

Issuers must have the capability (directly or through a third-party processor) to validate the 5CSC and the iCSC, if used, and must perform validation for all swiped and chip-read Transactions. Refer to Section 8.10.2, "5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program," on page 392 for details on Issuer requirements and Section 10.3.3, "5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program Non-Compliance Fees," on page 405 for details on non-compliance fees.

Issuers are also required to validate the PCSC value whenever it is provided in the POS Authorization Request (1100) message and are required to return the result of that validation (indicating whether or not the PCSC was valid) in the POS Authorization Response (1110) message. These requirements also apply to Issuers that choose to provide a One-Time Password (OTP) to their Cardmembers instead of the PCSC.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Issuers that do not meet these PCSC validation requirements are prohibited from filing a Chargeback under "ISO 4540 - Card Not Present" on page 330 when an S/E submits the PCSC in the POS Authorization Request (1100) message. Refer to "ISO 4540 - Card Not Present" on page 330 for more information. Issuers that do not comply may be subject to non-compliance fees.

In the case of Cardless Accounts that do not have a PCSC associated with them, Issuers should be aware that S/Es may not accept Transactions when a PCSC is not provided in addition to the Account number and the Expiration Date.

2.10.1.5 Issuer Liability for Licensed BINs

BINs are licensed to AEGNS Issuing Participants under terms and conditions specified in the Participant Agreement including, but not limited to, the following:

- Upon licensing, the Issuer accepts full responsibility and liability for all Transactions conducted on the licensed BIN ranges. See Section 5.3.9, "BIN Blocking," on page 250 for additional information.
- Issuers shall provide AEGNS a list of all its Card products by their respective BIN ranges.
- Issuers must ensure that Card products are allocated within their BINs in accordance with local regulatory requirements.
- Issuers may not configure the magnetic stripes on Cards in any way as to allow a Transaction on a Card to be routed to another network for Authorization, Clearing, or Settlement.
- Issuers must instruct their Cardmembers not to cause a Transaction on a Card to be routed over a network other than the AEGN.

2.10.2 Reporting to AEGNS

This section details information requirements that the Issuer shall furnish to AEGNS in order to participate on the Network.

2.10.2.1 Annual Plan Disclosure

To anticipate future load capacity, effectively administer the Network, and ensure protection of the American Express Brand, AEGNS must be made aware of Issuer plans that could affect the performance of the AEGN. Data regarding volume and future volume predictions helps AEGNS to plan for growth and to assess the need for operational and technical changes.

Issuers, at their sole expense, shall have the responsibility for preparing a yearly plan for their Card Issuing Business and shall submit such plan for AEGNS' review by the first of August of the preceding year. AEGNS shall be allowed to review such a plan in advance for purposes of assessing what effect the implementation of such a plan will have on the AEGN and for ensuring that all advertising and marketing aspects of the plan are consistent with guidelines for the protection of the American Express Brand. The plan, after review by AEGNS, will be effective for the following calendar year.

AEGNS must be informed immediately of any revision or re-forecast of such plan which may occur during the plan year.

2.10.2.2 Fraud Data

Issuers are required to provide fraud data to the AEGN electronically via the Fraud Repository or manually via the American Express Worldwide Fraud Information System (WFIS). The GNS Fraud Repository will be updated with information from Issuers to allow fraud to be monitored. See the "Security and Fraud" chapter beginning on page 375 for details. See Section 8.7, "Issuer Fraud Reporting," on page 382 for details on Issuer requirements and penalties for non-compliance.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.3 Cardmember Information - Data Requirements

Issuers are required to provide AEGNS with a monthly file containing Cardmember Information in accordance with this section.

2.10.3.1 Issuers in the United States

Refer to the requirements set out in the *Network Cardmember Information Guide* located on Knowledge Base.

2.10.3.2 Local Network Card Issuers Outside of the United States

Refer to the requirements set out in the *Network Cardmember Information Guide* located on Knowledge Base.

2.10.3.3 Non-Local Network Card Issuers Outside of the United States

Refer to the Participant Agreement for requirements that apply with respect to reporting Cardmember Information to AEGNS.

Issuers that do not comply with the requirements set out in Section 2.10.3, "Cardmember Information - Data Requirements," on page 113 may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.10.4 Use of Cardmember Information

2.10.4.1 Issuers in the United States and Non-Local Network Card Issuers Outside of the United States

Refer to the Participant Agreement for terms that govern AEGN use of Cardmember Information.

2.10.4.2 Issuers Outside of the United States

Consistent with Section 3.9.1.6, "Cardmember Agreement/Solicitation Materials," on page 207, Issuers outside of the United States shall provide appropriate notices to and procure any necessary consents from Cardmembers to enable the Cardmember Information to be shared with American Express Entities and for American Express Entities to carry out the following activities:

- To produce and provide to each Issuer, merchants, prospective merchants and other third parties, analyses and reports containing Cardmember Information, Cardmember spending and Cardmember characteristics compiled into an aggregated and anonymous format.
- For other purposes AEGNS deems reasonably necessary to support or promote the Network, reduce fraud on the Network and/or enhance the American Express Brand, including, without limitation, Network-wide offer fulfillment, statistical analysis of offer and advertising effectiveness, and other market research.

American Express Entities may supplement Cardmember Information provided from Issuers with Transaction data to further the activities set forth above. Subject to applicable law, American Express Entities and Participants have the right to use Transaction data that they receive or process in their role on the Network. Refer to Section 2.2.15, "Transaction Data Use," on page 24 for more information.

American Express Entities may supplement Cardmember Information provided from Issuers to further the activities set forth in the section immediately above.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.4.3 Issuer Obligations

Issuers will ensure that all uses of Cardmember Information and Cardmember lists, including, without limitation, mailings or other communications to Cardmembers, are in compliance with AEGNS policy and with all applicable laws and regulations and with any third-party agreements to which an Issuer is a party. In order to protect the American Express Brand, Issuers shall not, without prior written approval from AEGNS, include in any Card advertising or promotional materials or features the brand of any competing card network or system.

2.10.4.4 Third-Party Obligations

If Issuers make Cardmember Information or Cardmember lists available to third parties for such third parties' promotional or advertising purpose, the following compliance requirements must be met:

- Issuers shall ensure that the promotional or advertising activities for which access to Cardmember Information or Cardmember lists is given are in compliance with AEGNS policy and will in no way denigrate or degrade the American Express Brand;
- Access to Cardmember Information or Cardmember lists will not be granted to third parties for the purpose of marketing or promoting credit cards, charge cards, stored value cards, prepaid cards, debit cards, chip cards, mobile devices, travelers checks, or travel services (unless they allow the Card as a payment method); and
- There shall be no mention of American Express or any American Express Entity, or use of any American Express Licensed Marks or other related logos or indicia, in any materials sent to Cardmembers by such third parties (unless such third party has entered into a Card acceptance agreement with an Acquirer and except as is necessary to make the Card available as a payment method).

2.10.5 Cash Disbursement Issuer Requirements

AEGNS Issuers are required to monitor and report Cash Disbursement Transactions as prescribed by local law and in accordance with the following AEGNS requirements. Issuers must:

- Perform velocity controls on Cash Disbursement Transactions on a single Account and across multiple Card numbers tied to a single Account,
- Perform Cardmember/Account(s) due diligence and monitoring, and
- Report cash Transactions in accordance with local law. Refer to Section 2.3.3, "Additional Anti-Money Laundering (AML) Requirements for Cash Disbursements," on page 33 for additional information.

2.10.6 Stored Value Digital Facility Issuer Requirements

A Stored Value Digital Facility (SVDF) is an S/E-offered feature that allows for funds to be loaded into a digital wallet for subsequent payments, including purchases of Goods and Services, at single or multiple payment acceptors.

Specific Chargeback rights are afforded to Issuers for Transactions that fund an SVDF. Chargeback rights are not afforded to Issuers for any subsequent payments using funds loaded in an SVDF.

All subsequent payments using an SVDF are similar to those made with cash. AEGNS recommends Issuers advise Cardmembers that disputes of subsequent payments should be addressed directly with the S/E that offers SVDF or payment acceptor.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.7 Chip and Contactless Card Requirements

Issuers that implement Chip Cards must adhere to the following requirements:

- Certification to the latest AEIPS Chip Card Specifications is required.
- Chip Cards issued must contain both a chip and a magnetic stripe.
- Issuers must sign the Application Interchange Profile (AIP) on Chip Cards during the Chip Card personalization process.
- Chips on Chip Cards must utilize Dynamic Data Authentication (DDA) technology.
- Issuers must encode the iCSC value instead of the 5CSC on the magnetic stripe equivalent of AEIPS Chip Cards. Refer to Section 5.10.4.4, "iCSC," on page 266 and Section 8.10.2, "5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program," on page 392 for additional information.

See Section 3.2.7, "Chip Cards," on page 131 for additional information.

Issuers in designated countries must issue new and replaced Cards with AEIPS and Expresspay capability. Refer to Section 2.10.7.5, "AEIPS and Expresspay Enablement Program for Issuers," on page 116.

2.10.7.1 AEIPS Chip and PIN-Enabled Cards for EU/EEA & UK

Issuers within the European Union/European Economic Area and United Kingdom (EU/EEA & UK) must ensure that all Cards within the EU/EEA & UK are AEIPS Chip and PIN-enabled, unless local law or regulation deems otherwise.

2.10.7.2 Transaction Requirements for the EU/EEA & UK

Issuers within the European Union/European Economic Area and United Kingdom (EU/EEA & UK) are responsible for complying with the European Commission's revised Directive on Payment Services (PSD2) and must meet Strong Customer Authentication (SCA) Transaction requirements.

2.10.7.3 Certification Authority Public Key Management for Issuers

Issuers must follow the requirements detailed in Table 2-16, "CAPK Management Life Cycle," on page 116, including:

- The Issuer Certification Authority must not utilize a particular CAPK before the date specified in the "Earliest Date for Issuers to Use" in Table 2-16.

  Note: Issuers must not issue Cards with a particular CAPK before the date specified in the "Earliest Date for Issuers to Use" in Table 2-16.

- Issuers must move to the next length in sufficient time to prevent Cards in Force from expiring after the expiry date of the current CAPK length.

  Note: For example, Issuers currently using the 1152 CAPK must start issuing Cards with 1408 CAPK for Cards with a three (3) year tenure, and should have already started issuing Cards before the end of 2012 for Cards with a five (5) year tenure.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 2-16. CAPK Management Life Cycle

CAPK Length	Expiry Date	Required Date for Acquirers to Load	Earliest Date for Issuers to Use	Required Removal Date at Terminals
1152	31 December 2017	31 December 2005	1 March 2006	30 June 2018
1408	31 December 2024	31 December 2006	1 January 2007	Six (6) months after expiry date
1984	31 December 2027[1]	31 December 2006	1 January 2007	Six (6) months after expiry date

1. The earliest date this CAPK will expire.

2.10.7.4 PIN Bypass Requirements for Issuers

PIN Bypass occurs when a chip/PIN card meets (interfaces with) a chip/PIN terminal during a Transaction. The Card chip has been read but the PIN has not been verified because the cashier or Cardmember has taken a step to bypass PIN entry.

For additional information on PIN Bypass Transaction identification, please refer to the *AEIPS Terminal Technical Manual*, the AEIPS Chip Card Specifications, and the *American Express Automated Fuel Dispenser Guide (US Region)* on Knowledge Base.

Issuers who approve PIN Bypass Transactions do so at their own risk of increased fraudulent activity.

2.10.7.5 AEIPS and Expresspay Enablement Program for Issuers

Issuers located in the countries specified in Table 2-17, "AEIPS and Expresspay Enablement Program - Issuer Requirements" must:

- Be capable of processing AEIPS and Expresspay Transactions
- Ensure new and replaced Cards are AEIPS- and Expresspay-enabled in accordance with the AEIPS and Expresspay Chip Card Specifications available on Knowledge Base

Issuers that fail to comply with these requirements, as determined by AEGNS, may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

Issuers not located in the countries specified in Table 2-17 may choose to issue Cards with AEIPS and Expresspay capability, subject to approval by AEGNS.

Table 2-17. AEIPS and Expresspay Enablement Program - Issuer Requirements

Region	Country
Latin America	All[1]
EMEA	All EMEA
APAC	All APAC

1. Excludes Caribbean Countries

Note: Prepaid Cards, including non-reloadable Prepaid (Gift) Cards are exempt from the requirement to support Expresspay.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.8 Additional Marketing and Advertising Requirements for Issuers

Issuers must adhere to the following policies for development, review, and approval for marketing, advertising, and public relations materials, developed for or in conjunction with AEGNS.

2.10.8.1 Brand Advertising

Only American Express Entities may conduct "brand advertising" (i.e., advertising in support of the American Express Brand in general rather than of specific products or services).

2.10.8.2 Incentive Programs

Issuers may offer incentives to their Cardmembers, such as reward points, to use a particular Card. Incentive programs must follow the requirements set out in Section 2.2.10.1, "General Advertising Policies," on page 16. If Issuers use MCC data to fulfill Cardmember incentives based on industry spend, Issuers are advised to review the practices described in Section 2.2.7, "Systems Development and Maintenance," on page 14 and to refer to the *Industry Spend-Based Incentive Program Guidelines* located on Knowledge Base. Issuers are responsible for ensuring that communications to Cardmembers regarding such programs are accurate based upon the data obtained from the AEGN.

2.10.8.3 Issuer Eligible Marketing Region

Issuers generally may not advertise, promote, or market Cards or engage in the Card issuing business in any geographic territory other than the Territory specified in the Participant Agreement. If an Issuer markets Cards on the Internet, any such marketing or advertising shall clearly state that applicants for such Cards must be residents of the country or Territory in which such Issuer is licensed to issue Cards. This restriction shall not be construed to prohibit Issuers in the European Union/European Economic Area and United Kingdom from concluding passive sales within the EU/EEA & UK (regarding which, for purposes of definition only, reference should be made to the guidelines to EC Regulation 330/2010).

2.10.9 Recurring Billing Cancellation Service Requirements

The Recurring Billing Cancellation Service uses the information obtained from participating Issuers to block cancelled Recurring Billing Transactions.

The participating Issuer may use the Recurring Billing Cancellation Service when the Cardmember revokes consent to process Recurring Billing Transactions from that S/E on the Card and either:

- The Cardmember made a reasonable attempt to notify the Recurring Billing S/E that the Cardmember revoked their consent to process Recurring Billing Transactions from that S/E on their Card, or
- If local laws or regulations prohibit requiring the Cardmember to contact the Recurring Billing S/E, then the Cardmember's Issuer should make a reasonable attempt to notify the Recurring Billing S/E on behalf of the Cardmember.

The Recurring Billing Cancellation Service uses the information obtained from Issuers that participate in the service to block cancelled Recurring Billing Transactions that contain the appropriate indicator at Authorization and Presentment.

Following notification by the Issuer of a Recurring Billing cancellation, AEGNS will generate a decline Authorization Response to an Authorization Request or a reject for a Presentment where the Recurring Billing Transaction details match the cancellation instructions provided by the Issuer.

AEGNS will have no liability to an Issuer for declining or rejecting Recurring Billing Transactions as a result of the Issuer's participation in the Recurring Billing Cancellation Service. The Network will decline matching Transactions even when the Issuer is available as the Recurring Billing Cancellation Service is not limited to Stand-In processing. Refer to Section 1.6.9, "Exception File," on page 8 for more information on the Recurring Billing Cancellation Service.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.10 Conversion Rates

In cases in which the Cardmember's billing currency differs from the Participant's settlement currency with the Network, the Issuer shall convert such amounts for billing in the Authorized Currency at rates (including all mark ups) no less favorable on average to the Cardmember than the conversion rates used by the Issuer's major card competitors.

2.10.11 Transfer or Conversion of Card Portfolio

An Issuer must not transfer a Card portfolio, in whole or in part, to any third party (other than a subsidiary which is 100% owned by it) without the prior written consent of AEGNS. In the event an Issuer wishes to transfer a Card portfolio or any Card Accounts to such a 100%-owned subsidiary, it may do so upon sixty (60) days prior written notice, but only on the express conditions that:

- Such 100%-owned subsidiary must meet all the requirements set forth in the applicable Participant Agreement and in the AEGN Manuals, and otherwise be capable of performing the obligations of the applicable Issuer thereunder, and
- The Issuer guarantees and shall remain liable for the full performance and payment by such subsidiary of any and all obligations under the applicable Participant Agreement. An Issuer shall be permitted to transfer Cards and Card Accounts pursuant to this section no more frequently than once per year.

Any other entity to which an Issuer wishes to transfer a Card portfolio or Card Accounts must meet AEGNS' requirements and enter into a Participant Agreement with an American Express Entity.

For as long as its Participant Agreement is in effect, an Issuer shall not convert or attempt to convert or attempt to convert its American Express Card portfolio, in whole or in part, to any other network product. For the avoidance of doubt, Issuers are not prevented from issuing or marketing other network products; from accepting an application from any Person to obtain another network product or honor a request from a Cardmember to have a Card replaced with another network product issued by the Issuer; or from offering another network product to a Cardmember wishing to cancel a Card.

2.10.12 Participation in Securitization Programs

An Issuer is not prohibited from establishing or utilizing an asset-backed securities financing program relating to Charges arising prior to (or, subject to meeting the conditions stated in this section, after) the expiration or termination of its Participant Agreement on the following conditions:

- Issuer's participation in such program in accordance with its terms will not reasonably be expected to or actually result in a breach by the Issuer of its obligations under its Participant Agreement, and
- Issuer complies with paragraphs below.

An Issuer (or a related entity) shall at all times be responsible for management, administration and operation of its Card Issuing Business, and for servicing and collecting the receivables, in each case in accordance with the terms of its Participant Agreement and the AEGN Manuals (except upon a transfer of its servicing duties under the securitization program resulting from a service default thereunder, provided that the Issuer shall notify AEGNS in writing of any such service default immediately).

No Charges shall be subject to such securitization program, unless AEGNS has received full payment from the Issuer with respect thereto.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.13 American Express SafeKey Issuer Requirements

SafeKey is an industry-standard Authentication tool that, when employed by Issuers, Cardmembers, Acquirers, and S/Es, provides greater security for Transactions. Issuers must comply with the following requirements:

- AEGNS strongly recommends that all Issuers support SafeKey.
- Issuers not yet certified for SafeKey must submit a request to AEGNS that their SafeKey-eligible BINs are setup for SafeKey Attempts.
- Issuers in designated countries must support SafeKey in accordance with the following table:

Table 2-18. Issuer SafeKey Support Requirements

Region	Country
APAC	Australia, Bangladesh, Cambodia, Hong Kong (Special Administrative Region of China), India[1], Indonesia, Macao (Special Administrative Region of China), Malaysia, New Zealand, Philippines, Republic of Korea (South Korea), Singapore, Taiwan (Republic of China), Thailand, Vietnam
EMEA	European Union/European Economic Area (EU/EEA) and United Kingdom (UK)

1. SafeKey 2.0 is required for India in October 2023.

SafeKey Certification

- Prior to enabling SafeKey for their Cardmembers, Issuers must complete Certification according to the SafeKey specifications as described in the *American Express SafeKey Protocol Specifications*. Refer to the Network Specifications manuals and the *American Express SafeKey Guidelines* for more information.
- Issuers must comply with all SafeKey-related requirements contained in the American Express SafeKey Protocol Specifications, American Express SafeKey Issuer Implementation Guides, *American Express SafeKey Guidelines*, the *Business and Operational Policies* manual, and the Network Specifications manuals.
- Issuers must use a certified ACS provider. See www.amexenabled.com for a list of certified ACS providers.

SafeKey Issuer/Cardmember Requirements

- Issuers must notify Cardmembers of the availability of SafeKey and encourage Cardmembers to use SafeKey for eligible products.
- The American Express Verification Value (AEVV) must be recalculated and validated by the Issuer during the authorization process. Additionally, Issuers must be able to associate the Authentication and Authorization through the use of the AEVV.
- Issuers must work with their Partner Managers when requesting new/updating existing BINs to determine/confirm SafeKey-eligible Card products.
- Issuers may not enable SafeKey on a product where the Issuer has no means of contact with the user conducting a Transaction. Typically, this includes, but is not limited to, most Prepaid Cards, Gift Cards, and selected commercial products, such as the Business Travel Account.
- AEGNS recommends that Issuers maintain a log for at least two (2) years of all Authentication Data.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.10.14 Network Processing Requirements for U.S. and Canadian Issuing Participants

2.10.14.1 Automated Address Verification (AAV)

Automated Address Verification (AAV) is a Network service required of all U.S. and Canadian Issuers. When an S/E submits Cardmember address information in the POS Authorization Request (1100) message, the U.S./Canadian Issuer is required to validate the address information and submit the result in the POS Authorization Response (1110) message. AAV validation during Stand-In processing is not available. Refer to Section 5.10.1.1, "Automated Address Verification," on page 262 for details regarding this service.

2.10.14.2 Name and Address Verification (NAV) Program

The Name and Address Verification Program is a Network program required of all U.S. and Canadian Issuers. Each U.S. and Canadian Issuer is required to provide access to a call center with a toll-free number to allow U.S. and Canadian S/Es to contact the Issuer (via the S/E's Acquirer) and confirm name and address information from an Issuer representative. Refer to Section 5.10.1.2, "Name and Address Verification (NAV) Program," on page 262 for details regarding this program.

2.10.14.3 ZIP Code Verification (ZCV) Program

The ZIP Code Verification Program (ZCV) allows participating S/Es to submit the Cardmember's billing address ZIP code as part of the Authorization Request for Issuer validation as an additional fraud prevention measure. Refer to Section 4.2.20.5, "ZIP Code Verification (ZCV) Program," on page 233 for details regarding this program.

2.11 AEGNS' Right to Terminate or Suspend Participant Agreement and/or Authorized Activities

2.11.1 Conditions for Immediate Termination or Suspension

In addition to the termination rights set out in the Participant Agreement, AEGNS may terminate or suspend, immediately upon notice to the Participant, the Participant Agreement and/or license to conduct authorized activities under the following conditions:

- If the Participant fails to pay any sum owing under the Participant Agreement at any time outstanding where, following AEGNS' request for payment, the Participant has failed to honor such request within three (3) days of the date of the request;
- If the Participant fails to satisfy any payment obligation owed to a third party set forth in the Participant Agreement, subject to any cure period specified with respect to such obligation;
- If the Participant is, or otherwise admits that it has become, unable to pay its debts as they become due, or if the Participant becomes the subject of any bankruptcy, insolvency or similar proceedings, whether voluntary or involuntary, or a receiver or similar official is appointed for all of any substantial part of the Participant's assets;
- If the Participant fails at any time to satisfy any of the requirements set out in Section 2.2, "General Requirements for AEGN Participants," on page 11 and:
  - The failure is not capable of being cured within ninety (90) days from the occurrence of such failure, or
  - If capable of being cured, such failure has not been cured within ninety (90) days of the notice from AEGNS, requiring remedy of the failure and indicating that AEGNS intends to suspend or terminate the Participant Agreement or license to conduct authorized activities if the failure is not cured;

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- If the Participant fails to use commercially reasonable efforts to correct deficiencies identified in any financial or operational audit conducted pursuant to Section 2.2.17, "Audit Rights," on page 26 or, despite the use of such commercially reasonable efforts, a material deficiency identified in any such audit remains uncorrected 180 days following the completion of such audit;
- If the Participant fails to maintain in effect and enforce effective policies, procedures and internal controls to maintain regulatory compliance including those in the areas of money laundering and terrorist financing (as determined by AEGNS as the result of an audit or otherwise), or if the Participant fails to implement and maintain improvements to such policies, procedures or internal controls, as specified by AEGNS, and such failure has not been cured within thirty (30) days of the notice from AEGNS, requiring remedy of the failure and indicating that AEGNS intends to suspend or terminate the Participant Agreement or license to conduct authorized activities if the failure is not cured; or
- If AEGNS reasonably believes that the Participant is engaging in, or is facilitating or obscuring, any money laundering, terrorist financing activities, or other illegal activities, or is assisting any entities that attempt to or engage in such activities, and such activity has not been cured within thirty (30) days of the notice from AEGNS, requiring remedy and indicating that AEGNS intends to terminate the Participant Agreement or license to conduct authorized activities if the failure is not cured.

2.11.2 Conditions for Termination or Suspension Upon Thirty (30) Days' Notification

In addition to the termination rights set out in the Participant Agreement, AEGNS may terminate or suspend, upon thirty (30) days' notice to the Participant, the Participant Agreement and/or license to conduct authorized activities under the following conditions:

- If the Participant fails to provide or maintain in effect collateral in accordance with the Participant Agreement, or
- If the licensed authorized activity is discontinued for more than five (5) months.

2.12 Expiration or Termination of the Participant Agreement

2.12.1 Expiration/Termination of Acquirer Participant Agreement

From and after the expiration or termination of an Acquirer's Participant Agreement, in addition to those set out in the Participant Agreement, the following are the Acquirer's and AEGNS' continuing obligations.

2.12.1.1 Acquirer's Continuing Obligations

- The Acquirer is prohibited from soliciting and signing S/Es.
- The Acquirer must continue to accept charges from and pay S/Es as well as provide all processing services in accordance with performance measures and standards until AEGNS or its designee can make adequate arrangements for business continuation.
- The Acquirer must provide AEGNS or its designee with updated information on all local S/Es affiliated under the Participant Agreement, including names and addresses, payment and Chargeback history, for two (2) years preceding the date of providing the updated master file (including S/Es by Merchant category, S/E number, and Merchant Discount).
- Upon AEGNS' written request, the Acquirer must take the steps necessary to assign and transfer all its rights and obligations under designated agreements with local S/Es to AEGNS or its designee.
- Upon AEGNS' written request, the Acquirer must re-assign designated S/Es back to AEGNS or its designee together with the master file for all such S/Es (including S/Es by Merchant category, S/E number, and Merchant Discount).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- The Acquirer must return to AEGNS or its designee all documents, manuals, lists, and other documents and data (and all copies thereof) of any type containing confidential or proprietary information of AEGNS.
- The Acquirer must render all assistance and cooperation necessary to enable AEGNS or its designee to register with the relevant industry groups in the licensed market in order to permit AEGNS or its designee to perform the services.

2.12.1.2 AEGNS' Continuing Obligations

- AEGNS or its designee shall continue to accept charges made on Cards at local S/Es (and Multinational Accounts (MNAs), if applicable) in the licensed market and presented to AEGNS or its designee by the Acquirer during the period defined under Section 2.12.1.1, "Acquirer's Continuing Obligations," on page 121, and to settle for them in accordance with the conditions stated in the Participant Agreement.
- AEGNS or its designee shall continue to maintain all the technological, operational, and organizational infrastructure necessary for the Acquirer to provide processing services during the period defined under Section 2.12.1.1, "Acquirer's Continuing Obligations," on page 121.
- AEGNS or its designee shall cooperate fully to effect the assignment of agreements with local S/Es to AEGNS or its designee.

2.12.2 Expiration/Termination of Issuer Participant Agreement

From and after the expiration or termination of an Issuer's Participant Agreement, in addition to those set out in the Participant Agreement, the following are the Issuer's and AEGNS' continuing obligations.

2.12.2.1 Issuer's Continuing Obligations

After expiration or termination of its Participant Agreement, an Issuer shall comply with and be subject to the following requirements:

- Issuer shall cease the issuance of any new Cards, and shall not renew any outstanding and issued Cards. Issuer shall notify their Cardmembers that all Cards will no longer be effective from the time determined in accordance with this section, or as otherwise directed by AEGNS.
- Issuer may promptly cancel all outstanding and issued Cards, provided that Issuer does so in accordance with applicable legal requirements. If AEGNS determines that there will be financial risk to American Express or an American Express Entity or other Acquirers arising from the Issuer's Cards, AEGNS shall have the right to immediately suspend or terminate acceptance of such Issuer's Cards at S/Es and ATMs and other cash access locations.
- For a period of six (6) months following the expiration of the last outstanding Card, Issuer will be obligated to:
  - Continue accepting and paying for Charges, Cash Advances, ATM, and other cash access Transactions on its outstanding and issued Cards, and paying all amounts required to be paid pursuant to its Participant Agreement, and
  - Continue servicing and processing outstanding and issued Cards in accordance with the required servicing standards, in each case until all Charges, Credits, and amounts due have been processed and settled.
- If Issuer is unable to continue servicing and processing its outstanding and issued Cards, Issuer will direct any third-party vendor(s) and processors it uses for its Cardmember servicing to continue to service and process such Cards on behalf of AEGNS or its designee at Issuer's expense. Alternatively, Issuer will provide AEGNS or its designee with all necessary information and cooperation so that AEGNS or its designee can provide servicing and processing for such Cards, at Issuer's expense, up to the time of the cancellation or expiration of all of Issuer's outstanding and issued Cards.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.12.2.2 S/E Payables

From and after the expiration of an Issuer's Participant Agreement, to the extent AEGNS assumes and pays any of the S/E payables arising from the Issuer's Cards, and/or incurs any expenses servicing and/or processing the Issuer's Cards, AEGNS shall be entitled to recoup and offset the amounts of such payables and expenses against any amounts owed by AEGNS or any American Express Entity to the Issuer and in addition AEGNS shall be entitled to any and all accounts receivable of the Issuer to the extent arising from such payables whether billed by the Issuer or not. Each Issuer hereby assigns such accounts receivable to AEGNS and holds AEGNS harmless against any non-payment by such Issuer's Cardmembers. Issuers shall undertake to perfect AEGNS' rights in such receivables and to cooperate with AEGNS by providing AEGNS the necessary information and other reasonable assistance as requested by AEGNS to enable AEGNS to collect such receivables. Provided, however, that, subject to the Issuer's compliance with Section 2.10.12, "Participation in Securitization Programs," on page 118 of this AEGNS manual, nothing in this section shall authorize AEGNS to assert entitlement to any amounts beneficially owed to a Person other than the Issuer on account of a securitization program.

2.12.2.3 AEGNS Rights Upon Termination/Expiration

Anything herein to the contrary notwithstanding, in the event that AEGNS, in the exercise of its reasonable business judgment, determines that there will be financial exposure to AEGNS or American Express Entities arising from an Issuer's Cards upon and/or after expiration or termination of the Issuer's Participant Agreement, AEGNS shall have the right to immediately suspend or terminate acceptance of such Issuer's Cards at S/Es and ATMs and other cash access locations and to draw down any letter of credit or cash collateral, or enforce any guaranty provided by the Issuer, in addition to all other rights and remedies of AEGNS under the Participant Agreement, applicable law and equity.

2.12.2.4 AEGNS' Continuing Obligations

After expiration or termination of a Participant Agreement, AEGNS will be obligated to continue providing S/E processing and administering Chargebacks for the Issuer's Cards that have been issued in accordance with the applicable Participant Agreement until such Cards are cancelled or expire (without any renewal of the Cards, as provided in Section 2.12.2.1, "Issuer's Continuing Obligations," on page 122).

2.13 Operating Policy Compliance and Enforcement

Failure to comply with the policies in the *Business and Operational Policies* manual or related specifications and manuals may adversely affect Cardmembers, Participants, the American Express Brand, or undermine the integrity of the AEGNS Network. AEGNS reserves the right to enforce adherence to policies using various mechanisms, including the assessment of non-compliance fees.

2.13.1 Non-Compliance Fees

AEGNS may assess fees to Participants for violations of GNS policy documented in the *Business and Operational Policies* manual. Refer to the "Network Fees" chapter beginning on page 401 for additional information on fees.

Some AEGNS Policies have accompanying fee schedules for non-compliance fees. Regardless of whether non-compliance fees are described in a particular policy section, general non-compliance fees, as described in Section 10.7.1, "General Non-Compliance Fees," on page 411, are applicable to all sections of the *Business and Operational Policies* manual.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2.13.2 Determination of Violation

AEGNS may determine a violation of the *Business and Operational Policies* manual has occurred or is occurring by methods including, but not limited to:

- Information based on a response from a Participant to a request for information or other available information.
- Failure of a Participant to respond to a request for information or failure to provide all information requested.
- Monitoring of data or activity on the AEGN.
- The findings of an AEGNS audit, investigation, or questionnaire.

2.13.3 Notification of Violation Process

AEGNS will notify a Participant if it determines that a violation of policy has occurred or if it determines that a violation is continuing to occur. A notification of violation will include a description of the violation and a reference to policy.

2.13.4 Request for Information

AEGNS may request information from a Participant in order to assess adherence to policy or in response to a violation of policy. A Participant must respond to a request for information within the time period specified and by the method specified.

2.13.5 Action Plans

AEGNS may require a non-compliant Participant to complete and submit an Action Plan that is acceptable to AEGNS to address deficiencies. Participants are required to complete the actions in an Action Plan by the dates specified in the plan. AEGNS may periodically request a status update from a Participant for an Action Plan. Participants are required to respond to the request within the time specified by AEGNS along with any supporting Documentation. Failure to respond to requests from AEGNS or failure to complete the actions agreed in an Action Plan by the dates specified may result in AEGNS assessing non-compliance fees as described in Section 10.7.1, "General Non-Compliance Fees," on page 411.

2.13.6 Exceptions

A Participant that is unable to comply with a requirement found in the *Business and Operational Policies* manual or other related documents referenced in Section 1.4, "Related AEGNS Manuals, Guidelines, and Resources," on page 3 must submit a written Exception request to AEGNS. Any such request must specify the requirement for which the Exception is sought.

An approved Exception:

- Applies only to the specific circumstances of the request
- Is valid only to the Participant that submitted the request
- May be subject to conditions
- May have a defined expiration

AEGNS may rescind or amend any Exception upon notification to the Participant.

If a Participant fails to meet the conditions of the Exception, non-compliance fees may apply (see Section 10.7.1, "General Non-Compliance Fees," on page 411). Participants should contact their AEGNS representative for instructions on how to submit an Exception request.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3 Product Features and Specifications

3.1 Introduction

The purpose of this chapter is to inform Network Participants of the minimum requirements for issuing Cards and Accounts (American Express Enterprise Line and Blue Box Line) as well as the recommended features and benefits offered by Issuers and AEGNS for Consumer and Commercial products.

In addition, the chapter provides descriptions of the various features and benefits associated with Cards and Accounts as well as various services offered by Issuers and AEGNS. Refer to Section 1.6, "Network Services," on page 6 for additional information. The chapter also details the conditions under which Participants may issue Co-Brand and Affinity products.

Consult with your AEGNS representative to discuss availability in your market. This chapter does not address any aspects of products and features for Acquirers.

3.2 Overview of Products Supported by the AEGN

This section provides an overview of products available for license and issuance on the Network.

3.2.1 Consumer Cards

Consumer Cards include Charge Cards, Credit Cards, or Debit Cards issued by a bank, financial institution, or other qualified organization pursuant to an Agreement with an American Express Entity, and which bears either the American Express Enterprise Line Card design or the American Express Blue Box logo and is accepted at Service Establishments (S/Es) in payment for Goods and Services. If a chip is installed on the Card, the chip function must meet the GNS Chip Card requirements and specifications. Refer to Section 3.2.7, "Chip Cards," on page 131 and Section 2.10.7, "Chip and Contactless Card Requirements," on page 115 for additional information.

There are two (2) different categories of licenses that are available to Issuers, American Express Enterprise Line Cards and Blue Box Line Cards, which are described below. AEGNS has the sole discretion to determine what types of Cards Issuers will be licensed to issue.

Before being licensed to issue a specific Card, Issuers must sign a Participant Agreement for the particular Card, and agree to meet all standards as detailed in this chapter. In addition, the Issuer must comply with the Card design guidelines as described in the Network Specifications manuals and the Card Design Guidelines manuals located in the Marketing section on Knowledge Base. The Issuer must submit all Card designs, communications materials and collateral, as well as all advertising and media, for review and approval to their AEGNS representative before Card production and distribution in a market. Refer to Section 2.2.10.2, "Advertising and Marketing Review Requirements," on page 18.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.2.1.1 American Express Enterprise Line Consumer Cards

American Express Enterprise Line Consumer Cards follow the established Card design, positioning, and core features set out in American Express Card design and marketing guidelines. American Express Enterprise Line Consumer Cards must not be marketed in any manner that might suggest that the Card is issued by an American Express Entity.

The American Express Enterprise Line Consumer Cards are:

- The American Express® Card (green)
- The American Express® Gold Card
- The Platinum Card®
- The Centurion® Card
- The American Express® Credit Card (Blue)
- Blue from American Express®
- The American Express® Credit Card (green)
- The American Express® Gold Credit Card
- The American Express® Platinum Credit Card
- The American Express® Debit Card

3.2.1.2 Blue Box Line Consumer Cards

All Blue Box Line Consumer Cards must meet minimum Card product requirements as described in this chapter. The Card design and positioning may be tailored to meet target customer needs. Blue Box Line Cards must not be marketed in any manner that might suggest that the Card is issued by an American Express Entity.

The Blue Box Line Consumer Cards are:

- [Issuer Name] American Express® Card (Member)
- [Issuer Name] Select American Express® Card
- [Issuer Name] Max American Express® Card or [Issuer Name] Black American Express® Card
- [Issuer Name] Icon American Express® Card
- [Issuer Name] American Express® Generation Card
- [Issuer Name] American Express® Debit Card

3.2.2 Commercial Products

Commercial Products are those Cards or Accounts designed for use by both small and large businesses. They are grouped into two (2) types:

- Small Business Products, aimed at businesses with fewer than 50 employees; and
- Corporate Products, aimed at businesses with 50 or more employees.

Within Corporate Products, there are two (2) different levels of product functionality, Standard and Enhanced. Issuers will be informed by their GNS Corporate Account Management representative which level of specification applies to them. Please note that both the Standard and the Enhanced specifications represent only the minimum functionality that must be offered; Issuers may choose to offer a higher level of functionality, where this will better meet customer needs.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Whereas most Commercial Cards are designed to be carried by an individual and physically presented to make purchases, some Commercial Products are designed to be issued in the name of a company or department, and used to make purchases on behalf of multiple employees. These may be known as "Accounts" rather than "Cards."

Such products are used primarily for Card Not Present Transactions and may be offered as Cardless Accounts. These may take the form of an Account number on file with a travel agency and used to charge travel expenses on behalf of the client.

Cardless Accounts can provide increased convenience and security because the physical presence of the Card is not required. They are intended for use with a single or defined group of S/Es rather than for general, all-purpose spending.

For both the American Express Enterprise Line and Blue Box Line, Commercial Accounts may be offered as Small Business Products or as Corporate Products. Examples of Commercial Accounts are the Business Travel Account and the Travel Agency Account.

Before being licensed to issue a specific Commercial Product, Issuers must agree to meet all standards for the particular Product as detailed in this chapter. Issuers must also agree to follow the Card design guidelines as described in the Marketing section of Knowledge Base. The Issuer will submit all Card designs, collateral, and advertising for review by their AEGNS representative before production. Refer to Section 2.2.10.2, "Advertising and Marketing Review Requirements," on page 18.

3.2.2.1 American Express Enterprise Line Commercial Products

American Express Enterprise Line Commercial Products follow the established Card design, positioning, and core features set out in American Express Card design and marketing guidelines.

The American Express Enterprise Line Commercial Products are:

- Small Business Products
  - The American Express® Business Card
  - The American Express® Business Gold Card
  - The American Express® Business Platinum Card
  - The Business Centurion® Card
  - American Express® Travel Agency Account
  - American Express® Business Debit Card
- Corporate Products
  - American Express® Corporate Card
  - American Express® Corporate Gold Card
  - American Express® Corporate Platinum Card
  - American Express® Corporate Purchasing Card
  - American Express® Business Travel Account
  - American Express® Corporate Meeting Card

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.2.2.2 Blue Box Line Commercial Products

Commercial Products issued on a Blue Box Line must meet minimum requirements as described in this chapter. The Card design and positioning may be tailored to meet target customer needs. Blue Box Line Products must not be marketed in any manner that might suggest that the Product is issued by an American Express Entity.

The Blue Box Line Commercial Products are:

- Small Business Products
  - [Issuer Name] Member Business American Express® Card
  - [Issuer Name] Select Business American Express® Card
  - [Issuer Name] Max Business American Express® Card
  - [Issuer Name] Icon Business American Express® Card
  - [Issuer Name] American Express® Business Purchasing Card
  - [Issuer Name] American Express® Travel Agency Account
  - [Issuer Name] American Express® Business Debit Card
- Corporate Products
  - [Issuer Name] Corporate American Express® Card
  - [Issuer Name] Gold Corporate American Express® Card
  - [Issuer Name] Platinum Corporate American Express® Card
  - [Issuer Name] American Express® Business Travel Account

3.2.3 Account Card

Account Card functionality enables a Card to be linked to an asset account (for example, current account, deposit account) whereby a Charge is deducted from the asset account on a delayed basis, generally fifteen (15) days after the Transaction Date.

Account Card functionality can be applied to existing Consumer or Small Business products within the Centurion or Blue Box line, or can be issued as a separate and distinct American Express Enterprise Line or Blue Box Line Card product. The Account Card proposition may be tailored to meet target customer needs in accordance with product line guidelines and minimum product requirements.

3.2.3.1 Minimum Product Requirements for Account Card

If the Account Card is issued as a separate and distinct Centurion or Blue Box Line product, the Account Card must meet the minimum Card product requirements as listed below:

- Account Cards must be issued in a separately identifiable 6-digit BIN range. Individual products can be defined at the seventh- or eighth-digit level.
- Issuers of Account Card must provide Cardmembers with the ability to obtain a current Card balance in real-time during normal business and non-business hours (24 hours per day 365 days per year).
- Issuers of Account Card must provide Cardmembers with Emergency Assistance services at the basic level (Tier 1).
- The Account Card Issuer must offer a Cardmember loyalty program. It must be an Issuer or third-party rewards program on a Blue Box product or a Membership Rewards or cashback program on an American Express Enterprise Line product.
- Issuers of Account Card must comply with the Account Card Design and Communication Guidelines and all other applicable manuals located in the Marketing section on Knowledge Base.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

If the Account Card functionality is associated with any of the existing Card products defined in the following tables, then the minimum requirements for those Card products will apply in addition to the Account Card requirements listed above:

- Table 3-1, "Features and Benefits for American Express Enterprise Line Consumer Cards," on page 133
- Table 3-3, "Features and Benefits for American Express Enterprise Line Commercial Corporate Products," on page 161
- Table 3-4, "Features and Benefits for Blue Box Line Consumer Cards," on page 170
- Table 3-5, "Features and Benefits for Blue Box Line Small Business Commercial Products," on page 177

3.2.4 Dual Card Account

A Dual Card Account (Blue Box Line only) is an account accessible by two (2) distinct card products, a Blue Box Line Card and a card accepted on another payment network. A Dual Card Account features a single line of credit, one monthly statement, one (1) set of terms and conditions, one (1) annual account fee, and one (1) rewards/mileage pool. Dual Card Accounts may be offered as a Credit Card product only.

The following American Express-branded Blue Box Line products may be linked to Dual Card Accounts:

- Blue Box Line Consumer Cards
  - [Issuer Name] American Express® Card (Standard)
  - [Issuer Name] Gold American Express® Card
  - [Issuer Name] Platinum American Express Card®
  - [Issuer Name] Black American Express® Card
  - [Issuer Name] American Express® Generation Card
- Blue Box Line Commercial Products
  - [Issuer Name] Business American Express® Card
  - [Issuer Name] Gold Business American Express® Card

For additional details, please refer to the *Dual Card Account Marketing Requirements Guide* on the Marketing page of Knowledge Base.

3.2.5 Prepaid Cards

A Prepaid Card is one for which a monetary value is pre-loaded onto the Card. Prepaid Cards can be issued to Consumer or Commercial customers. In addition to the convenience of carrying a Card instead of cash, ease of use and wide acceptance, Prepaid Cards offer a flexible payment alternative in the form of travel cards, gift cards, incentive cards, payroll cards, teen cards, etc.

These Cards must meet minimum Card product requirements as described in this chapter. The Card design and positioning may be tailored to meet target customer needs, in accordance with product line guidelines. Prepaid Cards must not be marketed in any manner that might suggest the Card is issued by an American Express Entity. Prepaid Cards may be issued by AEGNS Issuers or any other entity with which AEGNS enters into an agreement for the issuance of a Prepaid Card. All Prepaid products must be marked "Prepaid" above the Blue Box on the back of Prepaid Cards in accordance with American Express' branding and style guidelines. Issuers of Prepaid Cards may, at their discretion, display the word "Prepaid" above the Blue Box on the front of the Card, in addition to (but not in lieu of) the required elements on the back of the Prepaid Cards as set forth in the preceding sentence.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.2.5.1 Types of Prepaid Cards

Prepaid Cards may be issued as reloadable or non-reloadable Cards. A reloadable Prepaid Card allows for replacement or additional funds to be added onto the Card until the Expiration Date of the Card. Funds cannot be added onto a non-reloadable Prepaid Card once the initial monetary Load is depleted.

Non-reloadable Prepaid Cards are typically issued as anonymous Cards, such as gift Cards, which are low-value denominated, have no ability to draw cash, and may be restricted for use in their country of origin. Both reloadable and non-reloadable Prepaid Cards may be issued as personalized or non-personalized Cards.

Some Prepaid Cards may be issued as Contactless Prepaid Cards. These Cards are issued with a chip containing an Expresspay Application that facilitates Contactless Transactions when the Cards are used at an Expresspay-enabled POS Device.



Prepaid Cards can vary substantially in how they operate, and in the value and functionality provided to the Cardmember. For example, an Issuer may restrict the usage of the Card to certain countries, industry segments, or at ATMs.

3.2.5.2 U.S. Multi-Network Prepaid Cards

A U.S. Multi-Network Prepaid Card is a Prepaid Card that is a "debit card" as defined in the Federal Reserve Board Regulation II, 12 CFR Part 235. Participants must comply with all applicable laws as stated in Section 2.2.1, "Initial Eligibility Requirements for Participants," on page 11, and the standards set out herein.

3.2.5.3 General Requirements for Issuers of Prepaid Cards

Issuers are responsible for advising Cardmembers of their policies regarding the usage of Prepaid Cards for pre-authorized Transactions (e.g., hotels, car rentals, and gas stations), Mail/Telephone/Internet Transactions, and Recurring Billing Transactions. AEGNS is not responsible for enforcing any usage restrictions that an Issuer places on a Prepaid Card. Before being licensed to issue Prepaid Cards, Issuers must agree to meet all standards for the particular Card as detailed in this chapter. Issuers must also agree to follow the Card design guidelines as described in the Network Specifications manuals. AEGNS recommends that all Prepaid Card Issuers advise their Cardmembers that some Prepaid Cards may not be accepted in the EU/EEA & UK.

Participants are responsible for maintaining an effective AML/ATF program for all Prepaid Cards in accordance with Section 2.3.4, "AML/ATF Requirements for All Prepaid Cards," on page 34. For Prepaid Card product development, Participants should contact their AEGNS representative.

Monthly statements are not required, but Issuers must provide Cardmembers with the ability to obtain a current Card balance during normal business and non-business hours. Issuers must also comply with ad hoc Cardmember requests for a statement of charges. Issuers are required to provide Cardmembers with emergency funds replacement within twenty-four (24) hours of being notified by the Cardmember of the loss of his Card.

Prepaid Cards must be issued in a separately identifiable 6-digit BIN range. Individual products can be defined at the seventh- or eighth-digit level. Issuers must allocate a separate BIN sub-range for Anonymous Non-Reloadable Prepaid Cards.

Issuers must ensure ISO 7813 track data contains a Service Code that, when interrogated by a POS device, instructs the device to request Authorization from the Issuer. AEGNS is not responsible for ensuring that Service Establishments are able to act on and interrogate Service Codes, and Issuers remain financially responsible for these Transactions, provided the Service Establishment has followed Card acceptance procedures as outlined in the "S/E and ATM Standards" chapter beginning on page 214.

Note: In order to take advantage of the services offered by Issuers of Prepaid Cards (e.g., replacement of lost/stolen Cards, Issuer-provided fraud protection, etc.), Cardmembers may be required to activate and/or register their Prepaid Cards.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.2.5.4 Prepaid Card Functionality

Prepaid Card Issuers must support the following Authorization-related functionality, unique to Prepaid Cards, as described below:

- For all non-reloadable, anonymous Prepaid Cards, Issuers must support:
  - Prepaid Card Partial Authorization with Balance Return - to enable Split Tender Transactions
  - Prepaid Card Authorization with Balance Return
  - Prepaid Card Balance Inquiry
- For all reloadable, Prepaid Cards, Issuers:
  - Must support Prepaid Card Partial Authorization with optional Balance Return - to enable Split Tender Transactions
  - May support Prepaid Card Authorization with Balance Return
  - May support Prepaid Card Balance Inquiry

In order to support this functionality, Participants must be certified by AEGNS. Refer to Section 5.3.3, "Prepaid Card Authorization Processing," on page 248 for additional information on Authorization-related requirements for Prepaid Cards.

3.2.6 Debit Cards

A Debit Card is any Card that accesses a demand deposit, current, savings, or other similar account. Debit Cards must be issued in a separately identifiable 6-digit BIN range. Individual products can be defined at the seventh- or eighth-digit level.

3.2.6.1 U.S. Multi-Network Debit Cards

A U.S. Multi-Network Debit Card is a Debit Card that is a "debit card" as defined in the Federal Reserve Board Regulation II, 12 CFR Part 235. Participants must comply with all applicable laws as stated in Section 2.2.1, "Initial Eligibility Requirements for Participants," on page 11, and the standards set out herein.

3.2.6.2 General Acceptance Requirements of Debit Cards

For Debit Cards, Acquirers are responsible for following acceptance policies outlined in the "S/E and ATM Standards" chapter beginning on page 214.

3.2.7 Chip Cards

Chip Cards can be issued for both Consumer and Business/Corporate customers.

American Express supports two (2) types of Chip Card terminal applications, AEIPS and Expresspay (Contactless).

Chip Cards must meet the specifications described in the AEIPS Chip Card Specifications, *AEIPS Terminal Technical Manual*, Expresspay Card Specifications, and Expresspay Terminal Specifications. These documents contain the AEGNS version of the EMV specification. Specifications include:

- Card specifications
- Personalization
- Issuer Host System
- Security

Refer to Section 2.10.7, "Chip and Contactless Card Requirements," on page 115 for more information.

Note: Issuers in designated countries must issue Expresspay Cards. Refer to Section 2.10.7.5, "AEIPS and Expresspay Enablement Program for Issuers," on page 116 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.2.7.1 AEIPS-Based Payments

In the case of an AEIPS-based payment, a chip-enabled Card is inserted into a Chip-Enabled Device, followed by an Authorization Response being returned based on the interaction between the Card and the terminal.

3.2.7.2 Contactless Cards (Expresspay)

Issuers of Contactless Cards are required to adhere to the following requirements:

- Acceptance marks on Cards issued by a Participant.
  - Card must be compliant to existing AEGNS Card design rules.
- AEGNS Issuer/Co-Brand Card Design.
  - Cards must be compliant to all existing AEGNS Card design rules. The following symbol will be required on all new Contactless Card designs:



- Issuer and co-brand Participants may not place any brand that relates specifically to the Contactless feature on the Card, other than Expresspay.

Note: Participants in designated countries must issue Expresspay Cards. Refer to Section 2.10.7, "Chip and Contactless Card Requirements," on page 115.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3 American Express Enterprise Line Consumer Cards

Table 3-1, "Features and Benefits for American Express Enterprise Line Consumer Cards," on page 133 summarizes the required and recommended features and benefits for American Express Enterprise Line Consumer Cards.

Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards

Product Feature	American Express® Card (green)	American Express® Gold Card	The Platinum Card®	The Centurion® Card	Blue from American Express®	American Express® Credit Card (green)	American Express® Gold Credit Card	American Express® Platinum Credit Card	American Express® Debit Card
Payment Functionality	Charge or Revolve	Charge or Revolve	Charge	Charge	Revolve	Revolve	Revolve	Revolve	Debit
Minimum Credit Limit (where applicable)	-	-	-	-	-	Required	Required	Required	-
Cash Access	Required	Required	Required	Required	Required	Required	Required	Required	Required
Direct Debit of Monthly Balance or Minimum Payment	Required	Required	Required	Required	Required	Required	Required	Required	-
Card Portfolio									
Linked Portfolio Requirement (existing portfolios required before issuing new product)	-	-	Required	Required	-	-	-	-	-
Metal Form Factor	-	-	Recommended	Required	-	-	-	-	-
Portfolio Size	-	-	Required	Required	-	-	-	-	-
Basic Card	Required	Required	Required	Required	Required	Required	Required	Required	Required
Supplementary Cards	Recommended	Recommended	Required	Required	-	-	-	-	-

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards (continued)

Product Feature	American Express® Card (green)	American Express® Gold Card	The Platinum Card®	The Centurion® Card	Blue from American Express®	American Express® Credit Card (green)	American Express® Gold Credit Card	American Express® Platinum Credit Card	American Express® Debit Card
Acquisition Requirements									
Cardmember Tenure	-	-	-	Required	-	-	-	-	-
Annual Submission of Acquisition Plan	-	-	Required	Required	-	-	-	-	-
Online Card application form	-	-	-	Not allowed	Required	-	-	-	-
Engagement Requirements									
First 100 Days Programs	-	-	Required	Required	-	-	-	-	-
Servicing									
Card Servicing	Required	Required	Required	Required	Required	Required	Required	Required	Required
Travel Servicing	-	-	Required	Required	-	-	-	-	-
Concierge Servicing	-	-	Required	Required	-	-	-	-	-
Third-Party Service Providers	-	-	Approval required	Approval required	-	-	-	-	-
Relationship Manager Servicing (RMS)	-	-	-	Required	-	-	-	-	-
Training	-	-	Required	Required	-	-	-	-	-
Cardmember Online Account Access Service	Required	Required	Required	Required	Required	Required	Required	Required	Required
Local Language Servicing	Required	Required	Required	Required	Required	Required	Required	Required	Required

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards (continued)

Product Feature	American Express® Card (green)	American Express® Gold Card	The Platinum Card®	The Centurion® Card	Blue from American Express®	American Express® Credit Card (green)	American Express® Gold Credit Card	American Express® Platinum Credit Card	American Express® Debit Card
Servicing Assessments and Partner Accreditation	-	-	Required	Required	-	-	-	-	-
Require Customer Relationship Management (CRM) capabilities	-	-	Required	Required	-	-	-	-	-
Implement and Use Premium Product Platform (PPP)	-	-	Required	Required	-	-	-	-	-
Cardmember Loyalty Programs									
Membership Rewards	Required	Required	Required	Required	Not allowed	Not allowed	Not allowed	Not allowed	-
Cashback	Not allowed	Not allowed	Not allowed	Not allowed	Either program required	Either program required	Either program required	Either program required	-
Local Rewards Program	Not allowed	Not allowed	Not allowed	Not allowed					-
Virtual Currency									
Travel Benefits									
Airport Lounge Access	-	-	Required	Required	-	-	-	-	-
Airline Core Benefit Programs	-	-	Required	Required	-	-	-	-	-
Local Airport Benefits	-	-	Required	Required	-	-	-	-	-

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards (continued)

Product Feature	American Express® Card (green)	American Express® Gold Card	The Platinum Card®	The Centurion® Card	Blue from American Express®	American Express® Credit Card (green)	American Express® Gold Credit Card	American Express® Platinum Credit Card	American Express® Debit Card
Private Jet Program	-	-	-	Required	-	-	-	-	-
Global Hotel Program	-	-	Required	Required	-	-	-	-	-
Hotel Partner Loyalty Programs	-	-	Required	Required	-	-	-	-	-
Car Partner Loyalty Programs	-	-	Required	Required	-	-	-	-	-
Cruise Programs	-	-	Required	Required	-	-	-	-	-
Travel Tactical Offers Program	-	-	Required	Required	-	-	-	-	-
Lifestyle Benefits									
Source Local Lifestyle Benefits and Discounts	-	-	Required	Required	-	-	-	-	-
Dining Program	-	-	Required	Required	-	-	-	-	-
Events Program	-	-	Required	Required	-	-	-	-	-
Ticket Access	-	-	Required	Required	-	-	-	-	-
Retail Offers or Services	-	-	Recommended	Required	-	-	-	-	-
Local Benefits	Required	Required	Required	Required	-	-	-	-	-
Protection									
Emergency Assistance	Required	Required	Required	Required	Required	Required	Required	Required	Required

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards (continued)

Product Feature	American Express® Card (green)	American Express® Gold Card	The Platinum Card®	The Centurion® Card	Blue from American Express®	American Express® Credit Card (green)	American Express® Gold Credit Card	American Express® Platinum Credit Card	American Express® Debit Card
Emergency Card Replacement	Required	Required	Required	Required	Required	Required	Required	Required	Required
Limited Liability for Lost/Stolen Cards/Fraud Protection Guaranteed	Required	Required	Required	Required	Required: two (2) of these three (3): • Limited Liability for lost/stolen cards/fraud protection guaranteed • Extended Warranty • Retail Protection Insurance	Required	Required	Required	Required
Extended Warranty	-	-	Required	Required		-	Required	Required	-
Retail Protection Insurance	Required	Required	Required	Required		-	Required	Required	-
Online Fraud Protection Guarantee	-	-	Required	Required	Required	-	-	-	-
Fully Comprehensive Travel Insurance	-	-	Required	Required	-	-	-	-	-
Travel Accident	Required	Required	Included in above	Included in above	-	-	-	-	-
Flight Delay	-	Required	Included in above	Included in above	-	-	-	-	-
Flight Cancellation	-	-	Included in above	Included in above	-	-	-	-	-
Luggage Delay	-	Required	Included in above	Included in above	-	-	-	-	-
Luggage Protection	-	-	Included in above	Included in above	-	-	-	-	-

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards (continued)

Product Feature	American Express® Card (green)	American Express® Gold Card	The Platinum Card®	The Centurion® Card	Blue from American Express®	American Express® Credit Card (green)	American Express® Gold Credit Card	American Express® Platinum Credit Card	American Express® Debit Card
Marketing Communication									
Annual Communications Calendar	Required	Required	Required	Required	Required	-	-	-	-
Publishing Magazine	-	-	-	Required	-	-	-	-	-
Product Website and or Designated Pages	-	-	Required	Required	Required	Required	Required	Required	Required
Adherence to Product Brand Guidelines	Required	Required	Required	Required	Required	Required	Required	Required	Required
Above the Line Advertising (ATL)	-	-	-	Not allowed	-	-	-	-	-
Annual Submission of Marketing Communications/ Engagement Plan	-	-	Required	Required	-	-	-	-	-
Portfolio Management/Reporting									
Dedicated Premium Product Manager	-	-	-	Required	-	-	-	-	-
Benefits and Servicing Reporting	-	-	Required	Required	-	-	-	-	-

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-1. Features and Benefits for American Express Enterprise Line Consumer Cards (continued)

Product Feature	American Express® Card (green)	American Express® Gold Card	The Platinum Card®	The Centurion® Card	Blue from American Express®	American Express® Credit Card (green)	American Express® Gold Credit Card	American Express® Platinum Credit Card	American Express® Debit Card
Quality Measurement Program (for example, Mystery Shopper)	-	-	-	Required	-	-	-	-	-
Annual Customer Satisfaction Survey	-	-	Required	Required	-	-	-	-	-

For more information on the required features and benefits American Express Enterprise Line Consumer Cards, refer to Section 3.3.1 "American Express Card (green)" on page 140 through Section 3.3.8 "American Express Platinum Credit Card" on page 151. For guidance on recommended features, Participants should access the marketing materials in The Orchard on Knowledge Base. Additional benefits, features, and functionality may be available in certain markets.

Please consult your AEGNS representative for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.1 American Express Card (green)

Issuers are required to provide the following minimum features and benefits for the American Express® Card (green):

- Payment Functionality - based on market practices and consumer preference, a Charge Card with no preset spending limit, or a Credit Card. The Credit Card product must offer the option to revolve a balance on a line of credit that is competitive or superior to other products in the same segment.
- Cash Access - with a recommended minimum cash limit that is competitive or superior to other products in the same segment.
- Direct Debit of Monthly Balance or Minimum Payment.

Card Portfolio:

- Basic Card

Servicing:

- Card Servicing
- Cardmember Online Account Access Service
- Local Language Servicing

Cardmember Loyalty Program:

- Membership Rewards
- Not allowed - Cashback or local Merchant awards

Protection:

- Emergency Assistance - Tier 1
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Retail Protection Insurance, which includes Theft and Damage Protection and Return Protection
- Travel Accident Insurance - the coverage level must be competitive or superior to other products in the same segment (minimum $100,000 USD)

Marketing Communication:

- Annual Communications Calendar
- Adherence to Product Brand Guidelines

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.2 American Express Gold Card

Issuers are required to provide the following minimum features and benefits for the American Express® Gold Card:

- Payment Functionality - a Charge Card with no preset spending limit, or a Credit Card. The Credit Card product must offer the option to revolve a balance on a line of credit that is competitive or superior to other products in the same segment.
- Cash Access - with a recommended limit of double the limit available on the American Express® Card (green) and competitive or superior to other products in the same segment.
- Direct Debit of Monthly Balance or Minimum Payment.

Card Portfolio:

- Basic Card

Servicing:

- Card Servicing
- Cardmember Online Account Access Service
- Local Language Servicing

Cardmember Loyalty Program:

- Membership Rewards
- Not allowed - Cashback and local Merchant awards

Protection:

- Emergency Assistance - Tier 2
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Travel Accident Insurance - the coverage level must be twice the level on the American Express® Card (green) and competitive or superior to other products in the same segment
- Retail Protection Insurance, which includes Theft and Damage Protection and Return Protection
- Flight Delay
- Luggage Delay Protection

Marketing Communication:

- Annual Communications Calendar
- Adherence to Product Brand Guidelines

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.3 The Platinum Card

Prior to being licensed to issue The Platinum Card®, the Issuer must meet the following Card issuance prerequisites:

- The Issuer must already issue the American Express® Card (green) and the American Express® Gold Card and must meet the contractually established performance levels as determined from at least one (1) year of issuing experience.
- The Issuer must be in compliance with all AEGNS policies.
- The Issuer must project a minimum Platinum Card base of 1,000 Cards in Force the first year and 5,000 Cards in Force by the fifth year.
- Ensure The Platinum Card® is the most exclusive and superior payment product in the market excluding The Centurion® Card.
- Establish external acquisition channels to target and attract select Affluent customers in the market.
- In markets where The Platinum Card® is the highest level of American Express Card product offered, the Issuer must agree to conduct acquisition via pre-approved applications to its select customers who are:
  - Existing American Express Cardmembers exhibiting annual spend history on their existing Cards of $40,000 (USD) or local socioeconomic equivalent, and/or
  - "Premium" bank customers (e.g., private banking clientele) who have an income of $80,000 (USD) or local socioeconomic equivalent.

Agree to follow the product guidelines in the *Platinum Card Product Guidelines*.

Issuers are required to provide the following minimum features and benefits for The Platinum Card®:

- Payment Functionality - a Charge Card with no preset spending limit

Card Portfolio:

- Plastic or metal form factor options available
- If metal form factor is being made available:
  - Must be in stainless steel with Contactless functionality
  - All new cards must be metal cards
  - All back book Basic Cards must be replaced into metal within twenty-four (24) months to maintain portfolio uniformity
  - Platinum products should be priced at a fee that represents the increased investment for metal
- Portfolio size - Projected Cards in Force (CIF) expectations: First year - 1,000 CIF, Fifth year - 5,000 CIF
- Basic Card
- Supplementary Cards - The Issuer must provide a total of four (4) Supplementary Cards, at no additional cost, as follows:
  - At least one (1) Platinum Card with form factor matching the Basic Card, and
  - Remaining three (3) can be Platinum, Gold, or Green Cards

Acquisition Requirements:

- Annual submission of acquisition plan – American Express approval required one (1) quarter in advance of deployment

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Engagement Requirements:

- First 100 Days Programs – American Express approval needed

Servicing:

- Dedicated Servicing: Card and Concierge. Required twenty-four (24) hours per day, seven (7) days per week, one (1) telephone number, dedicated team
- Dedicated Servicing: Travel. Required core hours and out of hours emergency assistance, one (1) telephone number, dedicated team
- Third-party Service Providers - American Express Vendor approval required
- Training – Continuous Partner Employee Training, and Assessment
- Cardmember Online Account Access Service
- Local Language Servicing
- Servicing Assessments and Partner Accreditation
- Customer Relationship Management (CRM) capabilities
- Implement and use Premium Product Platform (PPP) and/or successor platforms. Fees apply. Refer to Section 10.5.11, "Premium Product Platform (PPP) Fees," on page 409"

Cardmember Loyalty Program:

- Membership Rewards
- Not allowed - Cashback and local Merchant awards

Travel Benefits:

- Airport Lounge Access - American Express Global Lounges and unlimited complimentary access to Priority Pass for Basic Cardmember
- Local Airport Benefits – Include benefits such as Airport Fast Track, Meet and Greet Services, complimentary valet parking
- Airline Core Benefit Programs – International Airline Program
- Global Hotel Program – FHR (Fine Hotels and Resorts) and THC (The Hotel Collection)
- Hotel Partner Loyalty Programs, Card Partner Loyalty Programs, Cruise Programs, Travel Tactical Offers Program

Lifestyle Benefits:

- Source Lifestyle discounts and benefits, Dining Program, Events Program, Ticket Access, Golf Program

Local Benefits:

- Locally sourced travel or lifestyle offers worth at least $300 (USD) or local socioeconomic equivalent, where 50% is made up of benefits with a quantifiable monetary value for Cardmembers

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Protection:

- Emergency Assistance - Tier 3
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Extended Warranty
- Retail Protection Insurance
- Online Fraud Protection Guarantee
- Fully Comprehensive Travel insurance, including Travel Accident, Flight Delay, Flight Cancellation, Luggage Delay, Luggage Protection. The coverage level must be greater than the level on the American Express® Gold Card

Marketing Communication:

- Annual Communications Calendar. Minimum twelve (12) to include: two (2) Preview Magazines minimum, four (4) e-Newsletters, and four (4) Departures Magazines (if distributed)
- Dedicated Issuer-hosted website - Platinum-branded website highlighting Platinum Card benefits in local language
- Adherence to *Platinum Card Product Guidelines*
- Annual submission of marketing communications/engagement plan - American Express approval required minimum one (1) quarter in advance of deployment

Portfolio Management/Reporting:

- Benefits and Servicing Reporting - Monthly benefit and full service metrics
- Annual customer satisfaction survey - only required for American Express Enterprise Line Consumer Platinum Card Issuers if their market has an eligible mail base that equals or exceeds 3,000 accounts in force (AIF). Participant must fund the cost of the survey

For more details on the required features and benefits associated with this product, refer to Section 3.7, "Descriptions of Product Features and Benefits," on page 191.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.4 The Centurion Card

Prior to being licensed to issue The Centurion® Card, the Issuer must meet the following Card issuance prerequisites:

- The Issuer must already issue The Platinum Card® and must meet the contractually established performance levels as determined by American Express.
- The Issuer must be in compliance with all AEGNS policies.
- The Issuer must have a sizable base of The Platinum Card® (e.g., 3,000-5,000 Cards in Force) in the market.
- The Issuer must agree to conduct acquisition by invitation only via pre-approved applications to its select customers who are:
  - Existing American Express Cardmembers exhibiting annual spend history on their existing Cards of $150,000 (USD) or local socioeconomic equivalent, and/or
  - "Premium" bank customers (e.g., private banking clientele) who have a financial portfolio that justifies a line of credit of $150,000 (USD) or the local socioeconomic equivalent.
- Agree to follow the product guidelines in the *Centurion Card Product Guidelines*.

Issuers are required to provide the following minimum features and benefits for The Centurion® Card:

- Payment Functionality - a Charge Card with no preset spending limit
- Cash Access - with a recommended cash limit that is greater than the limit on The Platinum Card®.
- Direct Debit of Monthly Balance or Minimum Payment

Card Portfolio:

- Metal form factor for all Basic and Supplementary. Must be stainless steel with Contactless functionality
- Issuers are not allowed to issue partial metal cards to a portion of the portfolio
- Basic Card
- Supplementary Cards - Issuer must provide Centurion Supplementary Cards at no additional cost as follows:
  - Minimum of one (1) Centurion Supplementary Card at no extra cost
  - Maximum of four (4) Centurion Supplementary Cards at no extra cost
  - Additional Supplementary Cards can be Platinum, Gold, or Green

  A fee may apply for any additional Supplementary Cards.
- Portfolio Size - Projected Cards in Force (CIF) expectations: First year - 500 CIF recommended total size, 0.75% of American Express Enterprise Line CIF.

Acquisition Requirements:

- Cardmember Tenure - Twelve (12) months American Express Cardmember spend or sufficient assets under management
- Annual submission of acquisition plan – American Express approval required one (1) quarter in advance of deployment
- Acquisition by invitation only
- Not Allowed: Online Card application form

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Engagement Requirements:

- First 100 Days Programs - American Express approval required

Servicing:

- Dedicated Servicing: Card, Travel, and Concierge. Required twenty-four (24) hours per day, seven (7) days per week, one (1) telephone number, dedicated team supporting relationship manager.
- Third-party Service Providers - American Express Vendor approval required.
- Relationship Manager Servicing (RMS) - Named individual managing a portfolio of accounts.
- Training – Continuous Partner Employee Training, and Assessments.
- Cardmember Online Account Access Service.
- Local Language Servicing.
- Servicing Assessments and Partner Accreditation.
- Customer Relationship Management (CRM) capabilities.
- Implement and use Premium Product Platform (PPP) and/or successor platforms. Fees apply. Refer to Section 10.5.11, "Premium Product Platform (PPP) Fees," on page 409.

Cardmember Loyalty Program:

- Membership Rewards
- Not allowed - Cashback and local Merchant awards

Travel Benefits:

- Local Airport Benefits - Include benefits such as Airport Fast Track, Meet and Greet Services, complimentary valet parking
- Airport Lounge Access - American Express Global Lounges and unlimited complimentary access to Priority Pass for Basic and Supplementary Cardmembers
- Airline Core Benefit Programs - International Airline Program
- Private Jet Program
- Global Hotel Program - FHR (Fine Hotels and Resorts) and THC (The Hotel Collection)
- Hotel Partner Loyalty Programs
- Car Partner Loyalty Programs
- Cruise Programs
- Travel Tactical Offers Program

Lifestyle Benefits:

- Source Local Lifestyle discounts and benefits
- Dining Program
- Events Program (Local, International and Bespoke)
- Ticket Access
- Other Access Programs (Private Bars and Clubs Program or Privileges)
- Golf Program
- Retail Offers or VIP Shopping Experience

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Local Benefits:

- Locally sourced travel or lifestyle offers worth at least $1,000 (USD) or local socioeconomic equivalent, where 50% is made up of benefits with a quantifiable monetary value for Cardmembers.

Protection:

- Emergency Assistance - Tier 3
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Retail Protection Insurance
- Online Fraud Protection Guarantee
- Fully Comprehensive Travel Insurance, including Travel Accident, Flight Delay, Flight Cancellation, Luggage Delay, Luggage Protection, Pre-Trip Cancellation. The coverage level must be greater than the level on The Platinum Card®
- Extended Warranty

Marketing Communication:

- Annual communications calendar - Minimum twelve (12) communications to include four (4) Preview Magazines minimum, four (4) e-Newsletters, and four (4) Centurion Magazines
- Publishing Magazine - Centurion Magazine or equivalent Issuer magazine
- Dedicated Issuer-hosted and Centurion-branded website highlighting Centurion Card benefits in local language
- Adherence to *Centurion Card Product Guidelines*
- Not allowed - Above The Line Advertising (ATL)
- Annual submission of marketing communications engagement plan – American Express approval required minimum one (1) quarter in advance of deployment.

Portfolio Management/Reporting:

- Dedicated Premium Product Manager
- Benefits and Servicing Reporting - Monthly benefit and full service metrics
- Quality measurement program
- Annual customer satisfaction survey. Participant must fund the cost of the survey

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.5 Blue from American Express

Prior to being licensed to issue Blue from American Express®, the Issuer must meet the following Card issuance prerequisites:

- Confirm their market has a minimum coverage of 60% on the targeted spend industries
- Agree to follow the product launch communication approach in the *Blue Guidelines Manual* (Partnership Resource) available on Knowledge Base
- Commit to above-the-line communication to support product launch. A minimum level of media coverage will be agreed upon during the product development process

Issuers are required to provide the following minimum features and benefits for Blue from American Express®:

- Payment Functionality - a Credit Card product with a line of credit that is competitive or superior to other products in the same segment
- Cash Access - with a recommended cash limit of 20% of the line of credit
- Direct Debit of Monthly Balance or Minimum Payment

Card Portfolio:

- Basic Card

Acquisition Requirements:

- Online Card Application Form

Servicing:

- Cardmember Card Servicing
- Cardmember Online Account Access Services
- Local Language Servicing

Cardmember Loyalty Program:

- Not allowed - Membership Rewards
- The value proposition must be supported by one (1) of the following loyalty programs:
  - Cashback
  - Local Merchant Rewards

Protection:

- Emergency Assistance - Tier 1
- Emergency Card Replacement
- A minimum of two (2) of the following programs:
  - Extended Warranty
  - Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
  - Retail protection insurance
- Online Fraud Protection Guarantee

Marketing Communication:

- Annual communications calendar
- Product-designated website pages (Blue Zone) - Blue designated website pages that must conform to the templates available in the *Blue Guidelines Manual* on Knowledge Base
- Adherence to Product Brand Guidelines

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.6 American Express Credit Card (green)

Issuers are required to provide the following minimum features and benefits for the American Express® Credit Card (green):

- Payment Functionality - a Credit Card with a minimum line of credit of $1,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended cash limit of 20% of the line of credit
- Direct Debit of Minimum Payment

Card Portfolio:

- Basic Card

Servicing:

- Card Servicing
- Cardmember Online Account Access Service
- Local Language Servicing

Cardmember Loyalty Program:

- Not allowed - Membership Rewards
- The value proposition must be supported by one (1) of the following loyalty programs:
  - Cashback
  - Local Merchant Rewards

Protection:

- Emergency Assistance - Tier 1
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

Marketing Communication:

- Product website/designated pages
- Adherence to Product Brand Guidelines

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.7 American Express Gold Credit Card

Issuers are required to provide the following minimum features and benefits for the American Express® Gold Credit Card:

- Payment Functionality - a Credit Card with a minimum line of credit of $5,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended cash limit of 20% of the line of credit
- Direct Debit of Minimum Payment

Card Portfolio:

- Basic Card

Servicing:

- Card Servicing
- Cardmember Online Account Access Service
- Local Language Servicing

Cardmember Loyalty Program:

- Not allowed - Membership Rewards
- The value proposition must be supported by one (1) of the following loyalty programs:
  - Cashback
  - Local Merchant Rewards

Protection:

- Emergency Assistance - Tier 1
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Retail Protection Insurance

Marketing Communication:

- Product website/designated pages
- Adherence to Product Brand Guidelines

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.3.8 American Express Platinum Credit Card

Issuers are required to provide the following minimum features and benefits for the American Express® Platinum Credit Card:

- Payment Functionality - a Credit Card with a minimum line of credit of $10,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended cash limit of 20% of the line of credit
- Direct Debit of Minimum Payment

Card Portfolio:

- Basic Card

Servicing:

- Card Servicing
- Cardmember Online Account Access Service
- Local Language Servicing

Cardmember Loyalty Program:

- Not allowed - Membership Rewards
- The value proposition must be supported by one (1) of the following loyalty programs:
  - Cash rebate rewards program
  - Merchant offers program

Protection:

- Emergency Assistance - Tier 2
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Retail Protection Insurance

Marketing Communication:

- Product website/designated pages
- Adherence to Product Brand Guidelines

3.3.9 American Express Debit Card

Issuers are required to provide the following minimum features and benefits for the American Express® Debit Card:

- Payment Functionality - Debit
- Cash Access

Servicing:

- Card Servicing
- Cardmember Online Account Access Service
- Local Language Servicing

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Protection:

- Emergency Assistance
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

Marketing Communication:

- Adherence to Product Brand Guidelines

3.4 American Express Enterprise Line Commercial Products

The following tables summarize the required and recommended features and benefits for American Express Enterprise Line Commercial Products:

- Table 3-2, "Features and Benefits for American Express Enterprise Line Small Business Commercial Products," on page 152
- Table 3-3, "Features and Benefits for American Express Enterprise Line Commercial Corporate Products," on page 161

3.4.1 American Express Enterprise Line Small Business Products

Small Business Products are aimed at businesses with fewer than 50 employees.

Table 3-2 Features and Benefits for American Express Enterprise Line Small Business Commercial Products

Feature	The American Express® Business Card	The American Express® Business Gold Card	The American Express® Business Platinum Card	The Business Centurion® Card	American Express® Travel Agency Account	American Express® Business Debit Card
Payment Functionality	Charge or Revolve	Charge or Revolve	Charge or Revolve	Charge or Revolve	Charge Only	Debit
No Pre-set Spending Limit Functionality (if Charge Card)	Required	Required	Required	Required	Recom-mended	--
Minimum Credit Limit (where applicable)	$1,000 (USD)	$5,000 (USD)	$10,000 (USD)	Required	--	--
Cash Access	Required	Required	Required	Required	--	Required
Year-End Summary of Charges	Required	Required	Required	Required	Required	--
Air Addenda	Recom-mended	Recom-mended	Recom-mended	Recom-mended	Required	--
Cardless Account	--	--	--	--	Recom-mended	--
Cardmember Employee ID and Cost Center	--	--	--	--	--	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-2 Features and Benefits for American Express Enterprise Line Small Business Commercial Products (continued)

Feature	The American Express® Business Card	The American Express® Business Gold Card	The American Express® Business Platinum Card	The Business Centurion® Card	American Express® Travel Agency Account	American Express® Business Debit Card
Choice of Billing Frequency	--	--	--	--	--	--
Company Liability Options	--	--	--	--	Required: Company Only	--
Corporate Billing Options	Required: Central Billing Only	Required: Central Billing Only	Required: Central Billing Only	Required: Central Billing Only	Required: Central Billing Only	--
Descriptive Travel/Customer Reference Data (matched and merged with charge data)	--	--	--	--	--	--
Electronic Remittance File	--	--	--	--	--	--
Global Limits	--	--	--	--	--	--
Issuer-generated Data Files	--	--	--	--	--	--
Line Item Detail	--	--	--	--	--	--
Merchant Category Restrictions	--	--	--	--	Required	--
MIS Customized Reporting	--	--	--	--	--	--
MIS Standard Reporting	--	--	--	--	--	--
Open Item Billing	--	--	--	--	--	--
Proactive Data Quality Processes	--	--	--	--	--	--
Tax Invoice Capture/ Presentment (where permitted by regulations)	--	--	--	--	--	--
VAT/GST information (in markets where applicable)	Recommended	Recommended	Recommended	Recommended	Recommended	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-2 Features and Benefits for American Express Enterprise Line Small Business Commercial Products (continued)

Feature	The American Express® Business Card	The American Express® Business Gold Card	The American Express® Business Platinum Card	The Business Centurion® Card	American Express® Travel Agency Account	American Express® Business Debit Card
Card Portfolio						
Basic Card	Required	Required	Required	Required	Required	--
Supplementary Cards	Recommended	Recommended	Recommended	Recommended	--	--
Corporate Account Hierarchy	--	--	--	--	--	--
Corporate Account Management	--	--	--	--	--	--
Emergency Card Replacement	Required	Required	Required	Required	--	Required
Online Program Management	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
Online Reconciliation/ Expense Reporting Tool	--	--	--	--	--	--
Card Fees						
Basic Card	Required	Required	Required	Required	--	--
Supplementary Cards	--	--	--	--	--	--
Acquisition Requirements						
Field Sales Force	--	--	--	--	--	--
Engagement Requirements						
First 100 Days Programs	Recommended	Recommended	Recommended	Recommended	Recommended	--
Servicing						
Cardmember Customer Service	Required	Required	Required	Required	--	Required
Cardmember Online Account Access	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
Concierge Service	--	Recommended	Required	Required	--	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-2 Features and Benefits for American Express Enterprise Line Small Business Commercial Products (continued)

Feature	The American Express® Business Card	The American Express® Business Gold Card	The American Express® Business Platinum Card	The Business Centurion® Card	American Express® Travel Agency Account	American Express® Business Debit Card
Dedicated Operations Unit (for company-level servicing)	--	--	--	--	Recommended	--
Protection						
Business Travel Accident Insurance	Recommended	Recommended	Recommended	Recommended	Recommended	--
Car Rental Insurance	Recommended	Recommended	Recommended	Recommended	--	--
Emergency Assistance	Required	Required (Tier 3 recommended)	Required (Tier 3 recommended)	Required (Tier 3 recommended)	Recommended	Required
Flight Delay and Cancellation Insurance	Required	Required	Required	Required	Recommended	--
Luggage Delay Protection	Required	Required	Required	Required	Recommended	--
Luggage Loss Protection	Required	Required	Required	Required	Recommended	--
Travel Accident Insurance	Required	Required	Required	Required	Required	--
Travel Accident Insurance - Group Coverage	--	--	--	--	--	--
Limited Liability for Lost/Stolen Card/Fraud Protection Guaranteed	Required	Required	Required	Required	Required	Required
Loyalty Programs						
Cardmember Loyalty Program	Recommended	Recommended	Recommended	Recommended	--	--
Company Savings/Loyalty Program	Required	Required	Required	Required	Recommended	--
Membership Rewards	Required	Required	Required	Required	--	--
Virtual Currency						

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-2 Features and Benefits for American Express Enterprise Line Small Business Commercial Products (continued)

Feature	The American Express® Business Card	The American Express® Business Gold Card	The American Express® Business Platinum Card	The Business Centurion® Card	American Express® Travel Agency Account	American Express® Business Debit Card
Travel Benefits						
Airport Lounge Access	--	Recommended (if no Platinum)	Required	Required	--	--
Car Hire Loyalty Programs & Benefits	Recommended	Recommended	Required	Required	--	--
Global Hotel Program	--	--	Required	Required	--	--
Hotel Partner Loyalty Programs	--	--	Required	Required	--	--
Local Airport Benefits	--	Recommended (if no Platinum)	Required	Required	--	--
Membership Travel Service (Travel Agency)	--	Recommended	Recommended	Recommended	--	--
Travel Tactical Offers Program	Recommended	Recommended	Required	Required	--	--
Other Benefits						
Business Offers & Services	Recommended	Recommended	Recommended	Recommended	--	--
Local & Global Dining Benefits	Recommended	Recommended	Recommended	Recommended	--	--
Local Exclusive Events & Global Events Access	Recommended	Recommended	Recommended	Recommended	--	--
Other Access Programs	Recommended	Recommended	Recommended	Recommended	--	--
Retail Offers, Programs, & Services	Recommended	Recommended	Recommended	Recommended	--	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.4.1.1 The American Express Business Card

Issuers are required to provide the following minimum features and benefits for The American Express® Business Card:

- Payment Functionality - a Charge Card with no preset spending limit, or a Credit Card. The Credit Card product must offer the option to revolve a balance on a minimum line of credit of $1,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended monthly minimum cash limit of $1,000 (USD) or local socioeconomic equivalent
- Marketing Communication - Adhere to Product Brand Guidelines
- Travel Accident Insurance - with a minimum coverage level of $100,000 (USD) or local socioeconomic equivalent
- Cardmember Customer Service
- Central Billing
- Luggage Delay Protection
- Luggage Loss Protection
- Flight Delay and Cancellation Insurance
- Emergency Assistance
- Emergency Card Replacement
- Company Savings/Loyalty Program - Membership Rewards
- Year-End Summary of Charges
- Business Offers Program
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

3.4.1.2 The American Express Business Gold Card

Issuers are required to provide the following minimum features and benefits for The American Express® Business Gold Card:

- Payment Functionality - a Charge Card with no preset spending limit or a Credit Card. The Credit Card product must offer the option to revolve a balance on a minimum line of credit of $5,000 (USD) or local socioeconomic equivalent
- Card Portfolio:
  - Minimum one (1) Basic Card, with choice of plastic or metal form factor
  - Provide option for Supplementary Cards, up to a maximum limit
  - May assess a fee for Supplementary Cards
- Marketing Communication - Adhere to Product Brand Guidelines
- Cash Access - with a recommended monthly minimum cash limit of $1,000 (USD) or local socioeconomic equivalent
- Travel Accident Insurance - with a minimum coverage level greater than the level on The American Express® Business Card
- Cardmember Customer Service
- Luggage Delay Protection - the coverage level must be greater than the level on The American Express® Business Card

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Luggage Loss Protection - the coverage level must be greater than the level on The American Express® Business Card
- Flight Delay and Cancellation Insurance - the coverage level must be greater than the level on The American Express® Business Card
- Central Billing
- Emergency Assistance
- Emergency Card Replacement
- Company Savings/Loyalty Program - Membership Rewards
- Year-End Summary of Charges
- Business Offers Program
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

3.4.1.3 The American Express Business Platinum Card

Issuers are required to provide the following minimum features and benefits for The American Express® Business Platinum Card:

- Payment Functionality - a Charge Card with no preset spending limit or a Credit Card. The Credit Card product must offer the option to revolve a balance on a minimum line of credit of $10,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended minimum cash limit higher than the limit available on The American Express® Business Gold Card
- Card Portfolio:
  - Minimum one (1) Basic Card, with choice of plastic or metal form factor
  - Provide option for Supplementary Cards, up to a maximum limit
  - May assess a fee for Supplementary Cards
- Marketing Communication - Adhere to Product Brand Guidelines
- Cardmember Customer Service
- Travel Accident Insurance - with a minimum coverage level greater than the level on The American Express® Business Gold Card
- Luggage Delay Protection - the coverage level must be greater than the level on The American Express® Business Gold Card
- Luggage Loss Protection - the coverage level must be greater than the level on The American Express® Business Gold Card
- Flight Delay and Cancellation Insurance - the coverage level must be greater than the level on The American Express® Business Gold Card
- Central Billing
- Emergency Assistance - Tier 3 recommended
- Emergency Card Replacement
- Company Savings/Loyalty Program - Membership Rewards
- Concierge Service. Required twenty-four (24) hours per day, seven (7) days per week, one (1) telephone number, dedicated team.
- Year-End Summary of Charges
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Benefits

- Car Hire Loyalty Programs and Benefits
- Airport Lounge Access / Global Lounge Collection, International Airline Program, Local Airport Benefits
- Global Hotel Program
- Hotel Partner Loyalty Programs
- Travel Tactical Offers Program
- Lifestyle Benefits
- Business Offers Program

3.4.1.4 The Business Centurion Card

Prior to being licensed to issue The Business Centurion® Card, the Issuer must meet the following Card issuance prerequisites:

- The Issuer must already issue The American Express® Business Platinum Card and must meet the contractually established performance levels as determined by American Express.
- The Issuer must have a sizable base of The American Express® Business Platinum Card (e.g., 3,000-5,000 Cards in Force) in the country.
- The Issuer must agree to conduct acquisition by invitation only via pre-approved applications to its select customers who are:
  - Existing American Express Cardmembers exhibiting annual spend history on their existing Cards of $150,000 (USD) or local socioeconomic equivalent, and/or
  - "Premium" bank customers (e.g., private banking clientele) who have a financial portfolio that justifies a line of credit of $150,000 (USD) or the local socioeconomic equivalent.
- Agree to follow the product guidelines.

Issuers are required to provide the following minimum features and benefits for The Business Centurion® Card:

- Payment Functionality - a Charge Card with no preset spending limit or a Credit Card. The Credit Card product must offer the option to revolve a balance on a minimum line of credit higher than the one available for The American Express® Business Platinum Card
- Cash Access - with a recommended minimum cash limit higher than the limit available on The American Express® Business Platinum Card
- Card Portfolio:
  - Minimum one (1) Basic Card, with choice of plastic or metal form factor
  - Must provide at least one (1) supplementary Business Centurion® Card at no extra cost
  - All further Supplementary Cards can be Platinum, Gold or Green, up to a maximum limit
  - May assess a fee for Supplementary Cards
- Premium Cardmember Customer Service: Card, Travel, and Concierge. Required twenty-four (24) hours per day, seven (7) days per week, one (1) telephone number, dedicated team supporting relationship manager
- Relationship Manager Servicing (RMS) - Named individual managing a portfolio of accounts
- Cardmember Tenure - Twelve (12) months American Express Cardmember spend or sufficient assets under management
- Acquisition by invitation only
- Company Savings/Loyalty program - Membership Rewards

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Central Billing
- Year-End Summary of Charges
- Travel Accident Insurance - with a minimum coverage level greater than the level on The American Express® Business Platinum Card
- Luggage Delay Protection - with a minimum coverage level greater than the level on The American Express® Business Platinum Card
- Luggage Loss Protection - with a minimum coverage level greater than the level on The American Express® Business Platinum Card
- Flight Delay and Cancellation Insurance - with a minimum coverage level greater than the level on The American Express® Business Platinum Card
- Emergency Assistance - Tier 3 Recommended
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

Benefits

- Global Lounge Access, International Airline Program
- Car Hire Loyalty Programs and Benefits
- Global Hotel Program
- Hotel Partner Loyalty Programs
- Travel Tactical Offers Program
- Lifestyle Benefits
- Business Offers Program

3.4.1.5 American Express Travel Agency Account

This product is designed for small business customers who wish to bill all of their travel agency expenses to a single centralized account. It is intended to be lodged with the travel agency rather than carried by an individual.

Issuers are required to provide the following minimum features and benefits for the American Express® Travel Agency Account:

- Payment Functionality - Charge only
- Travel Accident Insurance - with a minimum coverage level of $100,000 (USD) or local socioeconomic equivalent
- Central Billing
- Company Liability Options
- Air Addenda
- Merchant Category Restrictions
- Year-End Summary of Charges
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.4.1.6 American Express Business Debit Card

Issuers are required to provide the following minimum features and benefits for the American Express® Business Debit Card:

- Payment Functionality - Debit
- Cash Access
- Marketing Communication - Adhere to Product Brand Guidelines
- Cardmember Customer Service
- Emergency Assistance
- Emergency Card Replacement
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

3.4.2 American Express Enterprise Line Corporate Products

Corporate products are designed for corporations with fifty (50) employees or more, and hence offer a number of specific features that are not required for consumer or small business products. Together these features support the concept of a "corporate expense management program," whereby the Issuer provides an integrated suite of payment products to help companies streamline their expenditure processes.

The requirements listed in this section represent the minimum level of functionality that is deemed sufficient for the lower and middle segments of the corporate spectrum. This typically includes businesses in the "mid-market" (up to 250 employees) segment, and the "national" segment (greater than 250 employees but concentrated in a single country).

If Issuers will be targeting companies in the multinational and global segments (typically those with more than 10,000 employees and operating globally or those that have an existing American Express relationship and/or have been referred to the Issuer by American Express), they must offer Enhanced functionality in addition to the Standard one. These additional requirements are listed in Section 3.4.3, "Enhanced Functionality Requirements for American Express Enterprise Line Corporate Products," on page 169 and include features and benefits which integrate with the corporate products in proprietary American Express markets as well as support the participation of Issuers in global client contracts.

Table 3-3, "Features and Benefits for American Express Enterprise Line Commercial Corporate Products," on page 161 summarizes the required and recommended features for American Express Enterprise Line Corporate Products.

Refer to Section 3.7, "Descriptions of Product Features and Benefits," on page 191 for more details on the features and benefits associated with various products.

Table 3-3 Features and Benefits for American Express Enterprise Line Commercial Corporate Products

Feature	American Express® Corporate Card	American Express® Corporate Gold Card	American Express® Corporate Platinum Card	American Express® Business Travel Account	American Express® Corporate Purchasing Card	American Express® Corporate Meeting Card
Payment Functionality	Charge Only	Charge Only	Charge Only	Charge Only	Charge Only	Charge Only
No Pre-set Spending Limit Functionality (if Charge Card)	Required	Required	Required	Recom-mended	--	Recom-mended

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-3 Features and Benefits for American Express Enterprise Line Commercial Corporate Products (continued)

Feature	American Express® Corporate Card	American Express® Corporate Gold Card	American Express® Corporate Platinum Card	American Express® Business Travel Account	American Express® Corporate Purchasing Card	American Express® Corporate Meeting Card
Minimum Credit Limit (where applicable)	--	--	--	--	--	--
Cash Access	Required	Required	Required	--	--	Required
Year-End Summary of Charges	--	--	--	--	--	--
Air Addenda	Recommended	Recommended	Recommended	Required	--	Recommended
Cardless Account	--	--	--	Recommended	Recommended	--
Cardmember Employee ID and Cost Center	Required	Required	Required	--	Required	Required
Choice of Billing Frequency	--	--	--	Recommended	Recommended	--
Company Liability Options	Required	Required	Required	Required: Company Only	Required: Company Only	Required: Company Only
Corporate Billing Options	Required	Required	Required	Required: Central Billing Only	Recommended	Recommended
Descriptive Travel/Customer Reference Data (matched and merged with charge data)	--	--	--	Required	--	--
Electronic Remittance File	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
Global Limits	Recommended	Recommended	Recommended	Recommended	Required	Required
Issuer-generated Data Files	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
Line Item Detail	--	--	--	--	Recommended	Recommended
Merchant Category Restrictions	--	--	--	Required	--	--
MIS Customized Reporting	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
MIS Standard Reporting	Required	Required	Required	Required	Required	Required

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-3 Features and Benefits for American Express Enterprise Line Commercial Corporate Products (continued)

Feature	American Express® Corporate Card	American Express® Corporate Gold Card	American Express® Corporate Platinum Card	American Express® Business Travel Account	American Express® Corporate Purchasing Card	American Express® Corporate Meeting Card
Open Item Billing	--	--	--	Recom-mended	--	--
Proactive Data Quality Processes	--	--	--	Recom-mended	Recom-mended	--
Tax Invoice Capture/ Presentment (where permitted by regulations)	--	--	--	Recom-mended	Recom-mended	Recom-mended
VAT/GST information (in markets where applicable)	Recom-mended	Recom-mended	Recom-mended	Recom-mended	Required	Recom-mended
Card Portfolio						
Basic Card	Required	Required	Required	Required	Required	Required
Supplementary Cards	Recom-mended	Recom-mended	Recom-mended	--	Recom-mended	Recom-mended
Corporate Account Hierarchy	Required	Required	Required	Required	Required	Required
Corporate Account Management	Required	Required	Required	Required	Required	Required
Emergency Card Replacement	Required	Required	Required	--	--	--
Online Program Management	Recom-mended	Recom-mended	Recom-mended	Recom-mended	Recom-mended	Recom-mended
Online Reconciliation/ Expense Reporting Tool	Recom-mended	Recom-mended	Recom-mended	Recom-mended	Required	Recom-mended
Card Fees						
Basic Card	Required	Required	Required	--	--	Required
Supplementary Cards	--	--	--	--	--	--
Acquisition Requirements						
Field Sales Force	Required	Required	Required	Required	Required	Required
Engagement Requirements						

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-3 Features and Benefits for American Express Enterprise Line Commercial Corporate Products (continued)

Feature	American Express® Corporate Card	American Express® Corporate Gold Card	American Express® Corporate Platinum Card	American Express® Business Travel Account	American Express® Corporate Purchasing Card	American Express® Corporate Meeting Card
First 100 Days Programs	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
Servicing						
Cardmember Customer Service	Required	Required	Required	--	--	Recommended
Cardmember Online Account Access	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended
Concierge Service	--	Required	Required	--	--	--
Dedicated Operations Unit (for company-level servicing)	Required	Required	Required	Required	Required	Required
Protection						
Business Travel Accident Insurance	Required	Required	Required	Required	--	Required
Car Rental Insurance	Recommended	Recommended	Recommended	--	--	--
Emergency Assistance	Required	Required (Tier 3 recommended)	Required (Tier 3)	Recommended	--	Recommended
Flight Delay and Cancellation Insurance	Required	Required	Required	Recommended	--	Recommended
Luggage Delay Protection	Required	Required	Required	Recommended	--	Recommended
Luggage Loss Protection	Required	Required	Required	Recommended	--	Recommended
Travel Accident Insurance	Required	Required	Required	Required	--	Required
Travel Accident Insurance - Group Coverage	--	--	--	--	--	Required
Loyalty Programs						
Cardmember Loyalty Program	Recommended	Recommended	Recommended	--	--	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-3 Features and Benefits for American Express Enterprise Line Commercial Corporate Products (continued)

Feature	American Express® Corporate Card	American Express® Corporate Gold Card	American Express® Corporate Platinum Card	American Express® Business Travel Account	American Express® Corporate Purchasing Card	American Express® Corporate Meeting Card
Company Savings/Loyalty Program	Recom-mended	Recom-mended	Recom-mended	Recom-mended	--	Required
Membership Rewards	Required	Required	Required	--	--	--
Travel Benefits						
Airport Lounge Access	--	Recom-mended (if no Platinum)	Required	--	--	--
Car Hire Loyalty Programs & Benefits	--	--	--	--	--	--
Global Hotel Program	--	--	--	--	--	--
Hotel Partner Loyalty Programs	--	--	--	--	--	--
Local Airport Benefits	--	Recom-mended (if no Platinum)	Required	--	--	--
Membership Travel Service (Travel Agency)	--	Recom-mended	Required	--	--	--
Travel Tactical Offers Program	--	--	--	--	--	--
Other Benefits						
Business Offers & Services	--	--	--	--	--	--
Local & Global Dining Benefits	--	--	--	--	--	--
Local Exclusive Events & Global Events Access	--	--	--	--	--	--
Other Access Programs	--	--	--	--	--	--
Retail Offers, Programs, & Services	--	--	--	--	--	--

For guidance on recommended features, Participants should access the marketing materials in The Orchard on Knowledge Base. Additional benefits, features, and functionality may be available in certain markets.

Please consult your AEGNS representative for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.4.2.1 American Express Corporate Card

Issuers are required to provide the following minimum features and benefits for the American Express® Corporate Card.

- Payment Functionality - Charge only, with no preset spending limit
- Cash Access
- Cardmember Customer Service
- Travel Accident Insurance - with a minimum coverage level of $100,000 (USD) or local socioeconomic equivalent.
- Business Travel Accident Insurance
- Flight Delay and Cancellation Insurance
- Luggage Delay Protection
- Luggage Loss Protection
- Customer Loyalty Program - Membership Rewards
- Company Liability Options
- Corporate Billing Options
- Corporate Account Hierarchy
- Corporate Account Management
- Field Sales Force
- Cardmember Employee ID and Cost Center
- Emergency Assistance
- Emergency Card Replacement
- Dedicated Operations Unit (for company-level servicing)
- MIS Standard Reporting

3.4.2.2 American Express Corporate Gold Card

Issuers are required to provide the following minimum features and benefits for the American Express® Corporate Gold Card.

- Payment Functionality - Charge only, with no preset spending limit
- Cash Access
- Cardmember Customer Service
- Travel Accident Insurance - coverage level must be greater than the level on the American Express® Corporate Card
- Business Travel Accident Insurance
- Flight Delay and Cancellation Insurance
- Luggage Delay Protection
- Luggage Loss Protection
- Customer Loyalty Program - Membership Rewards
- Company Liability Options
- Corporate Billing Options

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Corporate Account Hierarchy
- Corporate Account Management
- Field Sales Force
- Cardmember Employee ID and Cost Center
- Emergency Assistance
- Emergency Card Replacement
- Dedicated Operations Unit (for company-level servicing)
- Concierge Service
- MIS Standard Reporting

3.4.2.3 American Express Corporate Platinum Card

Issuers are required to provide the following minimum features and benefits for the American Express® Corporate Platinum Card.

- Payment Functionality - Charge only, with no preset spending limit
- Cash Access
- Cardmember Customer Service
- Travel Accident Insurance - coverage level must be greater than the level on the American Express® Corporate Card
- Business Travel Accident Insurance
- Membership Travel Service
- Flight Delay and Cancellation Insurance
- Luggage Delay Protection
- Luggage Loss Protection
- Customer Loyalty Program - Membership Rewards
- Benefits: Local Airport Benefits
- Company Liability Options
- Corporate Billing Options
- Corporate Account Hierarchy
- Corporate Account Management
- Field Sales Force
- Cardmember Employee ID and Cost Center
- Emergency Assistance (Tier 3)
- Emergency Card Replacement
- Dedicated Operations Unit (for company-level servicing)
- Concierge Service
- MIS Standard Reporting
- Other insurance/travel benefits in line with consumer Platinum Card product, where applicable

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.4.2.4 American Express Corporate Purchasing Card

Issuers are required to provide the following minimum features and benefits for the American Express® Corporate Purchasing Card.

- Payment Functionality - Charge only
- Company Liability Options
- Corporate Account Hierarchy
- Corporate Account Management
- Field Sales Force
- Cardmember Employee ID and Cost Center
- Dedicated Operations Unit (for company-level servicing)
- Global Limits
- Online Reconciliation/Expense Reporting Tool
- VAT/GST Information (in markets where applicable)
- MIS Standard Reporting

3.4.2.5 American Express Corporate Meeting Card

Issuers are required to provide the following minimum features and benefits for the American Express® Corporate Meeting Card.

- Payment Functionality - Charge only
- Cash Access
- Travel Accident Insurance - with a minimum coverage level of $100,000 (USD) or local socioeconomic equivalent
- Business Travel Accident Insurance
- Travel Accident Insurance - group coverage
- Company Liability Options
- Corporate Account Hierarchy
- Corporate Account Management
- Field Sales Force
- Cardmember Employee ID and Cost Center
- Dedicated Operations Unit (for company-level servicing)
- Company Savings/Loyalty Program (e.g., Meetings Exclusives)
- MIS Standard Reporting
- Global Limits

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.4.2.6 American Express Business Travel Account

Issuers are required to provide the following minimum features and benefits for the American Express® Business Travel Account.

- Payment Functionality - Charge only
- Travel Accident Insurance - with a minimum coverage level of $100,000 (USD) or local socioeconomic equivalent
- Business Travel Accident Insurance
- Central Billing
- Company Liability Options
- Corporate Account Hierarchy
- Corporate Account Management
- Air Addenda
- Dedicated Operations Unit (for company-level servicing)
- Descriptive Travel/Customer Reference Data (matched and merged with charged data)
- Field Sales Force
- Merchant Category Restrictions
- MIS Standard Reporting

3.4.3 Enhanced Functionality Requirements for American Express Enterprise Line Corporate Products

The features and benefits described in this section represent the minimum requirements Issuers must provide under Enhanced Functionality for American Express Enterprise Line of Corporate Products.

- Enhanced Global Management Information System (eGMIS)
- Global Rebates
- Electronic Remittance File
- Corporate Account Hierarchy - support for complex company structures, with at least three (3) levels of control accounts, and preferably up to six (6), if required
- Global Limits
- Option to extend payment terms (for special client contracts only, subject to local market conditions
- Choice of cycle cut dates
- Cardmember Loyalty Program
- English language support

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.5 Blue Box Line Consumer Cards

Table 3-4, "Features and Benefits for Blue Box Line Consumer Cards," on page 170 summarizes the required and recommended features for the Blue Box Line Consumer Cards.

Table 3-4 Features and Benefits for Blue Box Line Consumer Cards

Product Feature	Product Tier					
	Member	**Select**	**Max**	**Icon**		**Debit**
	[Issuer Name] American Express® Card (Member)	**[Issuer Name] Select American Express® Card**	**[Issuer Name] Max American Express® Card**	**[Issuer Name] Icon American Express® Card or [Issuer Name] Black American Express® Card**	**[Issuer Name] American Express® Generation Card**	**[Issuer Name] American Express® Debit Card**
Cash Access	Required	Required	Required	Required	Required	Required
Direct Debit of Monthly Balance or Minimum Payment	Required	Required	Required	--	--	
Minimum Credit Limit	Required ($1,000 min)	Required ($5,000 min)	Required ($10,000 min)	Required ($25,000 min)	Required (Defined by Basic Cardmember)	
Payment Functionality	Charge or revolve	Charge or revolve	Charge or revolve	Charge or revolve	Pre-set	Debit
Pre-set Spending Limit	--	--	--	--	Required (Defined by Basic Cardmember)	
Servicing						
Cardmember Customer Service	Required	Required	Required	Required	Required	Required
Cardmember Online Account Access Service	--	--	Required	Required	--	
Cardmember Site for Accessing Product Features and Benefits	--	--	Required	Required	--	
Concierge Service	--	--	Required	Required	--	
Customer Relationship Management (CRM) Capability	--	--	--	Required	--	
Implement and User Premium Product Platform (PPP)	--	--	--	Required	--	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-4 Features and Benefits for Blue Box Line Consumer Cards (continued)

Product Feature	Product Tier					
	Member	Select	Max	Icon		Debit
	[Issuer Name] American Express® Card (Member)	[Issuer Name] Select American Express® Card	[Issuer Name] Max American Express® Card	[Issuer Name] Icon American Express® Card or [Issuer Name] Black American Express® Card	[Issuer Name] American Express® Generation Card	[Issuer Name] American Express® Debit Card
Local Language Servicing	Required	Required	Required	Required	Required	Required
Servicing Assessment	--	--	--	Required	--	
Third-party Service Providers	--	--	--	Approval Required	--	
Travel Servicing	--	--	--	Required	--	
Cardmember Loyalty Programs						
Cardmember Loyalty Program	Recommended	Required	Required	Required	--	
Virtual Currency						
Travel Benefits						
Airport Lounge Access Program	--	--	--	Required	--	
Car Partner Loyalty Program	--	--	--	Required	--	
Hotel Partner Loyalty Program	--	--	--	Required	--	
Travel Related Offer Programs	--	--	--	Required	--	
Lifestyle Benefits						
Dining Program/Offers	--	--	--	Required	--	
Events Program	--	--	--	Required	--	
Retail Programs	--	Required [1 program]	Required	Required [2 programs]	--	
Protection						
Car Rental Insurance	--	--	--	Required [U.S. and Canada]	--	
Emergency Assistance	Required [Tier 1]	Required [Tier 1]	Required [Tier 2]	Required [Tier 3]	Required [Tier 3]	Required

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-4 Features and Benefits for Blue Box Line Consumer Cards (continued)

Product Feature	Product Tier					
	Member	Select	Max	Icon		Debit
	[Issuer Name] American Express® Card (Member)	[Issuer Name] Select American Express® Card	[Issuer Name] Max American Express® Card	[Issuer Name] Icon American Express® Card or [Issuer Name] Black American Express® Card	[Issuer Name] American Express® Generation Card	[Issuer Name] American Express® Debit Card
Emergency Card Replacement	Required	Required	Required	Required	--	Required
Limited Liability for Lost/Stolen/Counterfeit Cards	Required	Required	Required	Required	Required	Required
Luggage Delay Protection	Recommended	Recommended	Recommended	Required	--	
Luggage Loss Protection	Recommended	Recommended	Recommended	Required	--	
Retail Protection Program	Recommended	Required	Required	Required	--	
Travel Accident Insurance	Recommended	Required	Required	Required	--	
Cardmember Communication						
Cardmember Communication	--	--	Required	Required	--	

Additional benefits, features, and functionality may be available in certain markets. Please consult your AEGNS representative for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.5.1 Product Tier: Member

[Issuer Name] American Express® Card (Member)

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] American Express® Card (Member):

- Payment Functionality - a Charge Card with no preset spending limit, or a Credit Card product. The Credit Card product must offer a minimum line of credit of $1,000 (USD) or local socioeconomic equivalent
- Direct Debit of Monthly Balance or Minimum Payment
- Cash Access
- Cardmember Customer Service
- Emergency Assistance
- Emergency Card Replacement
- Limited liability for lost/stolen/counterfeit cards/fraud protection guarantee

3.5.2 Product Tier: Select

[Issuer Name] Select American Express® Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Select American Express® Card:

- Payment Functionality - a Charge Card with no preset spending limit, or a Credit Card product. The Credit Card product must offer a minimum line of credit of $5,000 (USD) or local socioeconomic equivalent
- Cash Access - the cash limit must be higher than that of the [Issuer Name] American Express® Card (Standard)
- Cardmember Customer Service

Cardmember Loyalty Program

- Cardmember Loyalty Program

Lifestyle Benefits

- Retail Program - a minimum of one (1) program

Protection

- Travel Accident Insurance - the coverage level must be a minimum of $100,000 (USD) or local socioeconomic equivalent
- Direct Debit of Monthly Balance or Minimum Payment
- Emergency Assistance - Tier 1
- Emergency Card Replacement
- Retail Protection Program
- Limited liability for lost/stolen/counterfeit cards/fraud protection guarantee

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.5.3 Product Tier: Max

[Issuer Name] Max American Express® Card

Prior to being licensed to issue a Max-tier product, the Issuer must agree to promote the Card as an exclusive offer to its select customers who are existing [Issuer Name] American Express Cardmembers or bank cardholders exhibiting annual spend history on their existing cards of $10,000 (USD) or the local socioeconomic equivalent.

Issuers are also required to provide the following minimum features and benefits for a Max-tier product:

- Payment Functionality - a Charge Card with no preset spending limit, or a Credit Card. The Credit Card product must offer a minimum line of credit of $10,000 (USD) or the local socioeconomic equivalent
- Cash Access - the cash limit must be higher than that of the [Issuer Name] Select American Express® Card
- Direct Debit of Monthly Balance or Minimum Payment

Servicing

- Cardmember Customer Service
- Concierge Service
- Cardmember site for accessing product features and benefits
- Cardmember online account access service
- Local language servicing
- Optional for Black product: Implement and use Premium Products Platform (PPP). Fees apply. Refer to Section 10.5.11, "Premium Product Platform (PPP) Fees," on page 409

Cardmember Loyalty Program

- Cardmember Loyalty Program - a minimum of one (1) type of program

Lifestyle Benefits

- Retail Programs - at least one (1) form of retail program

Protection

- Travel Accident Insurance - the coverage level must be a minimum of $250,000 (USD) or local socioeconomic equivalent, and higher than the coverage on the [Issuer Name] Gold American Express® Card
- Limited Liability for lost/stolen/counterfeit cards/fraud protection guarantee
- Retail Protection Program
- Emergency Assistance - Tier 2
- Emergency Card Replacement

Cardmember Communication

- Annual communications calendar: minimum four (4)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.5.4 Product Tier: Icon

[Issuer Name] Icon American Express® Card or
[Issuer Name] Black American Express® Card

Prior to being issued a Icon-tier product, the Issuer must agree to promote the Card as an exclusive offer to its select customers who are:

- Existing [Issuer Name] American Express Cardmembers or bank cardholders exhibiting annual spend history on their existing cards of $25,000 (USD) or local socioeconomic equivalent, and/or
- "Premium" bank customers (e.g., private banking clientele) who have a financial portfolio that justifies a line of $25,000 (USD) or the local socioeconomic equivalent.

Issuers are required to provide the following minimum features and benefits for an Icon-tier product:

- Payment Functionality - a Charge Card with no preset spending limit, or a Credit Card. The Credit Card product must offer a minimum line of credit of $25,000 (USD) or local socioeconomic equivalent
- Cash Access - a higher cash access limit than that of the [Issuer Name] Max American Express® Card is recommended
- Direct Debit of Monthly Balance or Minimum Payment

Servicing

- Cardmember customer service, travel and concierge service: Required, twenty-four (24) hours per day, seven (7) days per week, one (1) telephone number (out of hours emergency travel service permissible)
- Third-party Service Providers - American Express vendor approval required
- Implement and use Premium Products Platform (PPP). Fees apply. Refer to Section 10.5.11, "Premium Product Platform (PPP) Fees," on page 409
- Servicing assessment
- Customer Relationship Management capability (CRM)
- Cardmember site for accessing product features and benefits
- Local language servicing

Cardmember Loyalty Program

- Cardmember Loyalty Programs - at least one (1) type of Cardmember Loyalty Program

Travel Benefits

- Airport lounge access - global annual membership with unlimited membership with unlimited complimentary access for primary Cardmember
- Car partner loyalty program - at least one (1) type of program
- Hotel partner loyalty program - at least one (1) type of program
- Travel Related Offer Program

Lifestyle Benefits

- Dining Program/Offers

Events Program

- Retail Program - at least two (2) forms of retail program

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Protection

- Travel Accident Insurance - the coverage level must be a minimum of $1,000,000 (USD) in the U.S./Canadian market/$500,000 (USD) in other markets or local socioeconomic equivalent, and higher than the coverage on the [Issuer Name] Max American Express® Card
- Emergency Assistance - this feature must be provided at a Tier 3 level
- Emergency Card Replacement
- Car Rental Insurance - required for U.S. and Canadian Issuers only
- Limited Liability for lost/stolen/counterfeit cards/fraud protection guarantee
- Concierge Service
- Luggage Delay Protection
- Luggage Loss Protection
- Retail Protection Program

Cardmember Communication

- Annual communications calendar: minimum six (6)

3.5.5 Product Tier: Debit

[Issuer Name] American Express® Debit Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] American Express® Debit Card:

- Payment Functionality - Debit
- Cash Access
- Cardmember Customer Service.
- Emergency Assistance - Tier 1
- Emergency Card Replacement
- Limited liability for lost/stolen/counterfeit cards/fraud protection guarantee

3.6 Blue Box Line Commercial Products

The following tables summarize the required and recommended features and benefits for American Express for Blue Box Line Commercial Products:

- Table 3-5, "Features and Benefits for Blue Box Line Small Business Commercial Products," on page 177
- Table 3-6, "Features and Benefits for Blue Box Line Corporate Commercial Products," on page 185

3.6.1 Blue Box Line Small Business Products

Small Business Products are aimed at businesses with fewer than 50 employees.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-5 Features and Benefits for Blue Box Line Small Business Commercial Products

Product Feature	[Issuer Name] Member Business American Express® Card	[Issuer Name] Select Business American Express® Card	[Issuer Name] Max Business American Express® Card	[Issuer Name] Icon Business American Express® Card	[Issuer Name] American Express® Business Purchasing Card	[Issuer Name] American Express® Travel Agency Account	[Issuer Name] American Express® Business Debit Card
Payment Functionality	Charge or Revolve	Charge or Revolve	Charge or Revolve	Charge or Revolve	Credit Only	Charge only	Debit
No Preset Spending Limit" functionality (if Charge Card)	Recommended	Recommended	Recommended	Recommended	--	Recommended	--
Minimum Credit Limit (where applicable)	$1,000 (USD)	$5,000 (USD)	$10,000 (USD)	$20,000 (USD)	--	--	--
Cash Access	Required	Required	Required	Required	--	--	Required
Year-End Summary of Charges	Required	Required	Required	Required	Required	Required	--
Air Addenda	Recommended	Recommended	Recommended	Recommended	--	Required	--
Cardless Account	--	--			Required	Recommended	--
Cardmember Employee ID and Cost Center	--	--	--	--	--	--	--
Company Liability Options	--	--	--	--	--	Required: Company Only	--
Corporate Billing Options	Required: Central Billing Only	Required: Central Billing Only	Required: Central Billing Only	Required: Central Billing Only	--	Required: Central Billing Only	--
Global Limits	--	--	--	--	Required	--	--
Issuer-Generated Data Files	--	--	--	--	--	--	--
Line Item Detail	--	--	--	--	--	--	--
Descriptive Travel/Customer Reference Data (matched and merged with charge data)	--	--	--	--	--	--	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-5 Features and Benefits for Blue Box Line Small Business Commercial Products (continued)

Product Feature	[Issuer Name] Member Business American Express® Card	[Issuer Name] Select Business American Express® Card	[Issuer Name] Max Business American Express® Card	[Issuer Name] Icon Business American Express® Card	[Issuer Name] American Express® Business Purchasing Card	[Issuer Name] American Express® Travel Agency Account	[Issuer Name] American Express® Business Debit Card
Merchant Category Restrictions	--	--	--	--	Required	Required	--
MIS Customized Reporting	--	--	--	--	Required	--	--
MIS Standard Reporting	--	--	--	--	--	--	--
Proactive Data Quality Processes	--	--	--	--	--	--	--
VAT/GST Information (in markets where applicable)	Recommended	Recommended	Recommended	Recommended		Recommended	--
Card Portfolio							
Basic Card	Required	Required	Required	Required	Required	Required	Required
Supplementary Cards	Recommended	Recommended	Recommended	Recommended	Required	--	--
Corporate Account Hierarchy	--	--	--	--	Required	--	--
Corporate Account Management	--	--	--	--	Required	--	--
Emergency Card Replacement	Required	Required	Required	Required	--	--	Required
Online Reconciliation/ Expense Reporting Tool	--	--	--	--	Required	--	--
Online Program Management	Recommended	Recommended	Recommended	Recommended	Required	Recommended	--
Card Fees							
Basic Card	Recommended	Recommended	Recommended	Recommended	Required	--	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-5 Features and Benefits for Blue Box Line Small Business Commercial Products (continued)

Product Feature	[Issuer Name] Member Business American Express® Card	[Issuer Name] Select Business American Express® Card	[Issuer Name] Max Business American Express® Card	[Issuer Name] Icon Business American Express® Card	[Issuer Name] American Express® Business Purchasing Card	[Issuer Name] American Express® Travel Agency Account	[Issuer Name] American Express® Business Debit Card
Supplementary Cards (charged for)	--	--	--	--	Required	--	--
Acquisition Requirements							
Field Sales Force	--	--	--	--	--	--	--
Engagement Requirements							
First 100 Days Programs	Recommended	Recommended	Recommended	Recommended	--	--	--
Servicing							
Cardmember Customer Service	Required	Required	Required	Required	Required	--	Required
Cardmember Online Account Access	Recommended	Recommended	Recommended	Recommended	Required	Recommended	--
Concierge Service	--	Recommended (if no Platinum)	Required	Required	--	--	--
Dedicated Operations Unit (for company-level servicing)	--	--	--	--	--	Recommended	--
Protection							
Business Travel Accident Insurance	--	--	--	--	--	--	--
Car Rental Insurance	Recommended	Recommended	Recommended	Recommended	--	--	--
Emergency Assistance	Required	Required (Tier 3 recommended)	Required (Tier 3 recommended)	Required (Tier 3 recommended)		Recommended	Required
Flight Delay and Cancellation Insurance	Recommended	Recommended	Recommended	Recommended	--	Recommended	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-5 Features and Benefits for Blue Box Line Small Business Commercial Products (continued)

Product Feature	[Issuer Name] Member Business American Express® Card	[Issuer Name] Select Business American Express® Card	[Issuer Name] Max Business American Express® Card	[Issuer Name] Icon Business American Express® Card	[Issuer Name] American Express® Business Purchasing Card	[Issuer Name] American Express® Travel Agency Account	[Issuer Name] American Express® Business Debit Card
Luggage Delay Protection	Recommended	Recommended	Recommended	Recommended	--	Recommended	--
Luggage Loss Protection	Recommended	Recommended	Recommended	Recommended	--	Recommended	--
Travel Accident Insurance	Recommended	Recommended	Recommended	Recommended	--	Recommended	--
Limited Liability for Lost/Stolen Card/Fraud Protection Guaranteed	Required	Required	Required	Required	Required	Required	Required
Loyalty Programs							
Cardmember Loyalty Program	Recommended	Recommended	Recommended	Recommended	--	--	--
Company Savings/Loyalty Program	Required	Required	Required	Required	--	Recommended	--
Virtual Currency							
Travel Benefits							
Airport Lounge Access	--	Recommended (if no Platinum)	Required	Required	--	--	--
Car Hire Loyalty Programs & Benefits	Recommended	Recommended	Required	Required	--	--	--
Global Hotel Program	--	Recommended	Required	Required	--	--	--
Hotel Partner Loyalty Programs	--	--	Required	Required	--	--	--
Local Airport Benefits	--	Recommended (if no Platinum)	Required	Required	--	--	--

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-5 Features and Benefits for Blue Box Line Small Business Commercial Products (continued)

Product Feature	[Issuer Name] Member Business American Express® Card	[Issuer Name] Select Business American Express® Card	[Issuer Name] Max Business American Express® Card	[Issuer Name] Icon Business American Express® Card	[Issuer Name] American Express® Business Purchasing Card	[Issuer Name] American Express® Travel Agency Account	[Issuer Name] American Express® Business Debit Card
Membership Travel Service (Travel Agency)	--	Recommended	Recommended	Recommended	--	--	--
Travel Tactical Offers Program	Recommended	Recommended	Required	Required	--	--	--
Lifestyle Benefits							
Business Offers & Services	Recommended	Recommended	Required	Required			--
Local & Global Dining Benefits	Recommended	Recommended	Required	Required			--
Local Exclusive Events & Global Events Access	Recommended	Recommended	Required	Required			--
Other Access Programs	Recommended	Recommended	Required	Required			--
Retail Offers, Programs & Services	Recommended	Recommended	Required	Required			--

Additional benefits, features, and functionality may be available in certain markets.

Please consult your AEGNS representative for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.6.1.1 [Issuer Name] Member Business American Express Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Member Business American Express® Card:

- Payment Functionality - a Charge or a Credit Card. The Credit Card product must have a minimum line of credit of $1,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended monthly cash limit of $1,000 (USD) or local socioeconomic equivalent
- Card Portfolio:
  - Minimum one (1) Basic Card
  - Provide option for Supplementary Cards, up to a maximum limit
  - May assess a fee for Supplementary Cards
- Cardmember Customer Service
- Central Billing
- Emergency Assistance
- Emergency Card Replacement
- Company Savings/Loyalty Program
- Year-end Summary of Charges
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

3.6.1.2 [Issuer Name] Select Business American Express Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Select Business American Express® Card:

- Payment Functionality - a Charge or a Credit Card. The Credit Card product must have a minimum line of credit of $5,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended monthly minimum cash limit of $1,000 (USD) or local socioeconomic equivalent
- Card Portfolio:
  - Minimum one (1) Basic Card
  - Provide option for Supplementary Cards, up to a maximum limit
  - May assess a fee for Basic and Supplementary Cards
- Cardmember Customer Service
- Central Billing
- Emergency Assistance
- Emergency Card Replacement
- Company Savings/Loyalty Program
- Year-End Summary of Charges
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.6.1.3 [Issuer Name] Max Business American Express Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Max Business American Express® Card:

- Payment functionality - a Charge or a Credit Card. The Credit Card product must have a minimum line of credit of $10,000 (USD) or local socioeconomic equivalent
- Cash Access - with a recommended monthly cash limit of $1,000 (USD) or local socioeconomic equivalent
- Card Portfolio:
  - Minimum one (1) Basic Card, with choice of plastic or metal form factor
  - Provide option for Supplementary Cards, up to a maximum limit
  - May assess a fee for Basic and Supplementary Cards
- Cardmember Customer Service
- Concierge Service
- Central Billing
- Emergency Assistance
- Emergency Card Replacement
- Travel Accident Insurance - with a minimum coverage level greater than the level of the [Issuer Name] Select Business American Express® Card
- Company Savings/Loyalty Program
- Year-End Summary of Charges
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Benefits:
  - Airport Lounge Access - a minimum of one (1) program
  - Car Hire Loyalty Program - a minimum of one (1) program
  - Hotel Partner Loyalty Program - a minimum of one (1) program
  - Travel Tactical Offers Program
  - Lifestyle Benefits - a minimum of one (1) program
  - Business Offers Program

3.6.1.4 [Issuer Name] Icon Business American Express Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Icon Business American Express® Card:

- Payment Functionality - a Charge or a Credit Card. The Credit Card product must have a minimum line of credit of $20,000 (USD) or local socioeconomic equivalent
- Extended Payment terms - greater than the level of the [Issuer Name] Max Business American Express® Card
- Cash Access - with a recommended monthly cash limit of $1,000 (USD) or local socioeconomic equivalent
- Card Portfolio:
  - Minimum one (1) Basic Card, with choice of plastic or metal form factor
  - Provide option for Supplementary Cards, up to a maximum limit
  - May assess a fee for Basic and Supplementary Cards
- Cardmember Customer Service

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Premium Concierge Service
- Central Billing
- Emergency Card Replacement
- Travel Accident Insurance - with a minimum coverage level greater than the level of the [Issuer Name] Platinum Business American Express® Card
- Company Savings/Loyalty Program
- Year-End Summary of Charges
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee
- Benefits:
  - Airport Lounge Access - a minimum of one (1) program
  - Car Hire Loyalty Program - a minimum of one (1) program
  - Hotel Partner Loyalty Program - a minimum of one (1) program
  - Travel Tactical Offers Program
  - Lifestyle Benefits - a minimum of one (1) program
  - Business Offers Program

3.6.1.5 [Issuer Name] American Express Business Purchasing Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] American Express® Business Purchasing Card:

- Payment functionality - a Credit Card only
- Cardless Account
- Global Limits
- Merchant Category Restrictions
- MIS Customized Reporting
- Corporate Account Hierarchy
- Corporate Account Management
- Online Reconciliation/Expense Reporting Tool
- Online Program Management
- Cardmember Customer Service
- Cardmember Online Account Access
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.6.1.6 [Issuer Name] American Express Travel Agency Account

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] American Express® Travel Agency Account:

- Payment Functionality - Charge only
- Central Billing
- Company Liability Options
- Air Addenda
- Merchant Category Restrictions
- Year-End Summary of Charges
- Limited Liability for Lost/Stolen Card/Fraud Protection Guarantee

3.6.1.7 [Issuer Name] American Express Business Debit Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] American Express® Business Debit Card:

- Payment Functionality - Debit
- Cash Access
- Cardmember Customer Service
- Emergency Assistance
- Emergency Card Replacement
- Limited liability for lost/stolen/counterfeit cards/fraud protection guarantee

3.6.2 Blue Box Line Corporate Products

Table 3-6, "Features and Benefits for Blue Box Line Corporate Commercial Products," on page 185 summarizes the required and recommended features and benefits for the Blue Box Line Corporate Commercial Products.

Refer to Section 3.7, "Descriptions of Product Features and Benefits," on page 191 for more detail. .

Table 3-6 Features and Benefits for Blue Box Line Corporate Commercial Products

Product Feature	[Issuer Name] Corporate American Express® Card	[Issuer Name] Gold Corporate American Express® Card	[Issuer Name] Platinum Corporate American Express® Card	[Issuer Name] American Express® Business Travel Account
Payment Functionality	Charge only	Charge only	Charge Only	Charge only
No Preset Spending Limit" functionality (if Charge Card)	Recommended	Recommended	Recommended	Recommended
Minimum Credit Limit (where applicable)	--	--	--	--
Cash Access	Required	Required	Required	--
Year-End Summary of Charges	--	--	--	--
Air Addenda	Recommended	Recommended	Recommended	Required

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-6 Features and Benefits for Blue Box Line Corporate Commercial Products (continued)

Product Feature	[Issuer Name] Corporate American Express® Card	[Issuer Name] Gold Corporate American Express® Card	[Issuer Name] Platinum Corporate American Express® Card	[Issuer Name] American Express® Business Travel Account
Cardless Account	--	--		Recommended
Cardmember Employee ID and Cost Center	Required	Required	Required	--
Company Liability Options	Required	Required	Required	Required: Company Only
Corporate Billing Options	Required	Required	Required	Required: Central Billing Only
Global Limits	Recommended	Recommended	Recommended	Recommended
Issuer-Generated Data Files	Recommended	Recommended	Recommended	Recommended
Line Item Detail	--	--	--	--
Descriptive Travel/Customer Reference Data (matched and merged with charge data)	--	--	--	Required
Merchant Category Restrictions	--	--	--	Required
MIS Customized Reporting	Recommended	Recommended	Recommended	Recommended
MIS Standard Reporting	Required	Required	Required	Required
Proactive Data Quality Processes	--	--	--	Recommended
VAT/GST Information (in markets where applicable)	Recommended	Recommended	Recommended	Recommended
Card Portfolio				
Basic Card	Required	Required	Required	Required
Supplementary Cards	Recommended	Recommended	Recommended	--
Corporate Account Hierarchy	Required	Required	Required	Required
Corporate Account Management	Required	Required	Required	Required
Emergency Card Replacement	Required	Required	Required	--
Online Reconciliation/ Expense Reporting Tool	Recommended	Recommended	Recommended	Recommended

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-6 Features and Benefits for Blue Box Line Corporate Commercial Products (continued)

Product Feature	[Issuer Name] Corporate American Express® Card	[Issuer Name] Gold Corporate American Express® Card	[Issuer Name] Platinum Corporate American Express® Card	[Issuer Name] American Express® Business Travel Account
Online Program Management	Recommended	Recommended	Recommended	Recommended
Card Fees				
Basic Card	Recommended	Recommended	Recommended	--
Supplementary Cards (charged for)	Recommended	Recommended	Recommended	--
Acquisition Requirements				
Field Sales Force	Required	Required	Required	Required
Engagement Requirements				
First 100 Days Programs	Recommended	Recommended	Recommended	Recommended
Servicing				
Cardmember Customer Service	Required	Required	Required	--
Cardmember Online Account Access	Recommended	Recommended	Recommended	Recommended
Concierge Service	--	Recommended	Recommended	--
Dedicated Operations Unit (for company-level servicing)	Required	Required	Required	Required
Protection				
Business Travel Accident Insurance	Recommended	Recommended	Recommended	Recommended
Car Rental Insurance	Recommended	Recommended	Recommended	--
Emergency Assistance	Required	Required (Tier 3 recommended)	Required (Tier 3 recommended)	Recommended
Flight Delay and Cancellation Insurance	Recommended	Recommended	Recommended	Recommended
Luggage Delay Protection	Recommended	Recommended	Recommended	Recommended
Luggage Loss Protection	Recommended	Recommended	Recommended	Recommended
Travel Accident Insurance	Required	Required	Required	Required
Limited Liability for Lost/Stolen Card/Fraud Protection Guaranteed	Required	Required	Required	Required

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 3-6 Features and Benefits for Blue Box Line Corporate Commercial Products (continued)

Product Feature	[Issuer Name] Corporate American Express® Card	[Issuer Name] Gold Corporate American Express® Card	[Issuer Name] Platinum Corporate American Express® Card	[Issuer Name] American Express® Business Travel Account
Loyalty Programs				
Cardmember Loyalty Program	Recommended	Recommended	Recommended	--
Company Savings/Loyalty Program	Recommended	Recommended	Recommended	Recommended
Travel Benefits				
Airport Lounge Access	--	--	--	--
Car Hire Loyalty Programs & Benefits	--	--	--	--
Global Hotel Program	--	--	--	--
Hotel Partner Loyalty Programs	--	--	--	--
Local Airport Benefits	--	--	--	--
Membership Travel Service (Travel Agency)	--	Recommended	Recommended	--
Travel Tactical Offers Program	--	--	--	--
Lifestyle Benefits				
Business Offers & Services				
Local & Global Dining Benefits				
Local Exclusive Events & Global Events Access				
Other Access Programs				
Retail Offers, Programs & Services				

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.6.2.1 [Issuer Name] Corporate American Express Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Corporate American Express® Card:

- Payment Functionality - Charge only
- Cash Access
- Cardmember Customer Service
- Travel Accident Insurance - the coverage level must be a minimum of $100,000 (USD) or local socioeconomic equivalent
- Corporate Billing Options
- Company Liability Options
- Corporate Account Management
- Corporate Account Hierarchy
- Dedicated Operations Unit (for company-level servicing)
- Emergency Assistance
- Emergency Card Replacement
- Field Sales Force
- Cardmember Employee ID and Cost Center
- MIS Standard Reporting

3.6.2.2 [Issuer Name] Gold Corporate American Express Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Gold Corporate American Express® Card:

- Payment Functionality - a Charge Card
- Cash Access
- Cardmember Customer Service
- Travel Accident Insurance - the coverage level must be greater than the level on the [Issuer Name] Corporate American Express® Card
- Corporate Billing Options
- Company Liability Options
- Corporate Account Management
- Corporate Account Hierarchy
- Dedicated Operations Unit (for company-level servicing)
- Emergency Assistance
- Emergency Card Replacement
- Field Sales Force
- Cardmember Employee ID and Cost Center
- MIS Standard Reporting

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.6.2.3 [Issuer Name] Platinum American Express Corporate Card

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] Platinum American Express® Corporate Card:

- Payment functionality - a Charge only
- Cash Access - with a recommended monthly cash limit of $1,000 (USD) or local socioeconomic equivalent
- Cardmember Employee ID and Cost Center
- Corporate Billing Options
- Company Liability Options
- MIS Standard Reporting
- Corporate Account Management
- Corporate Account Hierarchy
- Emergency Card Replacement
- Field Sales Force
- Cardmember Customer Service
- Dedicated Operations Unit (for company-level servicing)
- Emergency Assistance
- Travel Accident Insurance

3.6.2.4 [Issuer Name] American Express Business Travel Account

Issuers are required to provide the following minimum features and benefits for the [Issuer Name] American Express® Business Travel Account:

- Payment Functionality - Charge only
- Travel Accident Insurance - the coverage level must be a minimum of $100,000 (USD) or local socioeconomic equivalent
- Central Billing
- Company Liability Options
- Corporate Account Hierarchy
- Corporate Account Management
- Dedicated Operations Unit (for company-level servicing)
- Air Addenda
- Descriptive Travel/Customer Reference Data (matched and merged with Charge data)
- Field Sales Force
- Merchant Category Restrictions
- MIS Standard Reporting

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7 Descriptions of Product Features and Benefits

This section provides a summary description of the required and recommended product features and benefits associated with Consumer and Commercial products. For Prepaid Card features and benefits, refer to Section 3.2.5, "Prepaid Cards," on page 129 and Section 3.9.3, "Additional Services for Prepaid Cards," on page 211.

Some of the features and benefits described in this section can be provided by American Express when purchased through AEGNS. However, feature availability may vary by market. For all features made available through AEGNS, the provisions of the insurance policy or policies and detailed descriptions of the programs govern. Contact your AEGNS representative to discuss details and specific availability which may vary by product in your market.

3.7.1 Air Addenda

When airline tickets are charged to a commercial product, this feature provides customers with additional, detailed information about the ticket: ticket number (or booking reference, in the case of ticketless airlines), routing (sector-by-sector airport names/codes, class of service, airline carrier) passenger name, fare basis, etc. Addenda information must be integrated with the basic Transaction data and appear on the statement (in abridged form if necessary) as well as in any transaction data files provided to the client.

3.7.2 Airport Lounge Access Program

This program enables Cardmembers to enjoy access to participating airport lounges. Such access may be provided to the Cardmember only or to the Cardmember and his or her guests.

Participants that desire to operate, manage, or control access to airport lounges that display any Amex Licensed Marks or branding must obtain AEGNS approval for establishment of such lounges. Such approval shall be granted in AEGNS' sole discretion, and may be conditioned upon satisfaction of AEGNS requirements relating to the features, benefits, and amenities offered to Cardmembers in such lounge.

Participants that operate, manage, or control access to any such American Express-branded airport lounge must ensure that all Cardmembers who hold The Platinum Card® and/or The Centurion® Card issued by any Issuer are granted access to such lounge on at least the same terms and conditions, including guest access, as all other Cardmembers, including Cardmembers who hold The Platinum Card® and/or The Centurion® Card issued by the Participant.

Participants seeking reimbursement for lounge usage of other Issuers' Cardmembers must enter into a separate agreement with an American Express Entity setting out the relevant terms and conditions for reimbursement and related processes.

3.7.3 Business Travel Accident Insurance

This feature is an extension to Travel Accident Insurance which automatically provides twenty-four (24) hour, door-to-door coverage during business trips lasting up to thirty (30) days, for accidents resulting in dismemberment or death while the employee is traveling for business. The transport component of the trip must be on a licensed common carrier with a ticket charged to the product.

This feature is required with a minimum coverage of $100,000 (USD) or up to whatever competitive benchmarking and research indicate is appropriate.

3.7.4 Car Rental Insurance

This program provides Cardmembers and their accompanying spouse and children coverage in excess of any existing insurance against damage to or loss of a rental automobile rented worldwide with the Card. This coverage applies when the entire cost of the car rental has been purchased with the Card or when rewards points have been used, and when the insurance waiver has been declined from the rental agency.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.5 Cardless Account

This type of Commercial Product is used by a group of employees in a client organization and does not require issuance of a physical Card.

Some local market regulations may mandate the issuance of a physical card for all products.

3.7.6 Cardmember Communication

As part of the Customer Engagement process, Participants are required to commit to a comprehensive annual communication plan that includes Acquisition, Welcome, and a frequent channel (e-newsletter or Direct Mail) to ensure ongoing communication with Cardmembers.

3.7.7 Cardmember Customer Service

For details on Cardmember Customer Service, refer to Section 3.9.2.1, "Cardmember Customer Service," on page 209.

3.7.8 Cardmember Employee ID and Cost Center

This feature provides the ability for Cardmembers or program administrators to specify an employee ID and/or cost center code to be associated with each Card. This information must be kept on file by the Issuer and be able to be included in Issuer-generated data files which are produced for the client.

3.7.9 Cardmember Loyalty Programs

This feature allows Cardmembers to earn rewards for their spending activity. There are four (4) types of Cardmember Loyalty Programs, as listed below:

- **Rewards Program**: This feature allows Cardmembers to earn points based on their spending that can be redeemed for various rewards (for example, travel, retail, dining, etc.).
- **Cash Rebate Rewards Program**: This feature allows Cardmembers to earn an annual rebate on non-cash charges.
- **Cardmember Values Program**: This feature allows Cardmembers to receive, on an ongoing basis, "special offers" from S/Es of select merchandise categories that are consistent with the positioning of the Card.
- **Virtual Currency Program**: This feature allows Cardmembers to earn Virtual Currency Rewards on non-cash charges.

Contact your AEGNS representative to discuss feature availability in your market.

3.7.10 Cardmember Online Account Access Services

This feature allows Cardmembers to check their Account balance information in a secured area online. In addition to enabling Cardmembers to access up to six (6) months of Account information and view itemized expenses for each statement period, other services such as balance transfer, downloading online statements, and a year-end summary analysis are also recommended.

3.7.11 Travel Servicing

Travel Servicing is the name for travel agency services provided to Platinum and The Centurion® Card Cardmembers, and is a required feature of the Platinum and The Centurion® Card.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.12 Choice of Billing Frequency

This feature provides customers with a choice in how frequently their Account cuts off and a bill is generated. For example, an Issuer might use monthly billing as standard but offer customers the option of bi-weekly. It is most useful for commercial clients, where it can enable a Card program to synchronize with the client's accounting or processing schedule. This feature is not applicable to Account Card products.

3.7.13 Choice of Cycle Cut Dates

This feature provides customers with a choice in the timing of when their Account cuts off and payment falls due. For example, in the case of monthly billing, clients may be offered a choice between beginning of the month, middle of the month, or end of the month. It is most useful for commercial clients, where it can enable a Card program to align more closely with the client's accounting or processing schedule. Where this feature is offered, clients must be given a minimum of three (3) options (and preferably eight (8) or more), spread evenly throughout the billing cycle. This feature is not applicable to Account Card products.

3.7.14 Company Savings/Loyalty Program

These programs offer valuable savings on business and travel related purchases, as negotiated by the Issuer and/or American Express. Offers must be pre-negotiated, business-oriented, and preferably unique. Categories may include, for example:

- Air/Rail, e.g., special ticket rates or upgrades
- Hotels, e.g., special rates, free upgrades, or meals
- Car Rental, e.g., special rates or upgrades
- Non-T&E, e.g., special rates on couriers, computer equipment, office supplies, etc.

3.7.15 Concierge Service

This feature is defined as non-emergency personal assistance such as arranging dining, entertainment, sports bookings, business center referrals, gift location, or flower ordering. When at home or while traveling outside the country, the Cardmember can expect, where possible, assistance in the local language concerning:

- Travel Information such as: weather, customs regulations, visa and vaccination requirements
- Cultural information on local special events
- Attractions and entertainment possibilities
- Information and referrals for restaurants, theaters, concerts, and special events
- Business arrangements for related services, such as secretarial and translation services

Contact your AEGNS representative to discuss feature availability in your market.

3.7.16 Corporate Account Hierarchy

Management information on commercial products is closely linked to the structure of a customer's account, that is, their corporate hierarchy or hierarchies.

This feature requires Issuers to develop and build appropriate systems to capture and maintain a client’s hierarchy, which is critical to enabling valuable Management Information Systems (MIS) reporting.

At a minimum, Issuers must support basic single-level grouping of Cards under a company master account. AEGNS recommends that Issuers support more complex hierarchies with additional levels of grouping via a “control account.”

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.17 Corporate Account Management

This feature requires that the Issuer provide a single point of contact to manage the day-to-day relationship with clients at the program administrator/decision maker level.

3.7.18 Corporate Billing Options

3.7.18.1 Corporate Products

This feature provides the Commercial clients with various billing options for their Cardmembers. These options include:

- Central Bill/Central Pay - the Charges made by Cardmembers are billed and paid from a central statement that includes all Charges for all Cardmembers, sub-totaled by Cardmember.
- Individual Bill/Individual Pay - the Charges made by Cardmembers are billed and paid individually by the Cardmember.
- Individual Bill/Central Pay - the Charges made by Cardmembers are billed individually to the Cardmember and paid centrally by the client.

Certain options may be restricted by local market regulations.

3.7.18.2 Small Business Products

Central Bill/Central Pay is the only option available and required for Small Business Products.

3.7.19 Company Liability Options

This feature provides the Corporate Card client with the following liability options:

- Company Liability - The Corporate Card client is liable for all Cardmember Charges.
- Individual Liability - The Corporate Card client is not liable for any Charges; only the Cardmember is liable.
- Joint and Several Liability - Both the Corporate Card client and the Cardmember are liable jointly and individually.
- Company Liability Waiver Option - The Issuer may offer to Corporate Card clients insurance to offset unauthorized, unpaid Cardmember Charges in conjunction with Corporate Joint and Several Liability. This feature provides coverage to the Corporate Card client to limit their liability for delinquent or unpaid Cardmember Charges made by their employee Corporate Cardmembers.

Certain options may be restricted by local market regulations.

3.7.20 Dedicated Operations Unit (for Company-Level Service)

This feature requires the Issuer to provide a dedicated corporate operations and program administration service. The dedicated operations unit supports clients' program administrators regarding billing issues, reconciliation, additional products, cancellations, replacements, etc.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.21 Descriptive Travel/Customer Reference Data (Matched and Merged with Charge Data)

This feature enables customers to receive, along with each Transaction, additional reference data that meets their specific requirements. Depending on the customer, this may include information such as invoice number, cost center, project code, requisition number, employee ID, pre-purchase approval codes, etc. Some of these fields may be collected as standard while others are available for customers to specify the required content. It is most useful for products that are billed and reconciled centrally, as it streamlines the reconciliation and accounting process.

The additional data must be collected either by the Merchant or (for products designed to be lodged with a travel agent) by the travel booking system, and must be matched and merged with the basic transaction data so they appear together on the statement.

This feature should provide a minimum of four (4) customer reference fields, each with a minimum of 50 characters.

3.7.22 Dining Program/Offers

This program provides valuable dining offers from the following dining categories consistently throughout the year. These categories include:

- Dining at special rates, or with free desserts or appetizers
- Reserved tables in restaurants in which it is difficult to get a reservation
- Access to special dining and wine tasting events

3.7.23 Direct Debit of Monthly Balance or Minimum Payment

Providing Cardmembers the option of having their monthly Card balance or minimum payment debited from their bank account is a required feature if it is considered a local business practice. It is offered as a convenience to the Cardmember and essentially removes a task from monthly bookkeeping.

3.7.24 Electronic Remittance File

For commercial clients using the central payment option, this feature ensures that remittances are allocated against the correct Card numbers. The Issuer must be able to receive an electronic remittance allocation file from the company (transmitted via a secure encrypted channel), link it with a corresponding remittance (typically received via wire transfer or automated clearing house) and credit the individual Cardmember Accounts accordingly.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.25 Emergency Assistance

Emergency Assistance includes a twenty-four (24) hour emergency referral service to local medical and legal providers worldwide for covered Cardmembers, as well as emergency ticket replacement, pre-trip advice (e.g., inoculation, visa, customs information), interpreters, and emergency Cash Advances.

There are three (3) Emergency Assistance Tier levels:

- **Emergency Assistance Tier 1** includes emergency transportation ticket replacement and emergency Cash Advances, which are to be charged to the Cardmember's Account and subject to Authorization by the Issuer. Coverage shall extend to the Cardmember's spouse, legally dependent children under nineteen (19) years of age, and any additional Cardmembers, their spouses, and legally dependent children under nineteen (19) years of age.
- **Emergency Assistance Tier 2** includes the core features of Emergency Assistance plus medical transportation or medical evacuation coverage.
- **Emergency Assistance Tier 3 (Premium Emergency Assistance)** includes the core features of Emergency Assistance Tier 2 plus medical expense coverage.

Contact your AEGNS representative to discuss feature availability in your market.

3.7.26 Emergency Card Replacement

Issuers are required to provide Emergency Card Replacement (ECR) service to their Cardmembers.

Issuers should make reasonable efforts to provide in-Territory ECR for their own Cardmembers within twenty-four (24) hours when the Cardmember is in the Territory of issuance, and expedite ECR delivery when the Cardmember is outside the Territory of issuance.

Emergency replacement Cards must be authorized with a maximum valid date of sixty (60) days from the date of issue. Issuers must request valid photo identification from the Cardmember prior to delivering the ECR. Refer to "S/E and ATM Standards" chapter beginning on page 214 for information regarding acceptable forms of ID.

3.7.27 English Language Support

In markets where the local language is not English, this feature helps support global and multinational Corporate clients whose staff may not all be fluent in the local language. Issuers should be able to provide, upon request, English-speaking staff to support client implementations, answer Cardmember inquiries and assist with company-level servicing. In addition, where possible, English-language versions of key customer-facing Documentation (such as application forms, welcome packs, program administrator guides) and MIS reports should also be available upon request.

3.7.28 Enhanced Global Management Information System (eGMIS)

This feature requires Issuers that manage global/multinational clients to establish and maintain a daily data feed conforming to the "eGMIS" specification. For more details, refer to the *Enhanced Global Management Information Systems Guidelines* on Knowledge Base. Use the Search function to locate this document.

3.7.29 Field Sales Force

This requirement involves the Issuer establishing and training a field sales force with deep product knowledge and strong consultative selling capabilities.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.30 Flight Delay and Cancellation Insurance

This feature applies if the departure of a covered Cardmember's confirmed scheduled flight from any airport is delayed by four (4) hours or more. The Cardmember will be reimbursed for charges incurred during the period of the delay for restaurant meals or refreshments and/or hotel accommodation up to a specified amount. The ticket must have been charged to their Card. The insurance also applies if the flight is cancelled or if the covered Cardmember is prevented from boarding the aircraft due to overbooking and no alternative transportation is made available to the covered Cardmember within four (4) hours of the scheduled departure time of such flight. Coverage extends to the covered Cardmember's spouse, legally dependent children under twenty-three (23) years of age, and any additional Cardmembers, their spouses, and legally dependent children under twenty-three (23) years of age. Contact your AEGNS representative to discuss feature availability in your market.

3.7.31 Global Limits

This feature enables customers to manage their spending by setting limits on what Transactions will be accepted. Limits can include the following:

- Total spend per billing cycle
- Cash withdrawals
- Industry/Merchant category
- Transaction size
- Cap (revolving limit)
- Relationship spend limits (calculated at corporation rather than Cardmember level)
- Preferred Supplier Lists
- Preferred Supplier Thresholds

3.7.32 Global Rebates

This feature requires Issuers to be able to offer financial incentives/rebates to commercial clients, usually calculated according to billing volume and cost drivers such as client held days, loyalty program expenses, etc. These are typically only offered to very large clients in a competitive bidding situation, and may be negotiated centrally as part of a global American Express deal. Issuers should be aware that as a consequence of this centralization, American Express will negotiate terms with clients that enable the Issuer to benefit from the global relationship.

Note that this requirement may be waived where local market conditions make it economically unfeasible.

3.7.33 Issuer-Generated Data Files

This feature requires the Issuer, upon client request, to produce electronic data files and transmit them securely to clients.

The data sets must provide:

- Cardmember Activity - Transaction information such as Cardmember name, Account number, tax information, supplier name, etc., and,
- Cardmember Listing - Information such as Cardmember name, Account number, cost center, Expiration Date, Account status, Account limits and type.

In addition, for the Business Travel Account product, this feature should provide an electronic billing support file, produced at the same time as the statement and including all Transactions and data fields from the statement as well as any further Descriptive Travel/Customer Reference Data Fields that are captured. The billing amounts on this file must reconcile to the statement.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.34 Limited Liability for Lost/Stolen Cards

This feature provides Cardmembers full or partial liability protection if a Card is reported lost or stolen within a specified period.

3.7.35 Line Item Detail

This feature requires the Issuer to provide a breakdown of each Transaction to the invoice line-item level (for example: part number, description, quantity, and unit cost.) For hotel charges, this data corresponds to the folio that is produced upon checkout.

3.7.36 Luggage Delay Protection

This feature automatically applies to a covered Cardmember's accompanied luggage, which was checked with a licensed common carrier on a flight where the ticket was charged to the Card and is not delivered within six (6) hours of the Cardmember's arrival at the scheduled destination point (not point of origin). The covered Cardmember will be reimbursed for charges incurred at such destination for the emergency purchase of essential clothing and requisites up to a specified dollar amount. Coverage extends to the covered Cardmember and the covered Cardmember's spouse, legally dependent children under twenty-three (23) years of age, and any additional Cardmembers, their spouses, and legally dependent children under twenty-three (23) years of age. Contact our AEGNS representative to discuss feature availability in your market.

3.7.37 Luggage Loss Protection

This feature automatically provides coverage, up to a specified amount, for baggage loss and damage in excess of the airline coverage for a covered Cardmember who flies on a scheduled airline when the ticket is charged to their Card. Coverage extends to the covered Cardmember and the covered Cardmember's spouse, legally dependent children under twenty-three (23) years of age, and any additional Cardmembers, their spouses, and legally dependent children under twenty-three (23) years of age. Contact your AEGNS representative to discuss feature availability in your market.

3.7.38 Management Information System (MIS) Standard Reporting

This feature requires Issuers that manage local/national clients to provide a standard management information system reporting package. Unless indicated otherwise, this means the following:

- Monthly Statement of Account (CBCP & IBCP)
- Card Account Financial Detail (IBIP)
- Consolidated Monthly Financial Summary
- Account Aging Report
- Vendor Report
- Account Handling Report
- Account Expenditure Analysis
- Account Billing Address
- Spend by Account (Current Month and Year-to-Date)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

In addition, the following reports may be offered on the Business Travel Account Product:

- Spend Comparison Report
- Airline Usage Report
- Top 10 Air Routings
- Traveler Analysis
- Customer Reference Analysis
- Trip Requisition Analysis

3.7.39 Merchant Category Restrictions

This feature ensures that a Card or Account can only be used at Merchants in certain pre-defined categories, by automatically blocking all other categories at the authorization stage. It is appropriate for products which are only designed for certain types of spending, and offers two (2) main benefits: reduced potential for fraud, and greater consistency of Merchant transaction data (e.g., air addenda).

3.7.40 MIS Customized Reporting

This feature requires the Issuer to provide commercial clients with flexible tools for querying data and building reports.

3.7.41 Online Card Application Form

This feature provides an online application form which prospective customers can complete and submit electronically. This form can also be printed and submitted via postal services or fax.

3.7.42 Online Fraud Protection Guarantee

This feature warrants that Cardmembers will not be held responsible for any unauthorized Charges when using American Express Cards to make purchases online. This feature encourages customers to use American Express Cards when shopping online by providing enhanced security and service, and is offered at no additional cost to Cardmembers.

3.7.43 Online Program Management

This feature enables commercial client program administrators to perform key Account maintenance functions online, quickly, and conveniently without having to phone Operations or their Corporate Account Management.

3.7.44 Online Reconciliation/Expense Reporting Tool

This feature enables commercial clients to easily review, reconcile, justify, reallocate, and approve their American Express Transactions. Issuers may choose to build it themselves, although it is recommended to Participants with an experienced expense reporting vendor such as Concur.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.45 Open Item Billing

This feature affects how the Issuer handles cases where a client has not paid their Account balance in full, for example because certain charges are disputed or have not been reconciled. It requires Issuers to provide, as part of the statement, an itemized list of any charges still unpaid (or part-paid) from the previous billing cycle. By contrast, without Open Item Billing, Issuers need only report the total balance outstanding from the previous billing cycle. As a result, the Account aging process happens at the Transaction level.

If possible, this feature should provide an electronic method (e.g., website or data file) for clients to notify which charges are being disputed and which are paid, as well as an automated process for using this information to allocate incoming remittances.

3.7.46 Option to Extend Payment Terms

This feature allows Issuers to grant Cardmembers an extension to the standard payment terms, where this is agreed as part of the client contract. It is typically invoked to address the needs of large corporate clients with complex processes for expense claims or accounts payable, making it difficult to meet the Issuer's normal deadline for payment. Where this option is implemented, any interest or late payment fees must be calculated in accordance with the extended term and not applied until said term has elapsed.

This requirement may be waived where local market conditions make it economically unfeasible.

3.7.47 Premium Product Platform (PPP)

The Premium Product Platform (PPP) is a service delivery tool which is made available for a fee to both Issuers and their contracted service vendors which have been approved by American Express. This tool has been specifically designed to support servicing teams to deliver the premium level of service required on the Platinum and Centurion portfolios. The Premium Product Platform (PPP) provides the following functionality and core modules: Person Account, Benefit Content, Recommendations, Elite Tier Registrations, Metrics, and Customer Preferences. These core modules are required to be sourced from the Premium Product Platform (PPP). In addition, Issuers can select Case Management. Refer to Section 10.5.11, "Premium Product Platform (PPP) Fees," on page 409.

Note: Customer Preferences and Case Management modules are required to be sourced from the Premium Product Platform (PPP) unless otherwise approved by AEGNS.

3.7.48 Pre-Set Spending Limits

This feature provides the advantage of customized spending controls and restrictions to regulate and manage spending. Limits can include:

- Limits that set a maximum expenditure per Transaction
- Monthly limits setting maximum totals for expenditures
- Preferred supplier restrictions that limit purchases to a selected supplier

For the [Issuer Name] American Express® Generation Card, the basic Cardmember defines the pre-set spending limit. The basic Cardmember can also adjust the pre-set spending limit or cancel the Card. The Issuer may define minimum and maximum limits to the pre-set spending limit.

3.7.49 Proactive Data Quality Processes

For Transactions where additional data is expected (for example: air addenda, descriptive travel data, or line item detail), this feature requires Issuers to monitor the quality and completeness of such data and, when gaps are identified, to follow up with the data source and close the gap as much as possible. This should preferably be done prior to sending the data to customers.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.50 Product-Designated Website Pages

This feature provides a product-designated website (e.g., Blue Zone for Blue from American Express) that allows Cardmembers of that specific product to obtain product information, such as features and benefits, special offers, chat rooms, and useful financial tools.

3.7.51 Promotional Program Capability

Promotional Program capability is a feature that drives spend and loyalty by closing the redemption loop in local S/E commerce utilizing the AEGN. It allows participating S/Es to provide a "coupon-less" discount to Cardmembers in the form of a billing statement credit.

Issuers designated in Table 4-4, "Promotional Program Markets," on page 233 must support and notify AEGNS of their ability to process these Transactions.

Issuers must also comply with Promotional Program servicing requirements outlined in the *Promotional Program Capability Implementation Guide.*

Refer to Section 4.2.20.7, "Promotional Program Capability," on page 233 and Table 4-4, "Promotional Program Markets," on page 233 for additional information related to designated markets.

Refer to Section 7.10.9, "Promotional Program Transactions," on page 362 for additional information related to disputes processed on a Promotional Program Transaction.

Refer to the Network Specifications manuals and the *Codes Reference Guide* for Promotional Program Transaction message information.

3.7.52 Publishing Magazine Title

A quality quarterly publication featuring products and destinations relevant to Cardmember lifestyle. The premium product magazine is a key part of the overall strategy of American Express for communicating its value story to Cardmembers.

3.7.53 Insurance Programs

Retail programs provide Cardmembers with coverage for their retail purchases. There are three (3) types of Retail Programs.

3.7.53.1 Warranty Protection

This feature extends the term of the original manufacturer's warranty on certain items purchased entirely with the Card for a period of time equal to the duration of the original manufacturer's warranty plus up to one (1) additional year on warranties of five (5) years or less. Coverage is limited to covered products costing a specific amount or less, up to a specified amount per Cardmember per year. Contact your AEGNS representative to discuss feature availability in your market.

3.7.53.2 Theft and Damage Protection

This feature protects a covered item purchased entirely with the Card against accidental damage and theft for ninety (90) days from the date of purchase, up to a specified amount per occurrence and a specified amount per Cardmember per year, in excess of other applicable insurance. For certain items, coverage is limited to a specified amount per occurrence regardless of the number of items for which a claim is made. Contact your AEGNS representative to discuss feature availability in your market.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.53.3 Return Protection

This feature provides credit for undamaged eligible retail items that Cardmembers are unable to return to the S/E due to specified reasons. Items must be purchased entirely with the Card and claims must be made within ninety (90) days from the date of purchase. Contact your AEGNS representative to discuss feature availability in your market.

3.7.54 Insurance Programs

Retail Protection offers excess insurance coverage on certain items purchased with Cards against accidental damage and theft during the first ninety (90) days following the purchase.

3.7.55 Tax Invoice Capture/Presentment

This feature requires the Issuer to receive legal invoices from the supplier, match them with the corresponding American Express Transactions, and present the result to customers electronically. It enables significant time savings for commercial clients by eliminating the manual step of reconciling between Card statements and supplier invoices, while still supporting VAT reclaim and meeting audit requirements.

This feature is subject to local market regulations governing the validity of electronic invoicing.

3.7.56 Travel Accident Insurance

This feature automatically provides coverage for accidental death and dismemberment while a Cardmember is traveling on a licensed common carrier with a ticket charged to their Card. Coverage extends to the covered Cardmember and the covered Cardmember's spouse, legally dependent children under twenty-three (23) years of age, and any additional Cardmembers, their spouses and legally dependent children under twenty-three (23) years of age, provided that the beneficiary's travel ticket was purchased on their Card. Contact your AEGNS representative to discuss feature availability in your market.

3.7.57 Travel Accident Insurance - Group Coverage

This feature is an extension to Travel Accident Insurance or Business Travel Accident Insurance which allows for more than one (1) Person traveling at the same time and affected by the same event.

3.7.58 Travel Related Offer Program

This program provides valuable offers from the following travel categories consistently throughout the year. The Issuer or its designated travel agency third-party vendor must negotiate these offers. The travel categories are:

- Travel packages at special rates
- Air/rail tickets at special rates or free companion tickets or free upgrades
- Hotel bookings at special rates, free upgrades, or free meals
- Car rentals at special rates or upgrades

3.7.59 VAT/GST Information

In markets with Value-Added Tax (VAT) systems, this feature provides information on the amount of VAT/GST contained within each charge. For commercial clients it can help streamline the process of calculating how much tax has been paid for reclaim purposes.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.7.60 Year-end Summary of Charges

This feature provides an annual reporting of charges itemized by category of spending, such as hotels, restaurants, transportation, retail, and auto. The summary is also broken down by month and Cardmember, where applicable.

3.8 Co-Brand and Affinity Card Agreements

This section sets out the conditions under which Issuers may issue Co-Brand and Affinity Cards involving the placement of a logo of a Co-Brand or Affinity Partner on a Card.

The section also sets forth the requirements and limitations imposed on the Issuers and such third parties with respect to Co-Brand and Affinity Card programs. Each Co-Brand or Affinity Card program must be reviewed and approved in writing by AEGNS prior to launch.

3.8.1 Co-Brand and Affinity Card Program

A Co-Brand or Affinity Card program involves a Card issued by an Issuer which has the name, logo, or other mark of a Co-Brand or Affinity Partner on the Card. Any such agreement between an Issuer and a Co-Brand or Affinity Partner must be approved by AEGNS.

Co-Brand and Affinity Cards are jointly marketed by the Issuer with the Co-Brand or Affinity Partner. The Co-Brand or Affinity Partner must add value to the Card product proposition in the form of special benefits, e.g., rewards, to the Cardmember for Co-Brand Cards, or to the Cardmember and the Affinity Partner organization, e.g., contributions to charities, in the case of Affinity Cards.

3.8.1.1 Blue Box Line Co-Brand and Affinity Card Program

Issuers of Blue Box Line Cards may issue Co-Brand or Affinity Cards for Blue Box Line Cards. The Issuer must add the Co-Brand or Affinity Partner special benefits to the required features of a Blue Box Line Card as described in Section 3.5, "Blue Box Line Consumer Cards," on page 170. The Issuer must also be licensed to issue the Blue Box Line Card upon which the Co-Brand or Affinity Card is based.

3.8.1.2 American Express Enterprise Line Co-Brand Program

Issuers of American Express Enterprise Line Cards may issue Luxury Retail or Hotel Co-Brand Cards for American Express Enterprise Line Cards. Issuers are not permitted to issue Affinity Cards for American Express Enterprise Line Cards. The Issuer must add the Co-Brand Partner special benefits to the required features of an American Express Enterprise Line Card as described in Section 3.3, "American Express Enterprise Line Consumer Cards," on page 133. The Issuer must also be licensed to issue the American Express Enterprise Line Card upon which the Co-Brand is based.

3.8.2 Ownership and Control of the Co-Brand and Affinity Card Program

Co-Brand and Affinity Card programs are subject to the same requirements that apply to all Card programs, in addition to the requirements in this section. The ownership and control of any Co-Brand or Affinity Card program shall at all times reside with the Issuer. The Issuer, in any contractual arrangement with a Co-Brand or Affinity Card Partner, must retain full ownership and control of the Card receivables and the management of the program.

An Issuer and a Co-Brand or Affinity Partner are not permitted to establish an agreement which enables the Co-Brand or Affinity Partner to effectively own and/or control the program arising from Co-Brand or Affinity Cards. AEGNS reserves the right to review the relevant portions of all contracts between an Issuer and its Co-Brand or Affinity Partner to ensure that the Co-Brand or Affinity Partner does not effectively own and/or control the program. Issuers shall ensure that their arrangements with Co-Brand or Affinity Partners permit such review.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Receivables arising from Co-Brand or Affinity Cards must not be owned or controlled by the Co-Brand or Affinity Partner. A Co-Brand or Affinity Partner is prohibited from indirectly or directly enjoying the benefits of being an Issuer without actually being approved to be an Issuer on the AEGN.

Issuers are responsible for ensuring that Co-Brand or Affinity Partners comply with all applicable AEGNS requirements. Issuers shall be liable and responsible to AEGNS for the actions and omissions of all of their Co-Brand and Affinity Partners.

If AEGNS determines that an Issuer or its Co-Brand or Affinity Partner is not in compliance with any of the above provisions, AEGNS shall have the right to require that any non-compliance is cured within thirty (30) days of AEGNS' notice to the Issuer of any non-compliance and to impose penalties including fines and/or termination of the Co-Brand or Affinity Card program on sixty (60) days prior written notice.

3.8.3 Approval of Co-Brand and Affinity Partners

All Co-Brand and Affinity Partners selected by Issuers must enhance the image and integrity of the American Express Brand. AEGNS will have final approval of all Co-Brand and Affinity Partners. Such approval decisions will be based on AEGNS' judgment of the consistency with the American Express Brand and the effect that a particular Co-Brand and Affinity Partner will have on the American Express Brand.

Specifically, the Co-Brand and Affinity Partner must not be an organization that will be inconsistent with usage of the American Express Brand on a Card. As a guideline, but not as a comprehensive or complete list, such unsuitable organizations would include organizations whose public image is primarily associated with operating the following businesses or being engaged in the following activities: political parties, liquor companies, tobacco companies, entities engaging in anti-government activities, organizations producing or promoting the use of weapons or illegal drugs, any gambling organization, any organization engaged in illegal business, any entity engaged primarily in sex-related businesses (e.g., escort services, pornographic videos). See the "Product Features and Specifications" chapter beginning on page 125.

3.8.4 Approval of Co-Brand or Affinity Programs

The Issuer must submit the industry category and name of the proposed Co-Brand and Affinity Partner (and a description of the business primarily engaged in by the Co-Brand and Affinity Partner) to the Issuer's AEGNS representative for review by AEGNS no later than thirty (30) Business Days prior to signing an agreement with the Co-Brand and Affinity Partner and at least sixty (60) Business Days prior to the intended launch of the Co-Brand or Affinity Card. AEGNS will provide its approval or disapproval within ten (10) Business Days of receipt of submission, any such approval or disapproval to be based solely on the industry category and consistency with the American Express Brand image as outlined in Section 3.8.3, "Approval of Co-Brand and Affinity Partners," on page 204.

AEGNS' approval of the Co-Brand or Affinity Card program must be received prior to launch. If the proposed Co-Brand or Affinity Partner and the proposed arrangement with the Co-Brand or Affinity Partner do not comply with the guidelines within this chapter, the issuance of the proposed Co-Brand or Affinity Card Agreement will not be approved. The Issuer shall in all cases indemnify and hold harmless all American Express Entities against any and all claims made by a Co-Brand or Affinity Partner or proposed Co-Brand or Affinity Partner.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.8.5 Advertising Standards and Card Design - Co-Brand and Affinity Partners

Issuers must ensure that all advertising, marketing, and Card design materials for Co-Brand and Affinity Cards comply with the policies described in this edition of the *Business and Operational Policies* manual and the Participant Agreement. Issuers must require that Co-Brand and Affinity Partners submit all Co-Brand advertising, marketing, and Card design materials for review and approval by the Issuer, and at the request of AEGNS, by AEGNS, prior to use.

To ensure compliance with this provision, Issuers are required to include in their contracts with Co-Brand or Affinity Partners, the following language:

> "All advertising, marketing, and Card design materials for the Co-Brand or Affinity Cards that are the subject of this Agreement must comply with American Express advertising and marketing policies. As the Co-Brand or Affinity Card Partner, your organization is required to have all such materials reviewed and approved by us and American Express prior to use to ensure such compliance. Failure to comply with this requirement may result in suspension and/or termination of the Co-Brand or Affinity Card program."

3.8.6 Co-Brand and Affinity Card - Acceptance Requirements

All Co-Brand and Affinity Partners must accept all Cards, regardless of Issuer, and must not discriminate against or suppress the use of Cards which do not carry the Partner's name or logo.

There must be absolute neutrality at the POS with respect to acceptance of Cards issued on the AEGN. This means that there may not be any special promotion at the POS that would position the Co-Brand or Affinity Card issued on the AEGN as superior, preferred, or accepted more readily than any other Card issued on the AEGN. This includes all signs, posters, marketing materials, and oral communications at the POS, including POS locations managed by or on behalf of the Co-Brand or Affinity Partner. This does not include:

- Applications for the Co-Brand or Affinity Card at the Partner's locations, or
- All non-POS communications, which remain subject to all of the guidelines in the Network Specifications manuals.

Any requests for exceptions or interpretations of these requirements must be directed to the Issuer's AEGNS representative.

Co-Brand or Affinity Partners or Issuers must not request or require any S/E (even if the S/E is affiliated with the Co-Brand or Affinity Partner) to display a POS sign of any type that combines the Co-Brand or Affinity Partner's name, trademark, service mark, logo or other proprietary designation with the American Express Blue Box logo or other POS signs that indicate the S/E accepts American Express Cards.

3.9 Issuer-Provided Services

Issuers are required to provide quality customer service to their Cardmembers in keeping with the American Express Brand positioning. Issuers are also required to track and monitor their own Internal Servicing Metrics in order to ensure delivery of high-quality service to customers that is consistent with the American Express Brand as described in the "AEGNS Service Performance Program" chapter beginning on page 400. AEGNS, upon request, may require Participants to provide Internal Servicing Metrics. Participants that fail to provide Internal Servicing Metrics upon request within the established timeframes set forth by AEGNS will be subject to non-compliance fees. Refer to Section 10.7.1, "General Non-Compliance Fees," on page 411 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.9.1 Issuer-Provided Card Account Services

The following activities are to be performed by the Issuer to service their Card Accounts regardless of whether the Card product issued is an American Express Enterprise Line or Blue Box Line product.

3.9.1.1 Account Setup and Plastic Issuance

3.9.1.1.1 Consumer Account Setup and Plastic Issuance

Consumer Card Issuers are responsible for soliciting and acquiring Cardmembers, setting up new Accounts and issuing Cards. It is the sole responsibility of Issuers to assess the creditworthiness of potential Cardmembers and bear all credit and collection risks with respect to Cardmembers.

3.9.1.1.2 Corporate Card Program Account Setup and Plastic Issuance

Corporate Card Issuers are responsible for soliciting and acquiring businesses to be Corporate Card Clients, setting up new Corporate Accounts, and issuing Cards to Corporate Card Client employees.

It is the sole responsibility of Issuers to assess the creditworthiness of potential Corporate Card Clients and Cardmembers and bear all credit and collection risks with respect to the Corporate Card Client and Cardmembers.

Program Administrators work to manage the Corporate Card Client's Card program and require specialized servicing beyond typical consumer Cardmember servicing. Program Administrators continuously manage program level features and benefits, such as account hierarchies, credit limit change requests, and data capture. Accordingly, as part of setting up a new Corporate Card Client, the Issuer is responsible for working with the relevant Program Administrator to define and implement the business's requirements, including establishing hierarchies, Cardmember limits, spend category limits and data access.

3.9.1.2 Billing and Collections

Issuers are responsible for Billing and collecting amounts owed from Cardmembers and corporate clients including producing and distributing Billing statements to Cardmembers and corporate clients at least monthly.

Issuers are required to advise their Cardmembers of the methods of Card Account payment available. Payment methods may include, but are not limited to:

- The deduction of a Cardmember's monthly balance or minimum payment amount directly from a designated Account.
- Cash or Check over the counter at one (1) of the Issuer's own bank branches.
- Check by mail to the Issuer's office or designated payment processor.
- Telephone or Internet banking. If this service is available, the Issuer is responsible for ensuring the Telephone/Internet banking providers hold the correct banking information for the Issuer.

AEGNS does not endorse payment of Cardmember Account balances at American Express Bank locations for the following reasons:

- Cardmember payments made at these locations across markets can take a considerable time to clear through international banking systems.
- AEGNS may be unable to confirm whether a payment was made via cash or check and cannot relay this information to the Issuer receiving payment.

AEGNS will not accept liability for any returned checks and will debit the check amount to the Issuer for collection from the Cardmember and corporate clients. A remittance fee will be charged by AEGNS to the Issuer when their Cardmembers and corporate clients make payments of this type. See the "Network Fees" chapter beginning on page 401 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.9.1.3 Card Pricing

All pricing to Cardmembers is the sole responsibility of Issuers.

3.9.1.4 Card Validity Period

Cards issued after April 17, 2015 must have a maximum validity period of five (5) years to include the usage of the Cryptographic Keys used when issuing the Cards.

Note: For Prepaid Cards, regardless of the validity period of the Card, the funds on the Card do not expire.

3.9.1.5 Card Production



Issuers are responsible for Card plastic production. Issuers are required to comply with the AEGNS guidelines regarding Card production, holographic images on the Card (either HoloMag™ Generation 2 or hologram), Chip Card specifications, signature panel specifications, and other Card production standards.

For Prepaid Cards, Issuers must ensure that ISO 7813 track data contains a Service Code that, when interrogated by a POS device, instructs the device to request Authorization from the Issuer. AEGNS is not responsible for ensuring that Service Establishments are able to act on and interrogate Service Codes, and Issuers remain financially responsible for these Transactions, provided that the Service Establishment has followed Card acceptance procedures as outlined in the "S/E and ATM Standards" chapter beginning on page 214.

For more information, refer to the following publications:

- *AEIPS Chip Card Specifications*
- AEIPS Terminal Technical Manual
- *Business and Operational Policies* manual, "S/E and ATM Standards" chapter beginning on page 214
- *Business and Operational Policies* manual, "Security and Fraud" chapter beginning on page 375
- *Codes Reference Guide*
- *Expresspay Card Specifications*
- *Expresspay Terminal Specifications*
- *GNS Card Design Guidelines* (located in the Marketing section on Knowledge Base)
- *Network Specifications manuals*

3.9.1.6 Cardmember Agreement/Solicitation Materials

Issuers shall enter into a written agreement with Cardmembers to whom they issue Cards. Such Cardmember agreements shall disclose the name of the Issuer and the terms of Card issuance and use, including the AEGNS Foreign Currency Factor.

The form of such agreements will be subject to the prior written approval of AEGNS to ensure consistency with the American Express Brand. All agreements, disclosures, communications, and solicitations targeted at Cardmembers or prospective Cardmembers must comply with applicable laws and regulations, the relevant terms of the Participant Agreement and the Manuals.

Issuers are required to send Cardmember agreements to potential Cardmembers prior to Card activation. Cardmember agreements establish the terms of the relationship between Issuers and their Cardmembers.

3.9.1.6.1 Disclosure of Foreign Currency Factor

Cardmember Terms and Conditions must disclose (a), that all Cardmember Charges in a foreign currency other than U.S. Dollars will be converted into U.S. Dollars before being converted into the billing currency, and (b), the fact that American Express assesses a Foreign Currency Factor on all foreign Charges and the amount of such assessment.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The amount of the Foreign Currency Factor and the fact that it is assessed by American Express must also be disclosed in advance to prospective Cardmembers in any solicitation materials that disclose the financial terms of the Card arrangement, such as application forms. It is recommended that Issuers disclose the amount of the Foreign Currency Factor and the fact that it is assessed by American Express in other solicitation materials, whether or not such materials disclose other financial terms.

3.9.1.6.2 Notice Regarding Cardmember Information

Cardmember agreements shall contain provisions authorizing Cardmember Information to be shared with American Express Entities for the purpose set out in Section 2.10.4, "Use of Cardmember Information," on page 113 subject to applicable legal requirements, Cardmember "opt out" requests or other choice options where required by law, which the Issuer is responsible for determining and advising to AEGNS. Such provisions may not be amended except with the prior written approval of AEGNS. Such notices must inform Cardmembers that, for the conduct of the Card Issuing Business, Cardmember Information may be stored or processed outside the jurisdiction of Cardmember's country or residence, or where such countries are within the European Union, outside of the European Economic Area.

3.9.1.6.3 Other Requirements

Cardmember agreements used by Issuers must contain provisions addressing choice of law and jurisdiction in case of dispute.

Cardmember agreements and related materials used in a language other than English shall be submitted to AEGNS in English and such other language.

If an Issuer introduces changes to its Cardmember agreements, it shall notify impacted Cardmembers of such modifications, clearly and transparently, with reasonable anticipation, and in accordance with applicable law and good industry practice.

If AEGNS has reasonable grounds to believe that a Cardmember is engaged in fraudulent, unlawful, or similarly objectionable activity that could create legal or financial risk to the Network or reflect unfavorably on the American Express Brand, AEGNS may require the Issuer to cancel its agreement with that Cardmember.

3.9.1.7 Additional Information for Prepaid Card Cardmember Agreement/Solicitation and/or Fulfillment Materials

Issuers must ensure that full disclosure is made to Cardmembers of all fees, rates, and processes associated with Prepaid Cards in accordance with applicable law including, but not limited to, initial Loads and Reloads, ongoing servicing, maintenance or cancellation, and any foreign exchange conversion factors that may be applied to Cardmembers' Reloads in foreign currency, if applicable.

In the case of reloadable Prepaid Cards, the Cardmember terms and conditions must disclose details of the initial funding and Reload processes. The Cardmember terms and conditions for all Prepaid Cards must also disclose that charges in a currency different from the currency in which the Prepaid Card is denominated will be converted by AEGNS to U.S. Dollars before being converted into the currency of the Prepaid Card, and the amount of Foreign Currency Factor assessed by American Express for such charges.

Issuers must also disclose restrictions and special provisions regarding certain Transaction types, including without limitation:

- Usage restrictions in Prohibited Industries.
- Other restricted Transaction types
- Special provisions related to pre-authorized or Recurring Billing Transactions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Purchases made with Anonymous Non-Reloadable Prepaid Cards, such as gift cards, are similar to those made with cash or Travelers Cheques. AEGNS recommends that Issuers of Prepaid Cards advise purchasers of Anonymous Non-Reloadable Prepaid Cards that disputes involving Transactions conducted with such cards, should be addressed directly with the S/Es where the Transactions took place. Depending on their return policies, S/Es may process a credit in the form of cash, funds returned to the Card, or in-store vouchers.

Disputes involving an Anonymous Non-Reloadable Prepaid Card will not be supported by AEGNS (except for ISO 4755 - No Valid Authorization).

3.9.1.8 Legal Compliance

Issuers are responsible for knowledge of and adherence to all applicable laws and regulations.

3.9.1.9 Risk Assessment

Issuers are responsible for owning and managing all policies, procedures, and decisions regarding the credit and fraud risk of their Cardmember Accounts.

3.9.2 Issuer-Provided Core Card Services

The Issuer must provide all of the core Card services listed in this section to their Cardmembers whether the Card product issued is an American Express Enterprise Line or Blue Box Line Card product, subject to applicable law. Provision of these core services is critical to protection of the American Express Brand.

Cash access, Emergency Card Replacement, and Emergency Assistance services *are not required* for the American Express® Corporate Purchasing Card.

3.9.2.1 Cardmember Customer Service

Issuers must, at their expense, provide their Cardmembers with customer service via a toll-free or collect call number within the Issuer's Territory and via a collect call number when outside the Issuer's Territory. In either case, the number must lead the Cardmember to the Issuer's dedicated American Express Card customer service line. For any calls received for services delivered by a third-party provider, the Issuer's customer service function must be able to forward these calls toll-free or provide the third-party provider's toll-free or collect call number.

The Issuer's customer service telephone number(s) shall be clearly printed on the reverse side of the Card. Issuers shall not print any AEGNS, American Express, or any American Express Entity telephone numbers on Cards they issue, or on any Card application or collateral materials, unless there is a separate signed agreement with AEGNS to allow such a number to be used.

Full services are to be provided during business hours via live operators and voice response, as needed. Business hours must be equal to or exceed the standard business hours for credit card servicing in the Issuer's Territory. During non-business hours, emergency calls are to be routed to a live operator who will provide emergency services (e.g., lost/stolen Card reporting, Emergency Card Replacement, emergency cash requests). Non-emergency calls can be handled via a voice response unit.

In some markets, cultural and religious observances during normal business hours may not allow full staffing of the customer service operation. At these times, emergency services must remain available, with non-emergency calls handled via a voice response unit.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.9.2.2 Cash Access

Issuers are required to provide cash access for their Cardmembers and the Card features necessary to facilitate cash access. This feature is *not required* for the American Express® Corporate Purchasing Card.

3.9.2.2.1 Cash Advances

Issuers are required to provide their Cardmembers with the ability to receive Cash Advances on their Credit Cards or Charge Cards. Cardmembers shall be able to present their Card at Issuer locations, such as ATMs or other authorized locations, and receive a Cash Advance. The Cash Advance is limited to the amount Authorized by Issuers, and by any applicable legal requirements.

3.9.2.2.2 Cash Disbursements

Cash Disbursements are manual disbursements of cash to Cardmembers by a teller at a Cash Disbursement Provider in the Cash Disbursement Provider's local currency. Cash Disbursement Transactions are identified by Merchant Category Code (MCC) 6010 - Financial Institutions, Manual Cash Disbursements.

Issuers may provide their Cardmembers with the ability to receive Cash Disbursements on their Cards in accordance with this program. The Cash Disbursement is limited to the amount Authorized by the Issuer, and by any applicable legal requirements.

3.9.2.2.3 Cash Withdrawal

Issuers are required to provide their Cardmembers with the ability to receive cash on their Debit Cards. Cardmembers shall be able to present their Card at Issuer locations, such as ATMs or other authorized locations, and receive a Cash Withdrawal. The Cash Withdrawal is limited to the amount Authorized by Issuers and by any applicable legal requirements.

3.9.2.2.4 Access to Participant's ATM Network

The Issuer is required to provide all Cardmembers, including those of other Issuers, access to all ATMs that the Issuer owns except as otherwise stated in an Agreement with an American Express Entity.

3.9.2.2.5 Access to Participant's Shared ATM Network

Issuers are required to use reasonable best efforts to provide all Cardmembers access to ATMs to which the Issuer has access through agreements with a local, regional, or national ATM network.

3.9.2.2.6 Access to the Amex Shared ATM Network

Except as otherwise agreed by AMEX or an American Express Entity, Issuers are required to provide their Cardmembers with access to the Amex Shared ATM Network, and must prioritize routing their Cardmembers' ATM Transactions through the Amex Shared ATM Network (i.e., Issuers must use the Amex Shared ATM Network as the first choice to route their Cardmembers' ATM Transactions).

3.9.2.2.7 Cash Access at Issuer's Branch Locations

Issuers are required to provide their Cardmembers with access to cash via their branch tellers.

3.9.2.2.8 PIN Issuance

Issuers are responsible for assigning a PIN to their Cardmembers. Cardmembers must use this PIN when obtaining cash with the Card whether at an ATM or elsewhere. Issuers are also responsible for maintaining the PIN database and for authorizing the PIN during Transactions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.9.2.3 Additional Optional ATM Services

An Issuer may participate, at its discretion, in the following additional optional ATM Services:

- PIN Management

Issuer Participation in ATM Optional Services

To participate in ATM optional services, an Issuer must:

- Obtain Certification from AEGNS.
- Understand that ATM optional services are provided at the discretion of ATM Providers.

Issuer Participation in ATM PIN Management Services

PIN Management is an optional feature that lets a Cardmember unblock or change their PIN on Chip Cards at certified Acquirers' ATMs.

An ATM PIN Management Transaction enables a Cardmember to:

- PIN Change - Issuer will receive a request from the Network/ATM Provider to change the PIN on the Card. The Issuer will approve the request before the ATM will execute the script from the Issuer.
- PIN Unblock - Issuer will receive a request from the Network/ATM Provider to unblock the PIN on the Card. The Issuer will approve the request and will send a script for the ATM to execute to unblock the PIN.

3.9.3 Additional Services for Prepaid Cards

Issuers are required to perform the following activities.

3.9.3.1 Funding of Prepaid Cards

The process of loading a balance onto a Prepaid Card is described in this section as funding. In all cases, funding processes must comply with applicable laws and regulations.

Initial Funding

Initial funding is performed as part of the Card purchase process. Cards must be activated in order to be used as described in Section 8.4.4, "Card Activation," on page 379.

Variable Load

Issuers must ensure that Cardmembers are able to purchase non-reloadable Prepaid Cards of variable amounts.

Single Currency Per Card

Each Prepaid Card may only be loaded with a single currency.

Reloads

Prepaid Cards may only be reloaded by Issuers unless explicitly approved by AEGNS. When permitted by AEGNS, Issuers may only use agents to reload Prepaid Cards that are regulated financial institutions and which maintain an AML/ATF program that conforms to AEGNS AML/ATF policies as well as local laws and regulations.

Issuers must have policies in place that incorporate Risk-based limits regarding the initial purchase and loading of reloadable Prepaid Cards. Issuers must also be able to verify the Cardholder's identity to ensure the Prepaid Card has not been transferred.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.9.3.2 Return of Prepaid Card Funds on Card Cancellation or Card Expiry

Issuers must return the funds held on Prepaid Cards to Cardmembers under the following circumstances:

- The Cardmember decides to cancel their Prepaid Card, or
- The Card validity date expires and the Cardmember requests a return of funds

Issuers must comply with all applicable regulations concerning the return of funds.

Issuers are required to inform their Cardmembers of the availability of this service, including Card cancellation procedures. Issuers must also disclose any authorized restrictions and limitations associated with this service in all Cardmember communications where this service is described. In particular, such Cardmember terms and conditions must disclose details of the Card cancellation and cash-out processes, and any associated fees. Where possible, Issuers should return funds to the original payment instrument used to Load the requested amount.

3.9.4 Additional Features

Issuers may choose to offer additional benefits and features to their Cardmembers which are designed to add value to their Cards. Additional benefits and features can be initiated, designed, and implemented by Issuers, or may be offered by AEGNS at additional fees to Issuers. In either case, AEGNS' approval is required prior to implementation in order to ensure service quality, reliability, value, and consistency with the American Express Brand image, and to enable AEGNS to assess operational feasibility and costs.

3.9.4.1 Guidelines for Additional Features

This section sets out the guidelines for additional benefits and features which Issuers should follow prior to submitting such benefits or features to AEGNS for approval. Contact your AEGNS representative for further information.

The additional benefit or feature:

- Must be consistent with the American Express Brand image. It must be of high quality, appeal to mid-to-upscale customers, and it must fully deliver on the promises made in advertising and collateral materials. This means that the Issuer is responsible for the quality, reliability, and service delivery of the benefit or feature whether the benefit or feature is provided directly by the Issuer or through a third party.
- Must not adversely impact the operations of S/Es on the AEGN. This includes, but is not limited to, possible delays in Authorizations, higher than average returns of merchandise and/or dispute levels, out-of-pattern processing by S/Es at the Point of Sale (POS).
- Must be operationally and technically feasible in terms of all AEGNS interfaces and processing.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3.9.4.2 Approval Process for Additional Features

This section sets out the approval process which Issuers must follow before additional benefits and features can be implemented. Contact your AEGNS representative for additional information.

1. The Issuer must submit a description of the proposed additional feature or benefit, including what it is; how it is positioned to consumers; how it is delivered (including any arrangements with third-party suppliers); any potential interfaces to or impact to the AEGN; projected development and launch timeframes with milestone dates; the names, responsibilities, and other relevant information pertaining to any new third-party suppliers requiring Certification, or any certified Authorized Processors which will be performing in new capacities.
2. The description of the proposed additional feature must be submitted to the Issuer's AEGNS representative at least sixty (60) days prior to the launch (e.g., marketing or advertising) if no additional interfaces to AEGNS are required. If interfaces are required, changes must be evaluated before approval can be given.
3. AEGNS will respond to the Issuer within ten (10) Business Days of the receipt of the above information. Issuers should build the approval process timeframes into their project plans.
4. In the event that AEGNS determines that a systems or operations adaptation by AEGNS would be needed in order to accommodate any such new feature or benefit, the Issuer and AEGNS shall negotiate:
    a. Whether AEGNS shall make any such adaptation, and
    b. Who should bear the cost.

AEGNS does not guarantee that it will make any or all such systems or operational adaptations. It is understood that any new or different pricing an Issuer wishes to offer is solely within the Issuer's discretion and is not subject to this section.

3.10 Issuer Access to American Express Sourced Benefits

American Express occasionally negotiates for benefits to be provided by certain Service Establishments and/or vendors at no additional cost to Cardmembers and Issuers. These benefits are generally related to customer experiences, with an enhanced focus on travel, lifestyle, and everyday benefits to support Card performance and customer engagement with the Network. Examples include, but are not limited to, travel discounts, dining programs, retail promotions, VIP access, and loyalty program membership.

By extending these American Express sourced benefits to their Cardmembers, an Issuer agrees to adhere to the Benefit Participation Terms and Conditions, and the terms of the Benefit Description Form (as defined in "Exhibit 10. Benefit Participation Terms and Conditions" on page 472) for the relevant benefit, which sets out all the relevant requirements, guidelines, restrictions, product and market eligibility, communication obligations, and terms and conditions applicable to the benefit to ensure all contractual obligations are met. To view the Benefit Participation Terms and Conditions refer to "Exhibit 10. Benefit Participation Terms and Conditions" on page 472.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4 S/E and ATM Standards

4.1 Introduction

This chapter details AEGNS' policy regarding Service Establishments (S/Es) and ATMs. The chapter includes information regarding Card acceptance and S/E charge processing, including ATM Card acceptance and processing procedures.

4.2 S/E Card Acceptance Procedures

Acquirers must incorporate these requirements in their Card acceptance agreements with S/Es. Refer to Section 2.9.3.3, "Compliant S/E Agreement Design," on page 87 for additional information.

4.2.1 Split Shipment Transactions

A Split Shipment Transaction occurs when a Cardmember makes a single purchase of multiple individually priced Goods, and the Goods are delivered to the Cardmember in multiple shipments. Unit prices and items sold as a set must not be billed as separate charges.

4.2.2 Multiple ROC Transactions with Single Authorization

An S/E may submit multiple ROCs with a single Authorization if they are one of the following:

- The S/E is an airline, a cruise line, or a lodging S/E.
- The S/E submits Split Shipment Transactions of Goods. Refer to Section 4.2.1, "Split Shipment Transactions," on page 214 for more information.

4.2.3 Card Acceptance Restrictions

S/Es are prohibited from doing the following:

- Capturing or processing Records of Charges (ROCs) on behalf of any other S/E or non-S/E.
- Submitting ROCs for Goods and Services identified in prohibited industries. Refer to Section 2.9.4.1, "Prohibited Industries," on page 94 for additional information.
- Requiring a photocopy of the Card.
- Requiring a photocopy of the legal ID.
- Submitting ROCs which do not represent a bona fide sale of Goods and Services.
- Submitting ROCs for amounts which do not correspond to the value of the Goods and Services provided.

  Note: This restriction does not apply in the case of Partial Authorizations. Refer to Section 5.3.3, "Prepaid Card Authorization Processing," on page 248 for additional details on Authorization-related requirements for Prepaid Cards.
- Submitting more than one (1) ROC for Goods and Services purchased in a single Transaction, except for airlines, cruise lines, and lodging S/Es, Split Shipment Transactions of Goods.
- Splitting a single charge by creating two (2) or more ROCs on a single Card for a single Charge in order to avoid Authorization.
- Except as otherwise required by applicable law, imposing any restrictions or disadvantages on use or acceptance of Cards that are not imposed equally on the use or acceptance of all other charge, debit, or Chip Cards, or similar cards, services or payment products.
- Requiring Cardmembers to waive their dispute rights at the time of Transaction.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.4 Discounts on Purchases

Except as specifically permitted below and in the Co-Brand or Affinity Partner's Card acceptance agreement, a discount that is not available on all Cards may not be delivered or awarded at a POS location solely upon presentation for payment of a Co-Brand or Affinity Card.

The following discount or incentive practices shall be permissible in connection with Co-Brand and Affinity Card programs:

- A discount that is not provided at the time of the Transaction, but subsequently provided (e.g., Credit on the Billing statement, rebates, etc.), and
- A discount activated by presentation of a separate instrument in addition to the Co-Brand or Affinity Card (e.g., coupons, vouchers, etc.).

Any requests for exceptions or interpretations of these requirements must be directed to the Issuer's AEGNS representative.

4.2.5 Discriminatory Treatment

As described in this section, except as otherwise required by applicable law, an S/E shall place no restriction on the acceptance of Cards that is not imposed on all other cards the S/E accepts.

4.2.5.1 Co-Brand and Affinity Partners

All Co-Brand and Affinity Partners must accept all Cards, regardless of Issuer, and must undertake not to discriminate against or suppress the use of Cards which do not carry the Co-Branded/Affinity Partner's name or logo.

Except as specifically permitted below and in the Co-Brand or Affinity Partner's Card acceptance agreement, there must be neutrality at the POS with respect to acceptance of Cards issued on the AEGN. This means that there may not be any special promotion at the POS that would position the Co-Brand or Affinity Card issued on the AEGN as superior, preferred, or accepted more readily than any other Card issued on the AEGN. This includes all signs, posters, marketing materials, and oral communications at the POS, including POS locations managed by or on behalf of the Co-Brand or Affinity Partner. This does not include:

- Applications for the Co-Brand or Affinity Card at the Partner's locations, or
- All non-POS communications, which remain subject to all of the guidelines in the Network Specifications manuals.

Any requests for exceptions or interpretations of these requirements must be directed to the Issuer's AEGNS representative.

4.2.6 Printed Card Security Code (PCSC) Validation

AEGNS strongly recommends that S/Es submit the PCSC in the POS Authorization Request (1100) message as an additional method of mitigating fraud losses.

If the S/E submits the PCSC value, the Acquirer must:

- Send the PCSC value as part of the POS Authorization Request (1100) message, to the AEGN, and
- Be certified to receive the PCSC validation response from the AEGN in the POS Authorization Response (1110) message.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.7 In-Person Charges

The Card must be presented for all in-person Charge requests, except for Split Shipment Transactions of Goods. If an S/E has electronic Authorization capabilities, the Card must be "swiped" through electronic data capture equipment or processed by a chip-capable POS device if the Card is chip-enabled. Obtaining Cardmember signature is optional, and at the discretion of the S/E, but is not required to complete the Record of Charge (ROC), unless required by applicable law. Where signature is required by applicable law, S/Es must adhere to the requirements in Section 4.2.7.1, "Obtaining Signature for In-Person Charges," on page 217. Signature must be obtained for the following Merchant Category Codes (MCCs):

- 4829 - Wire Transfers and Money Orders
- 6010 - Financial Institutions - Manual Cash Disbursements
- 6051 - Non-Financial Institutions - Foreign Currency, Money Orders (not Wire Transfer), Scrip and Travelers Checks

If the S/E processes Charges manually or the electronic capture device is inoperable, the S/E must Imprint the Card onto a ROC which conforms to the AEGN specifications as described in Section 4.2.21.1, "Completing Charge ROCs," on page 237. The S/Es may provide handwritten Card details on the ROC, only when:

- A POS device is not available, and
- A Card imprinter is not available or a flat-printed Card is presented.

Failure to obtain an Imprint may subject the Transaction to an "ISO 4527 - Missing Imprint" on page 326, unless the Transaction meets any of the conditions for exclusion.

For Charges made in Person, regardless of the amount of the Transaction and regardless of the S/E Floor Limit, the S/E must:

- Verify that the Card is not visibly altered or mutilated.
- For keyed Transactions, S/Es must key in the Card Account number, Expiration Date, and for embossed Cards, obtain an Imprint of the Card so that the Card and S/E data are legible on the ROC. No Imprint is required if the Transaction meets any of the conditions for exclusion for "ISO 4527 - Missing Imprint" on page 326. "Signature on file" is not an acceptable signature. A pencil rubbing or photocopy of the Card is not considered proof of a valid Imprint.
- If applicable, obtain the PIN to authenticate the Cardmember. No PIN is required to authenticate the Cardmember if the S/E and the Transaction qualify under the No Signature/No PIN Program. Refer to Section 4.2.20.4, "No Signature/No PIN Program," on page 232.
- Ensure that the Card is being used within the valid dates shown on the face of the Card. If only an Expiration Date appears on the Card, the date of Charge must be prior to this date.
- Complete a single ROC for the entire amount of the Charge Transaction, except for airlines, cruise lines, and lodging S/Es, and Split Shipment Transactions of Goods. S/Es may accept separate forms of payments for the same Transaction (i.e., Cardmember wishes to pay for part of the Transaction with the Card and the balance with another form of payment).
- If suspicious of a Card or Cardmember, S/Es are instructed to call their Acquirer Authorization center with a Code 10.
- Match the Card Account number and Expiration Date appearing on the front of the Card to the same information on the back of the Card and/or printed on the terminal receipt by the POS terminal.

The S/E is at risk of a Chargeback if a Charge proves to be fraudulent and the S/E completes the Transaction when the Cardmember is present and does not have his/her Card.

Refer to Section 5.10.3.1, "Issuer-Based Deferred Payment Plan," on page 263 and Section 5.10.3.2, "Acquirer-Based Deferred Payment Plan," on page 263 for information related to signature for Deferred Payment Plans.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.7.1 Obtaining Signature for In-Person Charges

If an S/E chooses or is required by law to obtain signature on a printed or electronic ROC, the S/E must:

- Ensure that the Card is signed and verify that the Cardmember's signature on the ROC reasonably matches the signature on the back of the Card. No signature is required on the ROC if the S/E and the Transaction qualify under the No Signature/No PIN Program. Refer to Section 4.2.20.4, "No Signature/No PIN Program," on page 232.

If an S/E requests Cardmember signature, and the signature panel on the Card is blank, in addition to requesting an Authorization the S/E must do all of the following:

- Require the Cardmember to sign the Card.
- Ask the Cardmember for an official form of identification bearing a signature, such as a driver's license or passport. Compare the signature on the Card to the official form of identification.
- If the Cardmember refuses to sign the Card, the Transaction should not be completed.

S/Es may provide the Cardmember's written signature or a signature obtained electronically on a Point of Sale device (for in-person Charges) on the ROC.

4.2.7.2 Service Code Interrogation Requirements

S/E POS devices, in markets enabled with floor limits, are required to interpret and act upon the Service Code for all Transactions in which the S/E has obtained a magnetic stripe-read of the Card. The definition of "interpret and act" is as follows:

- "Interpret" the Service Code means that the S/E Point of Sale device must understand the significance of the Service Code Value.
- To "act" on a Service Code once it has been interpreted means that the S/E Point of Sale device must weigh the information available at the Point of Sale with the requirements of the Service Code and decision the Transaction appropriately.

If an S/E in a Floor Limit region has all of the requisite information at the Point of Sale to act on a Service Code, the S/E is required to do so. A comprehensive list of available Service Code values and definitions can be found in Network Specifications manuals.

4.2.8 Expresspay Acceptance

An Expresspay Transaction is a Contactless Transaction initiated by the use of an Expresspay-enabled Card or Mobile Device at an Expresspay-enabled POS Device. Because the Expresspay Transaction may not follow standard S/E acceptance procedures, S/Es accepting an Expresspay or Expresspay Mobile are exempt from the requirements set forth in Section 4.2.7, "In-Person Charges," on page 216 except for the following requirements:

- S/Es must complete a single ROC for the entire amount of the Transaction. S/Es may accept separate forms of payment for the same Transaction (i.e., Cardmember wishes to pay for part of the Transaction with the Card and the balance with another form of payment).
- If suspicious of a Card or Cardmember, S/Es are instructed to call their Acquirer Authorization center with a Code 10. Refer to Section 4.3, "Code 10," on page 238 for additional information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- The S/E is at risk of a Chargeback if a Charge proves to be fraudulent and the S/E completes the Transaction when:
  - The Cardmember is present and does not have his/her Card or Mobile Device.
  - The Cardmember does not sign the ROC (if required - refer to the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide* available on Knowledge Base).

Acquirers and S/Es must comply with the Card, Expresspay, and Expresspay Mobile Terminal requirements as defined in the following:

- Acquirer Chip Card Implementation Guide
- Live Terminal Parameters AEIPS & Expresspay Guide
- Expresspay Terminal Specifications

4.2.9 Expresspay Transactions at Transit Access Terminals (TATs)

Expresspay Transactions that originate at TATs using an Expresspay-enabled Card or Mobile Device and include the TAT indicator are subject to special processing rules. These Transactions are exempt from the requirements set forth in Section 4.2.8, "Expresspay Acceptance," on page 217 and must instead meet the requirements detailed in this section. Acquirers that support Expresspay Transactions at TATs must be certified by AEGNS to comply with the Expresspay Terminal Specifications and Network Specifications.

4.2.9.1 TAT S/E Requirements

Expresspay Transactions at TATs must be classified with one (1) of the following Merchant Category Codes (MCCs):

- 4111 - Local and Suburban Commuter Passenger Transportation
- 4112 - Passenger Railways
- 4131 - Bus Lines
- 4784 - Tolls and Bridge Fares
- 7523 - Parking Lots and Garages

The MCC must be submitted in each POS Authorization Request (1100) message and POS First and Second Presentment (1240) message.

4.2.9.1.1 Card Acceptance Requirements for Expresspay Transactions at TATs

When accepting and processing Expresspay Transactions at TATs, the S/E must:

- Not accept Expired Cards
- Populate the TAT indicator in the Point of Service Data Code field of both the POS Authorization Request (1100) message and the POS First and Second Presentment (1240) message (see Point of Service Data Codes in the *Codes Reference Guide*)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.9.1.2 Authorization Requirements for Expresspay Transactions at TATs

When accepting an Expresspay Transaction at a TAT, the S/E must submit an Account Status Check for a nominal amount or an amount up to the Cumulative Spend Protection Threshold provided in Table 4-1, "Expresspay at TAT - Operational Parameters," on page 219 if the Card had not been used at an S/E TAT within the maximum number of contiguous days to authorize listed in Table 4-1.

If the Account Status Check is declined by the Issuer, the S/E must place the Card on the Deny List (refer to Section 4.2.9.3, "S/E Management of the Deny List," on page 221 for timing considerations).

S/Es must submit an Authorization Request for the full amount of a single fare or Aggregated Transaction if this amount exceeds the Cumulative Spend Protection Threshold listed in Table 4-1 within the maximum contiguous number of days to authorize listed in Table 4-1, beginning from the date of the last approved Authorization Request. The Authorization will be valid for the duration of the maximum contiguous days provided for each country in Table 4-1.

Failure to comply with the Authorization-related requirements may result in the S/E being subject to "ISO 4521 - Invalid Authorization" on page 321 and "ISO 4755 - No Valid Authorization" on page 345.

4.2.9.1.3 Submission Requirements for Expresspay Transactions at TATs

When accepting and processing Expresspay Transactions at TATs, the S/E may submit Aggregated Transactions representing individual fare purchases on a single Card. S/Es may combine fare purchases up to the Submission Frequency listed in Table 4-1 from the purchase of the first fare.

If an Authorization originating at a TAT is declined, the S/E can do one (1) of the following:

- If the value is less than or equal to the Declined Authorization Protection value, submit a Transaction for Settlement.
- If the amount is greater than the Declined Authorization Protection value, the S/E may request a new Authorization as outlined in Section 4.2.9.2, "S/E-Initiated Transit Debt Recovery," on page 220.

Note: Authorizations for partial fares cannot be submitted. An S/E must not split a Transaction with the intent of avoiding a single Authorization for the full amount of the purchase.

Table 4-1. Expresspay at TAT - Operational Parameters

Country	Cumulative Spend Protection Threshold	Authorization Expiration	Submissions Frequency
Australia	35 AUD	7 days	7 days
Canada	25 CAD	7 days	7 days
Israel	150 NIS	14 days	Daily
Italy	25 EUR	14 days	Daily
Hong Kong (Special Administrative Region of China)	100 HKD	7 days	7 days
Japan	1600 JPY	14 days	Daily
Poland	50 PLN	14 days	Daily
Singapore	30 SGD	14 Days	7 days
Sweden	250 SEK	14 days	Daily
UK	15 GBP	14 days	Daily
US	15 USD	7 days	7 days
All others	30 USD (or local equivalent)	14 days	7 days

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 4-2. Expresspay at TAT - Declined Authorizations

Region/Country	Declined Authorization Protection
AMERICAS	
Canada	12 CAD
US	6 USD
All others	3 USD
APAC	
Australia	8 AUD
Japan	1600 JPY
Singapore	12 SGD
All others	5 USD
EMEA	
UK	10 GBP
All others	5 USD

4.2.9.1.4 Charge ROC Requirements for Expresspay Transactions at TATs

For Expresspay Transactions originating at TATs, the S/E must ensure the Cardmember has access to the following information for a minimum of 120 days:

- S/E name
- Total Transaction amount
- Date of travel
- Start time of each individual journey, if available
- End time of each individual journey, if available
- Final Transaction date

4.2.9.2 S/E-Initiated Transit Debt Recovery

If an Authorization at a TAT is declined, S/Es may attempt to recover any outstanding debt providing all the following conditions are met:

- The value of the debt is greater than the Declined Authorization Protection value.
- The S/E obtains an approved Authorization for the full value of debt owed.
- The S/E does not attempt more than six (6) Authorizations after the initial declined Authorization Request.
- No more than thirty (30) days have elapsed since the initial declined Authorization Request.

S/Es should adhere to the requirements in Section 4.2.12, "Merchant-Initiated Transactions," on page 223 when processing S/E-Initiated Transit Debt Recovery Transactions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.9.3 S/E Management of the Deny List

The S/E must maintain a list of Card Account numbers for which Issuers have declined an Authorization Request for a Card Account previously used at a TAT. The S/E must add a Card Account number if the Issuer declines an Authorization Request. The S/E must remove a Card Account number if they receive an approved Authorization.

The S/E must add or remove Card Account numbers to this list based on any new Authorization approval or decline decisions at least once per day. AEGNS strongly recommends the S/E update the list more frequently when possible.

When a Card is presented at a TAT, the S/E must immediately check the list and deny entry to any Cardmember whose Card Account number appears on the Deny List.

S/Es must not submit Transactions initiated by Cards that appear on the Deny List at the time of the Transaction attempt.

4.2.9.4 Expresspay Card or Expresspay Mobile for Pay-In-Advance Transit Fares

The following provides the general policies that apply to using an Expresspay Card or Expresspay Mobile as a means to access the transit system for pay-in-advance transit fares.

A pay-in-advance transit fare occurs when a Cardmember purchases a value from a transit S/E in advance of travel. With the exception of time-based, unlimited travel passes, the value of the fare is reduced as the Cardmember uses the S/E's transport services.

An Expresspay Card or Expresspay Mobile can be used as a means to access the transit system for pay-in-advance accounts. In these situations, the S/E:

- Must limit the functions to account identification and fare validation
- Must not process "taps" at the TAT as a Transaction

4.2.10 Card Not Present Charges

For Charges made by mail, telephone, or Internet, where the Card is not present, the S/E must comply with the following procedures:

1. Obtain Authorization for every Charge.
2. Complete a ROC as described in Section 4.2.21, "Charge ROCs," on page 236, indicating "Internet Order," "Telephone Order," or "Signature on File," as applicable.
3. The S/E must ask the Cardmember for his/her name exactly as it appears on the Card, the Card Account number, the Expiration Date, the Cardmember address information, the PCSC (optional), and the address where the merchandise is to be shipped.
4. During the use of Automated Address Verification (AAV), the S/E will be notified whether or not the address matches the Cardmember's address information. Address Verification, which may be available in limited geographic regions, is a check, not a guarantee, that a Charge is legitimate.
5. If the order is shipped or delivered more than seven (7) days after the original Authorization, the S/E must obtain a new Authorization before shipping or delivering the merchandise. Charges may not be submitted for payment until the order is shipped. The Transaction Date of the Charge is the date the Goods are shipped or delivered.

   Note: S/Es are responsible for the actions of their delivery agents; therefore, S/Es are advised not to allow shipping address changes or interceptions to occur during the delivery. Whenever possible, the S/E should deliver merchandise to the matched Cardmember's address information, and except for S/Es in the United States and Canada, obtain a signature of the Person accepting the delivery.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6. If the Goods are ordered as a Card Not Present Transaction but they are to be paid for and collected by the Cardmember at a physical store, the Cardmember must present the Card and the S/E must adhere to the policies described in Section 4.2.7, "In-Person Charges," on page 216.

4.2.10.1 Internet S/E Card Acceptance Requirements

When conducting Transactions over the Internet, S/Es:

- Must use the appropriate Point of Service Data Code indicating the Transaction was processed via the Internet (for Recurring Billing Transactions conducted via an Internet S/E, see Section 4.2.15, "Recurring Billing," on page 225). See Point of Service Data Codes in the *Codes Reference Guide.*
- Must electronically authorize and electronically submit all Internet Transactions.

All Internet sales must have a zero (0) Floor Limit.

Note: Internet Charges made with Chip Cards through a Chip-Enabled Device are considered to be Card Present Transactions.

4.2.10.2 American Express SafeKey Card Acceptance Requirements

SafeKey is an industry-standard Authentication method that, when employed by Issuers, Cardmembers, Acquirers, and S/Es, provides greater security for Transactions. When conducting SafeKey Transactions, S/Es:

- Must initiate a single Authentication request per Transaction
- Must not reuse Authentication Data other than as stated in Section 2.9.18.1, "Reuse of SafeKey Authentication Data," on page 108

AEGNS recommends that S/Es should not submit a POS Authorization Request (1100) message when the Cardmember's SafeKey Authentication failed.

4.2.10.3 Online Order/In-Store Pick-up Transaction Processing

This section details the requirements related to Transactions involving Internet orders for Goods scheduled to be picked up at a designated physical store.

Transactions that are authorized and paid for in-store, prior to the Goods being picked up, are considered Card Present Transactions, and are subject to the policies outlined in Section 4.2.7, "In-Person Charges," on page 216.

Internet Transactions conducted via online order, where the Goods are later picked up in-store, may be authorized using SafeKey, an industry-standard Authentication method that provides greater security for Internet Transactions. SafeKey Transactions must adhere to the SafeKey policy requirements detailed in the following sections:

- Section 2.9.18, "American Express SafeKey Acquirer Requirements," on page 107
- Section 2.10.13, "American Express SafeKey Issuer Requirements," on page 119
- Section 4.2.10.2, "American Express SafeKey Card Acceptance Requirements," on page 222
- Section 7.10.8.3, "American Express SafeKey Fraud Liability Shift," on page 361
- Section 8.9.6.1, "American Express SafeKey Fraud Liability Shift Qualification S/E Fraud Thresholds," on page 391

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

To increase the security of Internet Transactions and mitigate fraud, AEGNS strongly recommends Acquirers encourage their S/Es to participate in the SafeKey program, and implement procedures that mitigate fraud during in-store pick-up that occurs after Internet Transactions were completed/processed. Such procedures may include:

- Clear and easy to understand pick-up policies at the time an online order is placed
- Acknowledgment option by the Cardmember of having read the S/E's policies on in-store pick-up of Goods ordered online
- Specific timeframes for the pick-up of Goods
- Policies addressing scenarios when Goods have not been picked up within the timeframes specified by the S/E
- Process to ensure that Goods purchased through an Internet Transaction are picked up by the Cardmember who placed the order, or by the authorized third party designated by the Cardmember at the time of the Internet Transaction

S/Es should follow all policy requirements detailed in Section 2.9.11, "S/E Card Acceptance Process," on page 102; Section 4.2.17, "Acceptable Forms of ID," on page 226; and Section 5.10.2, "Cardholder Verification Methods," on page 263.

When a Cardmember purchases Goods through an Internet Transaction and such Goods are subsequently not picked up before the pick-up deadline specified in the S/E's policy, the S/E's standard return policies shall apply.

4.2.11 Credentials-on-File

Credentials-on-File include any Cardmember account data, including, but not limited to, PAN or Token, that is stored by or on behalf of S/Es.

S/Es must obtain Cardmember consent before storing Cardmember credentials. AEGNS recommends that S/Es process an initial Authorization upon receiving Cardmember consent to store credentials.

S/Es may store Cardmember credentials to initiate Merchant-Initiated Transactions (MITs). Cardmembers may also use their stored credentials to initiate Transactions.

4.2.12 Merchant-Initiated Transactions

A Merchant-Initiated Transaction (MIT) is a Transaction that is initiated by the S/E through use of Credentials-on-File without direct participation from the Cardmember.

S/Es must obtain Cardmember consent to initiate an MIT, or a series of MITs, after storing a Cardmember's credentials. Cardmember consent for MITs and Credentials-on-File may be obtained simultaneously.

AEGNS recommends that S/Es submit MITs only after an initial Cardmember-Initiated Transaction (CIT) or an initial Authorization accompanying a Cardmember's request to store credentials.

AEGNS recommends that S/Es submit MITs with the following data elements in the Authorization Request:

- MIT indicator
- Original TID

S/Es must adhere to the requirements in Section 4.2.10, "Card Not Present Charges," on page 221 when processing MITs.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.13 Aggregated Transactions

This section explains the general policies and rules that apply to the processing of multiple purchases as a single Aggregated Transaction.

These policies apply only to Transactions processed by S/Es conducting business over the Internet; as such, they are considered Card Not Present Transactions.

4.2.13.1 General Requirements

Acquirers must ensure that their S/Es comply with the following requirements when processing Aggregated Transactions:

- Individual purchases that comprise the Aggregated Transaction must be incurred on the same Card Account number and S/E number.
- Prior to the Transaction being authorized, the S/Es must disclose that individual purchases may be aggregated and obtain the Cardmember's consent to combining such purchases into one (1) Aggregated Transaction.
- S/Es must obtain an Authorization not greater than $15 (USD or local currency equivalent) in advance of a Transaction being aggregated. Refer to Section 5.2.1, "Online Authorization Processing," on page 245 and Section 5.6.2, "Card Not Present Authorization Requests," on page 254 for information on Authorization procedures.
- S/Es must create a Record of Charge for the full amount of the Aggregated Transaction (not to exceed $15), in accordance with policies in Section 4.2.21, "Charge ROCs," on page 236.
- S/Es are required to provide a confirmation to the Cardmember of the date, amount, and description of each individual purchase, as well as the date and amount of the Aggregated Transaction.

4.2.13.2 Submission Requirements

Acquirers must submit a Record of Charge for each Aggregated Transaction within the timeframe outlined in Section 2.9.12, "Acquirer Transaction Processing Requirements," on page 102. The Transaction Date of the ROC is the date the last individual purchase was incurred.

Acquirers must ensure that a meaningful description of the products and/or services that comprise a single Aggregated Transaction is included as part of the submission (outclearing) process to the Network. Refer to Section 2.9.15, "Internet Transaction Descriptor Information," on page 103.

The amount of the Aggregated Transaction submitted to the AEGN must not exceed $15.

4.2.14 Customer Activated Terminals

S/Es using Customer Activated Terminals (CATs) must be identified in the Authorization Request message via the Point of Service Data Code. All Transactions at CATs must be Authorized. Refer to the *Network Specifications - Authorization* manual and *Codes Reference Guide*.

Acquirers must ensure that all (new, replaced, or existing) unattended chip-enabled offline or online capable Customer Activated Terminals (CATs) (except terminals using Expresspay Specification 1.0 (EP1.0), Transit Access Terminals (TATs) and ATMs) support "No CVM" for Expresspay and AEIPS Transactions.

Acquirers must ensure that the terminal examines the chip CVM list in priority order and selects the first CVM supported by both the terminal and the chip. Refer to the *AEIPS Terminal Technical Manual*, Expresspay Terminal Specifications, *Acquirer Chip Card Implementation Guide*, *AEIPS Terminal Implementation Guide*, and *American Express Contactless Terminal Implementation Guide* located on Knowledge Base.

At AEGNS' discretion, Acquirers and their S/Es may support PIN Bypass at CATs. Refer to Section 2.9.17.3, "PIN Bypass Requirements for Acquirers," on page 105.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.15 Recurring Billing

Recurring Billing is a payment method whereby the Cardmember has authorized the S/E to bill the Cardmember's Card account on a periodic basis for a product or service agreed in writing by the Cardmember. Each payment may be for a variable or a fixed amount. S/Es should adhere to the requirements in Section 4.2.12, "Merchant-Initiated Transactions," on page 223 when processing non-initiated Charges for Recurring Billing:

- Disclose the material terms of the Recurring Billing Transaction Agreement to the Cardmember including, but not limited to, the duration of the Recurring Billing agreement, the amount, and frequency with which the Recurring Billing Transactions will be submitted, and
- Notify the Cardmember that they can revoke their consent to process Recurring Billing Transaction on their Card
- Ensure Recurring Billing Transactions (including those that originate from an Internet S/E) contain the POS Data Code populated with the Recurring Billing Indicator in the POS Authorization Request (1100) message and POS First and Second Presentment (1240) messages
- Submit an Authorization Request for all Recurring Billing Transactions (see Section 5.6.2, "Card Not Present Authorization Requests," on page 254 for details)
- Obtain the Cardmember's express consent to process Recurring Billing Transactions on their Card for Goods/Services, and
- Obtain the Cardmember's express consent to renewals, and
- Retain Documentation that validates the Cardmember's consent to process Recurring Billing Transactions. This Documentation must be maintained for the length of the Recurring Billing agreement or two (2) years from the last Recurring Billing Transaction, whichever is longer.

Any change to the Recurring Billing Transaction agreement must be lawful and in accordance with that agreement. Such change must be effective prior to the submission of any subsequent Recurring Billing Transactions on the Card.

S/Es that submit Recurring Billing Transactions must provide a simple and expeditious cancellation process for Recurring Billing Transactions. This cancellation process must be clearly and conspicuously disclosed to the Cardmember at the time of the Cardmember's consent to submit Recurring Billing Transactions on the Card.

If the Cardmember withdraws consent for future transactions in a series of Recurring Billing Transactions, the Recurring Billing S/E must not submit future Recurring Billing Transactions on the Card. Notification may come from the Cardmember directly, or if local laws or regulations prohibit requiring the Cardmember to contact the Recurring Billing S/E, notification may come from the Cardmember's Issuer. If a Cardmember withdraws consent but the Recurring Billing S/E continues to submit Recurring Billing Transactions, AEGNS may reject the Transaction or the S/E may be subject to Chargebacks. Refer to "ISO 4544 - Cancellation of Recurring Goods/Services" on page 332 for more information and Section 1.7, "The Transaction Life Cycle," on page 10.

4.2.15.1 Introductory Offers

Recurring Billing S/Es that provide Introductory Offers to Cardmembers must comply with the following requirements, in addition to those stated in Section 4.2.15, "Recurring Billing," on page 225:

- Disclose the material terms of the Introductory Offer to Cardmember, clearly and conspicuously, including a simple and expeditious cancellation process that allows the Cardmember to cancel before the first Recurring Billing Transaction occurs.
- Obtain the Cardmember's express consent to enter into the terms and conditions of the Introductory Offer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Send Cardmember a confirmation notification in writing upon enrollment in the Introductory Offer.
- Send Cardmember a reminder notification in writing before the first Recurring Billing Transaction is set to occur, that allows the Cardmember a reasonable amount of time to cancel.

4.2.16 Installment Sales

S/Es should adhere to the requirements in Section 4.2.12, "Merchant-Initiated Transactions," on page 223 when processing installment sales.

S/Es may not complete a Transaction when only a part of the total amount is on the ROC unless the Cardmember pays the balance by other means at time of purchase or if the purchase is an installment sale. All installment sales must be Authorized and may not include finance fees from the S/E. S/Es may not charge the first installment until the merchandise is shipped to the Cardmember and thereafter no sooner than the monthly anniversary dates of the original sale. S/Es must be able to retrieve a copy of the written agreement for the length of the installment sale or for two (2) years, whichever is longer.

4.2.17 Acceptable Forms of ID

The following are considered acceptable forms of Cardmember identification when required:

- Passport
- Driver's license with photograph and signature
- Military identification document
- National ID

4.2.18 Non-Real Time (Delayed) Authorizations

S/Es should obtain Authorization for Transactions in excess of the Floor Limit, prior to completion of the Transaction with the Cardmember. Legitimate exceptions may occur in Industries where the S/E is not able to connect to their Acquirer or Acquirer Processor at the time of the Transaction. For example:

- In-flight commerce Transactions where the airline requests Authorization after landing and the Cardmember has already disembarked.
- Craft fairs, flea markets or other remote environments where the S/E's electronic POS device does not have an online connection to the Acquirer or the Acquirer's Processor, or the S/E produces manual Record of Charges (ROCs)

S/Es should submit Delayed Authorization Requests to their Acquirer or Acquirer Processor as soon as connectivity is available.

Acquirers are required to submit Delayed Authorizations to the Network as described in Section 5.2.1.3, "Online Authorization Process," on page 245.

Acquirers may not submit a POS First Presentment (1240) message following a declined Authorization Request. Transactions presented following a declined Authorization may be subject to Chargeback, as described in the "Chargeback Policies" chapter beginning on page 280.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.19 Estimated Charge Amounts

An estimated Charge is an S/E's best estimate for the final Transaction amount that will be submitted. An S/E must inform the Cardmember of any estimated amount for which Authorization will be requested and must obtain the Cardmember's consent to the estimated amount before initiating the Authorization Request.

Lodging, cruise line, car rental, restaurant, and taxicabs/limousine S/Es are permitted to obtain an Authorization for an estimated Charge amount, provided they comply with their respective requirements as follows:

- For lodging S/Es, refer to Section 4.2.19.1, "Lodging," on page 227
- For cruise line S/Es, refer to Section 4.2.19.2, "Cruise Lines," on page 227
- For car rental S/Es, refer to Section 4.2.19.3, "Car Rental," on page 227
- For restaurant S/Es, refer to Section 4.2.19.4, "Restaurants and Bars," on page 228
- For taxicabs/limousine S/Es, refer to Section 4.2.19.5, "Taxicabs/Limousines," on page 229
- For Card Not Present grocery and retail S/Es, refer to Section 4.2.19.6, "Card Not Present Grocery and Retail," on page 229

4.2.19.1 Lodging

A lodging S/E must obtain an estimated Authorization at check-in based on the Cardmember's intended length of stay, the room rate, applicable tax and/or service charge rates, and the S/E's procedure for estimating additional ancillary Charges. Before initiating an Authorization Request, an S/E must inform the Cardmember of any estimated amount for which Authorization will be requested and obtain the Cardmember's consent to the estimated amount.

The Authorization will be valid for the duration of the lodging stay, provided the final submitted Transaction amount does not exceed more than 15% of the Authorization amount.

If upon Cardmember checkout, the final Transaction amount is greater than the estimated Charge by more than 15%, the S/E must obtain Authorization for any additional amount of the Charge that is greater than the original estimated Authorization amount.

4.2.19.2 Cruise Lines

A cruise line S/E may obtain an estimated Authorization at embarkation based on the Cardmember's intended length of stay, the room rate, applicable tax and/or service charge rates, and the S/E's procedure for estimating additional ancillary Charges. Before initiating an Authorization Request, an S/E must inform the Cardmember of any estimated amount for which Authorization will be requested and obtain the Cardmember's consent to the estimated amount.

If the S/E does make an estimated Charge, the Authorization will be valid for the duration of the stay, provided the final submitted Transaction amount does not exceed more than 15% of the Authorization amount.

If, upon Cardmember checkout, the final Transaction amount is greater than the estimated Charge by more than 15%, the S/E must obtain a new Authorization for any additional amount of the Charge that is greater than the original estimated Authorization amount.

4.2.19.3 Car Rental

On the first day of the rental, the car rental S/E shall obtain Authorization for the full estimated amount of the Charge. The estimated Charge shall be determined by multiplying the applicable rental rate, tax and/or mileage rates and any ancillary charges by the rental period reserved by the Cardmember. The S/E shall not overestimate this amount and under no circumstances shall the estimated Transaction amount include ancillary Charges that represent either an amount for any possible damage to or theft of the vehicle or the insurance deductible amount when the Cardmember waives the insurance coverage at the time of rental.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Before initiating an Authorization Request, an S/E must inform the Cardmember of any estimated amount for which Authorization will be requested and obtain the Cardmember's consent to the estimated amount.

The Authorization will be valid for the life of the rental agreement, provided the final submitted Transaction amount does not exceed more than 15% of the Authorized amount.

If upon return of the rental vehicle, the final Transaction amount is greater than the estimated Charge by more than 15%, the S/E must obtain Authorization for the amount of the Charge which is greater than the original estimated Authorization amount.

4.2.19.3.1 Capital Damages to Rental Vehicles - Charge Submission Requirements

If upon return of a rental vehicle, the car rental S/E discovers that the vehicle has been damaged and the Cardmember has not purchased the car rental S/E's collision or loss insurance, the car rental S/E may submit a Charge for a specific-amount estimate of the capital damages incurred.

The Charge, which shall be submitted separately from any Charge submitted for the cost of the car rental, may be submitted, provided the following conditions are met:

1. Prior to billing, the car rental S/E has obtained the Cardmember's agreement in writing to:
   - A specific estimate of the capital damages,
   - Accept responsibility for the capital damages, and
   - Select American Express as the payment method for the capital damages.
2. The car rental S/E has obtained a separate and additional Authorization for the specific estimate of the capital damages to which the Cardmember has agreed in condition 1 above.
3. The original Charge for the car rental was made on an American Express Card of the Cardmember who agreed to the details referred to in condition 1 above. A car rental S/E must never include the following in an Authorization Request or in a Charge Submission:
   - Losses due to theft of the vehicle, or
   - Loss of revenue incurred by the car rental S/E due to loss of use of the rental vehicle in question.
4. The Charge submitted for capital damages may not exceed the following:
   - 15% above the amount established in the specific estimate of the capital damages, or
   - The replacement cost of the vehicle, in the case of a total loss, due to damages caused by the Cardmember.

S/Es should adhere to the requirements in Section 4.2.12, "Merchant-Initiated Transactions," on page 223 when processing Capital Damages.

4.2.19.3.2 Capital Damages to Rental Vehicles - Documentation

The S/E must comply with requests from the Cardmember or the Cardmember's insurance adjustor to supply Documentation related to the capital loss incident.

4.2.19.4 Restaurants and Bars

An Authorization obtained by a restaurant or bar S/E is considered to be valid if the Authorization Request is within a plus or minus 30% (20% for Prepaid Cards and Debit Cards) range of the final submitted amount. Before initiating an Authorization Request, an S/E must inform the Cardmember of any estimated amount for which Authorization will be requested and obtain the Cardmember's consent to the estimated amount. The estimated Charge amount is valid for up to seven (7) days from the date of the Authorization.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.19.5 Taxicabs/Limousines

An Authorization obtained by a taxicab/limousine S/E is considered valid if the Authorization Request is within a plus or minus 20% range of the final submitted amount. Before initiating an Authorization Request, an S/E must inform the Cardmember of any estimated amount for which Authorization will be requested and obtain the Cardmember's consent to the estimated amount. The estimated Charge amount is valid for up to seven (7) days from the date of the Authorization.

4.2.19.6 Card Not Present Grocery and Retail

An Authorization obtained by a Card Not Present grocery or retail S/E is valid if the Authorization Request is within a plus or minus 15% range of the final submitted amount. Before initiating an Authorization Request, an S/E must inform the Cardmember of any estimated amount for which Authorization will be requested and obtain the Cardmember's consent to the estimated amount. The estimated Charge amount is valid for up to seven (7) days from the date of the Authorization.

4.2.20 Special Programs

Special Programs with specific requirements exist to facilitate unique processing environments. These programs enable Participants to provide specialized service to their S/Es and Cardmembers as well as help Participants reduce costs associated with processing Transactions on the AEGN.

4.2.20.1 No Show Reservations Program

This policy supports the agreement/contract between an AEGN Acquirer and lodging S/Es to participate in the No Show Reservations Program (Assured Reservation Program). The program allows Cardmembers to guarantee their reservation for one (1) night's stay at a lodging S/E. The S/E must advise the Cardmember of its cancellation policy at the time of the reservation and, if the Cardmember fails to cancel in accordance with this policy, the S/E may charge the Cardmember for one (1) night's stay. S/Es should adhere to the requirements in Section 4.2.12, "Merchant-Initiated Transactions," on page 223 when processing No Show Reservation Transactions.

Lodging S/Es participating in the No Show Reservations Program are required to meet the following policy requirements for reservations, cancellations, and alternate accommodations.

4.2.20.1.1 Lodging Reservation

A Cardmember may contact a lodging S/E and provide his/her Card Account number and Expiration Date to hold a reservation for one (1) night's stay. The S/E must inform the Cardmember of the rate for the room accommodation for one (1) night. At the time of the reservation, the S/E must provide the Cardmember with a confirmation code and cancellation policy. The S/E must reserve accommodations until the published check-out time the following day.

4.2.20.1.2 Lodging Cancellation

Upon a Cardmember cancellation, the S/E must provide the Cardmember with a cancellation number and maintain a record of such cancellation number.

If the accommodations are not claimed or cancelled within the time specified in the S/E's cancellation policy, the S/E may charge the Cardmember's Account for one (1) night's lodging. To charge a Cardmember's Account, either the words "No Show" must appear on the signature line of the ROC, or the S/E must transmit the appropriate Lodging Special Program Code, "No Show Reservation Transaction," to the AEGN. Failure to do so may result in the Issuer initiating an "ISO 4513 - Credit Not Presented" on page 312 Chargeback.

Refer to the *Codes Reference Guide* for more information on the Lodging Special Program Code.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.20.1.3 Alternate Lodging Accommodations

The S/E must arrange and pay for alternate accommodations if the reserved accommodations are not available on the specified date and time. The S/E will provide the Cardmember with the following services at no additional charge:

- Comparable accommodations for one (1) night at another establishment
- If requested, a three (3) minute phone call
- Transportation to the alternate establishment's location

4.2.20.2 No Show Reservation Requirements for Other Industries

Special processing requirements apply to S/Es that submit No Show Reservation Transactions in the following rental industries:

- Vehicle rental
- Aircraft rental
- Bicycle rental
- Boat rental
- Equipment rental
- Motor home rental
- Motorcycle rental
- Trailer park and campgrounds rental

4.2.20.2.1 Rental Reservation

Upon providing the appropriate Card credentials, Cardmembers may have the rental S/E hold a rental reservation for one (1) day's rental or the relevant incremental equivalent (such as hourly) of the rate agreed. The S/E must:

1. Inform the Cardmember of the rental rate, and
2. Provide the Cardmember with a reservation confirmation code
3. Provide the Cardmember the S/E's cancellation policy including the cancellation deadline to avoid a no show charge as well as the no show charge amount.

4.2.20.2.2 Rental Cancellation

If a Cardmember decides to cancel a No Show Reservation Transaction in accordance with the S/E's agreed-upon cancellation policy, the S/E must provide the Cardmember a cancellation number and maintain a record of such cancellation.

If the rental services are not cancelled in compliance with the S/E's cancellation policy, the S/E may submit a No Show Reservation Transaction equivalent to one (1) day's rental charge, or the relevant incremental equivalent (such as hourly) of the rate agreed.

To charge a Cardmember's account, the S/E must either:

- Print the words 'No Show' on the signature line of the ROC, or
- Transmit to the AEGN the appropriate Additional Amount Type Code "No Show Charge."

Failure to do so may result in the Issuer initiating an "ISO 4513 - Credit Not Presented" on page 312.

Refer to the Network Specifications manuals and the *Codes Reference Guide* for more information on the Additional Amount Type Code "No Show Charge."

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.20.2.3 Alternative Rental Services

If an S/E cannot fulfill a rental reservation on the specified date and time, the S/E must provide comparable accommodations, and/or services, when reasonably available, at no additional cost to the Cardmember in accordance with the S/E's rental agreement and/or local laws and regulations.

4.2.20.3 Advance Deposit or Payment Program

This policy supports the agreement between the AEGN Acquirer and lodging S/Es to participate in the Advance Deposit or Payment Program. The Advance Deposit or Payment Program allows Cardmembers to charge the payment of an advance deposit to their Card when such a deposit is required.

This Advance Deposit or Payment will hold a reservation for the intended length of stay. S/Es may not present an Advance Deposit or Payment Transaction for an amount that exceeds the cost of a fourteen (14) night stay plus applicable taxes.

4.2.20.3.1 Reservation Policy Disclosure

When taking an Advance Deposit or Payment from a Cardmember, the S/E must inform the Cardmember of the Advance Deposit or Payment requirements and the cancellation policy for such reservations. The S/E is required to provide the Cardmember with written confirmation of the arrival and departure dates, the amount of the Advance Deposit or Payment, a confirmation number and the S/E's cancellation policy.

For each Advance Deposit or Payment, the S/E must complete a Record of Charge with the following information:

1. The S/E must write the words "Advance Deposit" on the signature line of the ROC or transmit the appropriate Advance Deposit description on the Charge data.
2. The S/E must indicate the scheduled arrival date on the Record of Charge.

4.2.20.3.2 Cancellation Policy Disclosure

Upon cancellation of the reservation, the S/E must send written cancellation notice indicating the cancellation number to the Cardmember within three (3) Business Days. If a refund is due, the S/E must submit a Credit record with the words "Advance Deposit Cancellation" on the signature line or transmit the appropriate Advance Deposit indicator on the Credit Transaction.

If the arrival date of an Advance Deposit or Payment is changed, the S/E is required to send the Cardmember a written confirmation of the change within three (3) Business Days.

4.2.20.3.3 Alternate Accommodations

If the S/E is unable to honor the reserved accommodations and the reservation was not cancelled by the Cardmember, the S/E must:

- Issue a Credit ROC for the Advance Deposit or Payment.
- Pay for accommodations at a comparable location nearby until the duration of the original reservation expires (up to fourteen (14) nights), or until accommodation become available at the original location, whichever occurs first.
- Pay for transportation to the alternate establishment and for a return to the original location once per day until the original accommodations are available.
- Provide up to two (2) three-minute telephone calls for the Cardmember's alternate accommodations.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.20.4 No Signature/No PIN Program

The No Signature/No PIN Program allows an S/E to process a Card Present Transaction without obtaining the Cardmember's signature or PIN as required in Section 4.2.7, "In-Person Charges," on page 216, unless required by local law or regulation, if all of the following requirements are met:

- The S/E is in a designated country listed in the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide*.
- The Transaction amount is equal to or less than the amount listed in the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide*.
- The S/E Merchant Category Code (MCC) is not listed in Table 4-3, "Ineligible Merchant Category Codes for the No PIN Program," on page 232.
- The Transaction is Authorized.
- The Point of Service Data Code values provided in the POS First Presentment (1240) message must indicate a Card Present and Cardmember Present Transaction.

Note: Obtaining Cardmember signature on Card Present Transactions is optional to complete a ROC, and at the discretion of the S/E, unless required by applicable law.

Table 4-3. Ineligible Merchant Category Codes for the No PIN Program[1]

Code	Description
4814	Telecommunications Services
4816	Comp Network/Information Services
4829	Wire Transfers and Money Orders
4899	Cable and Other Pay Television Services
5542	Automated Fuel Dispensers
5964	Direct Marketing - Catalog Merchants
5966	Direct Marketing - Outbound Telemarketing Merchants
5967	Direct Marketing - Inbound Telemarketing Merchants
6010	Financial Institutions - Manual Cash Disbursements
6011	Financial Institutions Automated Cash Disbursements
6051	Non Financial Institutions - Foreign Currency, Money Orders (not Wire Transfer), Scrip and Travelers Checks
7273	Dating and Escort Services
7297	Massage Parlors
7375	Information Retrieval Services
7393	Detective Agencies, Protective Agencies and Security Services

1. S/Es in these MCCs must obtain PIN if an AEIPS Chip and PIN Card is presented at a Chip and PIN-enabled POS device.

If all of the above requirements are met, the AEGN will provide the Issuer with a Program Indicator in the POS First Presentment (1240) message. The Program Indicator with a "No Signature/No PIN" value indicates that the Transaction qualifies for the No Signature/No PIN Program. Refer to the *Network Specifications - Financial/Non-Financial* manual for details on the POS First Presentment (1240) message.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.20.5 ZIP Code Verification (ZCV) Program

The ZIP Code Verification Program (ZCV) allows participating S/Es to submit the Cardmember's billing address ZIP code as part of the Authorization Request for Issuer validation as an additional fraud prevention measure. If the Transaction meets all of the requirements listed below, an Issuer may not submit a 6006 - "Legal Request or Fraud Analysis" Retrieval Request to AEGNS.

- The Transaction must be initiated by a Card issued in the U.S. or Puerto Rico at a participating S/E located in the U.S. or Puerto Rico.
- The Transaction must be swiped and magnetic stripe data must be transmitted in the Authorization Request.
- The S/E's POS device must have prompted for the Cardmember's billing address ZIP Code.
- The Acquirer must populate the Program Indicator on the POS First Presentment (1240) message with the value corresponding to the ZCV Program. Refer to the *Network Specifications - Financial/Non-Financial* manual for details on the POS First Presentment (1240) message.

Refer to ISO Message Reason Code 6006 - Legal Request or Fraud Analysis in Table 7-3, "Retrieval Request Notification Reasons," on page 289 for information regarding the ZIP Code Verification Program

Note: Refer to the Codes Reference Guide for a list of all valid Message Reason Codes.

4.2.20.6 Name and Address Verification (NAV) Program

The Name and Address Verification Program allows a U.S. or Canadian S/E to contact a U.S. or Canadian Issuer (via the S/E's Acquirer) to confirm Cardmember name and address information during the Authorization process. Refer to Section 5.10.1.2, "Name and Address Verification (NAV) Program," on page 262 for more information.

4.2.20.7 Promotional Program Capability

Promotional Program capability is a feature that drives spend and loyalty by closing the redemption loop in local S/E commerce utilizing the AEGN. It allows participating S/Es to provide a "coupon-less" discount to Cardmembers.

Promotional Program Transactions are supported in the following markets:

Table 4-4. Promotional Program Markets

Markets	Countries
Europe/Middle East/Africa	• United Kingdom • Netherlands • Spain • France • Sweden

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 4-4. Promotional Program Markets (continued)

Markets	Countries
Americas	• Canada • United States • United States Territories
Asia Pacific	• Australia • Hong Kong (Special Administrative Region of China) • India • Japan • Republic of Korea (South Korea) • New Zealand • Singapore

Refer to Section 7.10.9, "Promotional Program Transactions," on page 362 for additional information related to disputes processed on a Promotional Program Transaction.

Refer to the Network Specifications manuals and *Codes Reference Guide* for Promotional Program Transaction message information.

4.2.20.8 POS Online PIN Certification and Enablement Program

In designated countries, AEGNS mandates that Chip and PIN-enabled POS devices must be capable of processing Online PIN and Offline PIN.

Acquirers in designated countries must deploy this program in two (2) stages:

- New and Replaced: AEGNS requires that new and replaced Chip and PIN-enabled POS devices must have Online and Offline PIN processing enabled.
- All POS Devices: AEGNS requires that all existing, active Chip and PIN-enabled POS devices must have Online and Offline PIN processing enabled. Any Chip and PIN-enabled POS device that is unable to process Online and Offline PIN must be decommissioned.

All Chip and PIN-enabled POS devices must be certified to support Online and Offline PIN prior to deployment.

The POS Online PIN Certification and Enablement Program requirements are in addition to existing chip and PIN requirements, including AEIPS Certification for PIN-capable devices. This mandate applies to Chip and PIN-enabled POS devices only and does not apply to POS devices that are not PIN capable.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Refer to the following table for a list of designated countries and effective dates:

Table 4-5. POS Online PIN Certification and Enablement Program Participation

Region	Countries	Effective Date
Americas	Caribbean Countries, United States, and United States Territories	Dec 31, 2016 - New and Replaced Dec 31, 2018 - All POS Devices
	Brazil	Dec 31, 2017 - New and Replaced Dec 31, 2019 - All POS Devices
	Chile, Peru	Dec 31, 2020 - New and Replaced Dec 31, 2021 - All POS Devices
	Paraguay	Dec 31, 2021 - New and Replaced Dec 31, 2022 - All POS Devices
	Costa Rica	Jul 1, 2022 - All POS Devices
	Mexico, Uruguay	Apr 14, 2023 - New and Replaced Apr 12, 2024 - All POS Devices
APAC	India	Jun 30, 2013 - All POS Devices
	Australia, New Zealand	Oct 5, 2015 - All POS Devices
	Indonesia	Jul 1, 2015 - All POS Devices
	Bangladesh	Jun 30, 2016 - All POS Devices
	Cambodia	Oct 18, 2016 - All POS Devices
	Malaysia	Jan 1, 2017 - All POS Devices
	Nepal	Oct 18, 2017 - All POS Devices
	China, Sri Lanka	Dec 31, 2019 - New and Replaced Dec 31, 2020 - All POS Devices
	Fiji, Maldives, Pakistan	Dec 31, 2021 - New and Replaced Dec 31, 2022 - All POS Devices
	Papua-New Guinea	Oct 14, 2022 - All POS Devices
	Brunei, Cook Islands, Philippines, Samoa, Solomon Islands, Thailand, Tonga, Vanuatu	Apr 14, 2023 - New and Replaced Apr 12, 2024 - All POS Devices

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 4-5. POS Online PIN Certification and Enablement Program Participation (continued)

Region	Countries	Effective Date
EMEA	Denmark, Norway, Russia, Turkey	Dec 31, 2017 - New and Replaced Dec 31, 2019 - All POS Devices
	Bahrain, Germany, Iraq, Italy, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, South Africa, United Arab Emirates, Yemen	Dec 31, 2019 - New and Replaced Dec 31, 2020 - All POS Devices
	Albania, Algeria, Angola, Azerbaijan, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Côte d'Ivoire (Ivory Coast), Czechia, Demo. Rep. of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Finland, Gabon, Gambia, Georgia, Ghana, Guinea, Guinea Bissau, Guyana, Kazakhstan, Kenya, Kyrgyzstan, Liberia, Libya, Macedonia (Formerly Yugoslav Republic of), Madagascar, Malawi, Mali, Mauritania, Mauritius, Mayotte, Moldova, Montenegro, Morocco, Mozambique, Namibia, Niger, Nigeria, Réunion, Rwanda, Sao Tome and Principe, Senegal, Serbia, Sierra Leone, Somalia, Swaziland, Sweden, Switzerland, Tajikistan, Tanzania, Togo, Tunisia, Uganda, Ukraine, Zambia, Zimbabwe	Dec 31, 2020 - New and Replaced Dec 31, 2021 - All POS Devices
	Armenia, Austria, Belgium, Croatia, Cyprus, Czech Republic, Greece, Hungary, Iceland, Ireland, Latvia, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Spain	Dec 31, 2021 - New and Replaced Dec 31, 2022 - All POS Devices
	Lesotho, North Sudan, Seychelles, South Sudan	Oct 14, 2022 - All POS Devices
	Bosnia, Bulgaria	Apr 14, 2023 - New and Replaced Apr 12, 2024 - All POS Devices

4.2.21 Charge ROCs

For every Charge, the S/E must complete a ROC at time of purchase. Examples of ROCs include pre-printed ROC forms supplied to the S/E by the Acquirer, a Transaction receipt created by an electronic POS device such as an Authorization terminal with printer, or a checkout register.

Regardless of whether the ROC is manually imprinted or electronically created, a copy must be provided to the Cardmember at the conclusion of the Transaction. If an S/E changes the ROC information, it must provide a revised copy to the Cardmember.

S/E requirements for Charge ROCs:

- All electronically printed ROCs must truncate the Primary Account Number (PAN) and not display the Expiration Date in accordance with the PCI DSS in place at the time of the Transaction or according to applicable local law. S/Es may truncate the Primary Account Number (PAN) on their own copies in accordance with the PCI DSS in place at the time of the Transaction or according to applicable local law. Refer to Section 2.4, "Participant Data Security Policy," on page 38 for additional information.
- All ROCs must be kept for at least one (1) year (or longer if required by local law)

Note: For Expresspay Transactions using an Expresspay-enabled Card originating at Transit Access Terminals (TATs), a Record of Charge (ROC) is not required at the time of the Transaction. Please refer to Section 4.2.9.1.4, "Charge ROC Requirements for Expresspay Transactions at TATs," on page 220 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.21.1 Completing Charge ROCs

When a printed or electronic ROC is provided to the Cardmember, the S/E must ensure the ROC contains the following:

- The Card Account number truncated in accordance with requirements stated in Section 4.2.21, "Charge ROCs," on page 236. For manually imprinted ROCs provided to the Cardmember, the Account number and Expiration Date are required.
- Date the Charge was incurred.
- Amount of the Charge, which must be the total purchase price of Goods and Services purchased, including applicable taxes, tips, postage, and shipping charges. (Any tip amount, when required, should be filled in by the Cardmember before the total is entered in the form.)
- Description of the Goods and Services purchased.
- The S/E name (DBA, "Doing Business As" Name), address

  Note: If S/Es request Cardmember signature, S/Es may not require Cardmembers to sign a ROC until the total amount is shown.
- The words "No Refund," if a no-refund policy is applicable, or other wording describing a return policy which conforms to local laws or regulations.

4.2.22 Credit ROCs

When a Cardmember returns merchandise purchased with a Card or for any reason is due Credit toward a submitted Charge made with a Card, the S/E must comply with requirements established in Section 4.2.22.1, "Completing Credit ROCs," on page 237 and Section 4.2.22.2, "Credit ROC Restrictions," on page 238.

4.2.22.1 Completing Credit ROCs

A copy of the Credit ROC must be provided to the Cardmember at the conclusion of the Transaction. If an S/E changes the Credit ROC information, it must provide a revised Copy to the Cardmember.

The S/E must ensure that a printed or electronic Credit ROC contains:

- The Primary Account Number (PAN) or Token, the date of the Credit, the amount of the Credit, and the S/E name and address.
- The Cardmember signature, if required by law.
- All electronically printed Credit ROCs must truncate the PAN or Token and not display the Expiration Date in accordance with the PCI DSS in place at the time of the Transaction or according to applicable local law. S/Es may truncate the PAN or Token on their own copies in accordance with the PCI DSS in place at the time of the Transaction or according to applicable local law. Refer to Section 2.4, "Participant Data Security Policy," on page 38 for additional information.
- All Credit ROCs must be kept for a one (1) year period.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.2.22.2 Credit ROC Restrictions

S/E processing of Credit Transactions is subject to the following requirements and restrictions:

- An S/E must never issue a Credit unless that S/E previously processed a corresponding Charge.
- An S/E must only issue a Credit Transaction to the Account used in the original Charge. For Digital Wallet Program Transactions, the Credit can be processed using either the Mobile Device or the corresponding Card. The Payment Account Reference (PAR) can assist S/Es in verifying that the Primary Account Number (PAN) or Token presented corresponds to the Account used in the original Charge. Refer to Section 2.5.6, "Payment Account Reference," on page 70 for more information.
- There is no requirement for the S/E to obtain Authorization for a Credit.

  Note: S/Es may submit an Authorization on Credit for refunds outlined in Section 5.3.5, "Authorization on Credit," on page 249.
- An S/E must never refund Cash against a previously submitted Charge, except as follows:
  - If applicable law requires an S/E to refund cash to a Cardmember.
  - If the refund is being requested by the recipient of a gift purchased by a Cardmember.
  - The original Charge was processed on a Prepaid Card and that Prepaid Card is no longer available

  Note: S/Es may apply their in-store return policy when Prepaid Cardmembers no longer have their Card.

4.2.23 Delayed Delivery

A Delayed Delivery Transaction occurs when a Cardmember agrees to make a deposit or down payment for a purchase and the remainder of the purchase is made in a second Transaction when the Goods are shipped or delivered.

The S/E must clearly mark the first Transaction ROC as a 'deposit' and the second Transaction ROC as a 'balance'. Each ROC must be separately Authorized. The S/E must submit the 'balance' Transaction only when the Goods are shipped or delivered. S/Es should adhere to the requirements in Section 4.2.12, "Merchant-Initiated Transactions," on page 223 when processing Delayed Delivery Charges.

4.3 Code 10

If suspicious of a Card or Cardmember, S/Es should follow their own in-store policy and, if directed to do so, call their Acquirer and report a Code 10 Transaction. The S/E will be asked questions which require only a "yes" or "no" response so that the Cardmember's attention is not drawn to the clerk.

4.3.1 Suspect Cards

An S/E has cause to be suspicious of a Card if one (1) or more of the following signs of tampering are obvious (not restricted to this list):

- The signature panel has been taped over.
- A signature has been erased or covered with correction fluid.
- The embossing on the face of the Card appears uneven.
- The Account number on the back of the Card does not match the number on the front.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.3.2 Suspect Cardmember

If the Cardmember exhibits one (1) or more of the following behaviors (not restricted to this list), the S/E has cause for suspicion:

- The Cardmember is attempting to rush through the Transaction.
- The Cardmember is trying to determine the S/E's Floor Limit.
- The Cardmember needs to see the Card in order to sign the ROC.
- The Cardmember wants to collect Goods ordered via telephone, mail or Internet without presenting their Card.
- The Cardmember asks to split the payment between two (2) or more charge/credit products.
- The Cardmember regularly makes purchases with a Prepaid Card and attempts to return the items for cash.
- The Cardmember attempts to use a Prepaid Card to purchase another Prepaid Card.
- The Cardmember wants to use a large number of Prepaid Cards to make a single purchase.

4.3.3 Card Capture

In order to halt any further unauthorized use of a lost or stolen Card, an Issuer may instruct the S/E to "Pick Up" the Card. While this is the Issuer's prerogative, the S/E is not obligated to do so if capturing the Card might create a disturbance or the use of force by the individual presenting the Card. S/Es who do capture Cards under instructions of the Issuer and who then forward them to their Acquirer may be entitled to a reward based on the Acquirer's policy

Note: Some S/E POS devices are incapable of displaying either "Pick Up" or "Referral" responses. In their place, a "Deny" message will be displayed. AEGNS has no means to communicate back to the Issuer the response which actually appeared at the S/E terminal.

4.4 Card Recovery

AEGNS enables Acquirers to report recovered Cards to Issuers and facilitates the transfer of monetary awards from Issuers to Acquirers in instances where an Acquirer (via their S/E) has recovered (retained from the Cardmember) a Card believed to be altered, counterfeit or used fraudulently.

4.4.1 Card Recovery Criteria, Procedures and Cash Awards

S/Es may choose to recover Cards when:

- S/Es receive a "Pick Up Card" response in the POS Authorization Response (1110) message
- S/Es are advised to recover the Card as a result of a Code 10 (refer to Section 4.3, "Code 10," on page 238 for additional information), initiated, for example, if the last four (4) digits of the Card Account number printed on the terminal receipt by the POS terminal do not match those appearing on the front of the Card.

If a Card is recovered in circumstances not described above, the Acquirer must notify the Issuer or contact their AEGNS representative for further assistance. An award for a Card recovered outside of the above guidelines will be paid at the Issuer's discretion.

An S/E should only recover a Card in accordance with Acquirer-defined procedures and when it is safe to do so. To ensure full disablement, S/Es should destroy recovered Cards by cutting vertically through the magnetic stripe and chip, if one (1) is present.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Issuer award amounts for recovered Cards are as follows:

- A reward of $50 for any Card recovered after an S/E receives a "Pick up Card" response to an Authorization Request.
- A reward of $100 for any Card recovered after an S/E has been advised to recover the Card as a result of a Code 10.

In addition, Issuers will pay a $20 handling fee for the return of the recovered Card.

4.4.2 Recovered Card Reporting and Cash Award - Acquirer Responsibilities

To report a recovered Card and initiate an award claim, Acquirers should contact the Card Issuer.

- Issuers can be identified by the BIN number as part of the Card Account number on the Card, or by the bank name printed on the front of the Card. Issuer contact information relating to Card recovery can be found in the Participant Directory on Knowledge Base.
- Acquirers must complete the AEGNS Card Recovery Award Form. Refer to "Exhibit 12. AEGNS Card Recovery Award Form" on page 478 for a sample. Should the Issuer request it, the recovered Card must be mailed to the Issuer within five (5) Business Days from the date of the request.

4.4.3 Recovered Card Reporting and Cash Award - Issuer Responsibilities

If an Issuer chooses to obtain the recovered Card from the Acquirer, the Issuer should provide the Acquirer with the requisite address information when contacted about the Card recovery.

4.4.4 Payment of the Cash Award

Once the recovered Card has been reported and the AEGNS Card Recovery Award Form has been emailed to gnsfraud@aexp.com, the Network will facilitate Issuer payment to the Acquirer as part of the Settlement Process. Refer to Section 6.4.1, "Settlement Process," on page 272 for additional information.

4.5 Cash Disbursements

Cash Disbursement Transactions are the manual disbursements of cash to Cardmembers by a Cash Disbursement Provider. Refer to the Network Specifications manuals for specific processing information about Cash Disbursement Transactions.

Acquirers and their Cash Disbursement Providers are subject to all of the applicable requirements for Acquirers and S/Es as described in this chapter.

4.5.1 Card Acceptance Requirements for Cash Disbursement Providers

Cash Disbursement Providers are branch locations of Participants that have been certified to process Cash Disbursements. In addition to the requirements for S/Es in Section 4.2.7, "In-Person Charges," on page 216, Cash Disbursement Providers are required to perform the following steps when accepting a Card for a Cash Disbursement Transaction.

- Cardmember identification must be verified by the Cash Disbursement Provider at the time of the Transaction and the ID serial number must be recorded on the Record of Charge unless prohibited by local law or regulation. Refer to Section 4.2.17, "Acceptable Forms of ID," on page 226 for acceptable forms of identification.
- The PCSC must be entered when prompted by the POS device.
- All Cash Disbursement Transactions must be submitted to the Card Issuer for Authorization.
- Cash Disbursement Transactions may not be Voice Authorized and/or keyed.
- Transactions must be identified with a Merchant Category Code (MCC) 6010 - Financial Institutions Manual Cash Disbursements.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.6 ATM Requirements

AEGNS will provide Cardmembers with access to the Amex Shared ATM Network in accordance with this Section 4.6 and other applicable sections of the AEGN Manuals. AEGNS acts as a conduit for the provision of access to the Amex Shared ATM Network, which consists entirely of ATMs owned and operated by third parties. Each Participant, and not the AEGN, is responsible for its participation in, and their Cardmembers' access to, the Amex Shared ATM Network and compliance with all applicable rules including, but not limited to, requirements pertaining to PIN issuance and verification procedures and use of third-party trademarks.

The following requirements apply to Participants that either gain access to the Amex Shared ATM Network or act as an ATM Acquirer:

- Participants shall install and maintain the communication lines, modems, and telecommunication equipment which may be required to connect Participant's host computer and the host computer of AEGNS. Such connection(s) shall enable Authorization Requests and Authorization Responses, as applicable, in the Amex Shared ATM Network. Each Participant shall bear the costs related to utilization, maintenance, and removal of modems and telecommunication equipment located on such Participant's premises.
- Each Participant must maintain all of its ATMs in good repair and working order, and must maintain and update their ATM operating system software, as required. ATM Participant must indemnify American Express and hold American Express harmless from any third-party claims related to the operating system software in accordance with generally accepted industry standards and practices including, but not limited to, the relevant provisions of the PCI DSS.
- In addition to the above, each Issuer must provide to their Cardmembers access to the Amex Shared ATM Network, in accordance with the Participant Agreement and/or ATM Agreement and the following:
  - Section 1.6, "Network Services," on page 6
  - Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30
  - Section 3.9.2.2, "Cash Access," on page 210
  - Section 4.6, "ATM Requirements," on page 241
  - Section 5.3, "AEGNS Authorization Services," on page 247
  - Section 5.4, "Issuer Authorization Requirements," on page 251
  - Section 5.11, "ATM Authorizations," on page 266
  - Table 7-12, "Additional Data Required for ATM Transactions," on page 299
  - Section 7.10.3, "ATM Chargebacks," on page 354
  - Section 10.5.4, "ATM Service Fees," on page 407
  - The Network Specifications manuals
- In addition to the above, each ATM Acquirer must enable access to such Participant's ATM Network and/or Participant Shared ATM Network for all Cardmembers, in accordance with the ATM Agreement and the following:
  - Section 1.6, "Network Services," on page 6
  - Section 2.3, "Anti-Money Laundering, Screening, U.S. Sanctions, and Anti-Corruption Requirements," on page 30
  - Section 2.9.2.2.2, "On-Us POS and ATM (1340) Message Submission Requirements," on page 85
  - Section 3.9.2.2, "Cash Access," on page 210

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Section 4.6, "ATM Requirements," on page 241
- Section 5.3, "AEGNS Authorization Services," on page 247
- Section 5.5, "Acquirer Authorization Requirements," on page 253
- Section 5.11, "ATM Authorizations," on page 266
- Table 7-12, "Additional Data Required for ATM Transactions," on page 299
- Section 7.10.3, "ATM Chargebacks," on page 354
- Section 10.5.4, "ATM Service Fees," on page 407
- The Network Specifications manuals

In addition, AMEX is not responsible for the acts or omissions of any third-party member of the Amex Shared ATM Network, and will not be liable to Participants or any holders of Participants' Cards for any third-party member's refusal or failure to perform in accordance with the terms of this section.

4.6.1 ATM Access - Acquirers

ATM Acquirers providing access to ATMs are responsible for complying with AEGNS policies, rules, and procedures (including AEGNS manuals), as well as the applicable policies, rules, and procedures of any third-party ATM network in which the ATM Acquirer participates, regardless of whether such access is obtained or provided through AEGNS.

4.6.1.1 Terminal Requirements

A Participant that is an ATM Acquirer must provide access for all Cards to the Participant ATM Network. An ATM Acquirer must use reasonable best efforts to obtain Cardmember access to Participant Shared ATM Networks. The American Express Blue Box decal must be displayed at all ATMs at which Cards are accepted. The Blue Box decal must be of equal size and prominence to marks of other cards accepted.

ATM screen displays must support, at a minimum, the English language and the local language of the country where the ATM is located.

4.6.1.2 ATM Transaction Processing

ATM Acquirers must connect their ATMs and route Transactions directly to the AEGN as described in the Network Specifications manuals. All Card Transactions must be transmitted to the AEGN for Authorization and Settlement, except On-Us Transactions.

ATM Acquirers' ATMs must be able to process both the ISO and ANSI magnetic stripe formats at all ATMs accessed by Cardmembers.

ATM Acquirers' ATMs must be able to process transactions initiated by AEIPS-compliant Chip Cards or magnetic stripe cards, and process both the ISO and ANSI magnetic stripe formats at all ATMs. If an ATM Participant (or its processor) is AEIPS-compliant and enabled by American Express, then ATM Transactions with Chip Cards must be processed as AEIPS-compliant chip transactions. If an ATM Participant (or its processor) is not AEIPS-compliant and enabled by American Express, ATM Transactions must be processed as magnetic stripe transactions. In the event that the EMV chip embedded within the card is damaged, the ATM Transaction must not be completed.

ATM Acquirers' ATMs must provide ATM cash withdrawal services to Cardmembers. The minimum amount dispensable in a single ATM withdrawal transaction must be $20 (USD) or less (or the local currency equivalent). The maximum amount dispensable in a single transaction must be at least $500 (USD) or more (or the local currency equivalent). Other services, including providing ATM Balance Inquiry or balance transfer options, are offered to the ATM Acquirer's local Cardmembers at the ATM Acquirer's discretion.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4.6.1.3 ATM Card Acceptance

ATM Acquirers are responsible for ensuring that ATMs conform to the Card acceptance procedures as defined in this section.

4.6.1.3.1 Service Delivery

An ATM Acquirer shall place no restriction on the acceptance of Cards for cash withdrawal that is not imposed on all other cards that are accepted at the ATM. Discriminatory treatment of Cards is prohibited.

4.6.1.3.2 Transaction Log Archival Storage

The ATM Acquirer must maintain Transaction Logs for all Transactions submitted to Issuers via the AEGN. The ATM Acquirer must retain the original or electronically store Transaction Logs for all Transactions. The Transaction Log and other supporting Documentation for any Transaction must be supplied to the Issuer upon receipt of a Retrieval Request Notification (1642) message from the Issuer. The Transaction Log and other supporting Documentation must be available to the Issuer for a period of at least one (1) year (or as required by local law) following the Network Processing Date of the Transaction.

4.6.1.3.3 ATM Security Pictures

An ATM security picture request is an optional service, and availability is dependent on applicable laws and regulations.

If cameras are available, and whenever possible upon request, the ATM Participant (or its processor) may provide the Issuer with reasonably clear pictures of the user associated with any attempted Transaction at any of its ATM terminals. The request for ATM security pictures may follow a Retrieval Request, Documentation, and Fulfillment process. Refer to Section 7.4, "Retrieval Request and Fulfillment," on page 288.

Note: To request a picture on AEGNS Network Disputes Manager (NDM), specify "ATM security picture request" in the "Add new comments" section during the relevant Disputes Process Transaction Life Cycle.

4.6.2 ATM Access - Issuers

Issuers are required to provide access for their Cardmembers to the Amex Shared ATM Network. Refer to Section 3.9, "Issuer-Provided Services," on page 205 for additional information.

Issuers are responsible for complying with AEGNS policies, rules, and procedures (including AEGNS manuals), as well as the applicable policies, rules, and procedures of any third-party ATM network in which the Issuer participates, regardless of whether such access is obtained or provided through AEGNS.

4.6.3 ATM Card Capture

To halt unauthorized use of a lost or stolen Card, an ATM may capture a Card used during an attempted ATM Transaction. This policy applies for Cards captured in this manner.

AEGNS will route ATM Card capture requests from Issuers to ATM Acquirers. At the request of the Card Issuer, all Acquirers of ATM transactions are required to capture American Express-branded Cards used at ATMs they own or operate. The Acquirers are required to record the following information for all such Cards that are so captured:

- Card Account number
- Cardmember name
- Date and Time of Card capture

All Cards that are captured must be destroyed by cutting vertically through the magnetic stripe and chip, if one (1) is present, to ensure full disablement of the Card.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Captured card logs must be retained for a minimum of two (2) years.

AEGNS and American Express Entities are not responsible or liable for any Cards or non-American Express-branded cards that are not captured, captured in error, or for the logging or failure to log any information relating to Cards or non-American Express-branded cards, or for any claims arising from Cards or non-American Express-branded cards that are captured.

4.6.4 ATM Locations

As a Cardmember benefit and to promote the services of ATM Acquirers, AEGNS collects ATM location information and makes it available to all Cardmembers via the AEGNS ATM Locator website. ATM Acquirers must submit quarterly to AEGNS a complete listing of all ATMs for which the ATM Acquirer provides access.

Such information shall be provided by the ATM Acquirer within fifteen (15) days following receipt by the ATM Acquirer from AEGNS of a template listing all data fields which must be completed for each ATM. AEGNS will submit such template to the ATM Acquirer no more frequently than on a quarterly basis. The response file must be submitted in the required electronic format to AEGNS or a designated third-party vendor via secure email using the template provided. No incomplete or anticipated changes should be included in the list. The information must be provided in the English language.

The required information includes:

- Name - Complete name of where the ATM is located (for example, bank name).
- Address - Physical address of where the ATM is located.
- ATM ID - Terminal identification number of the ATM.
- Airport Code - If the ATM is located in an airport, this is the IATA Airport Code. The list of codes is included in the template.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5 Authorizations

5.1 Introduction

This chapter provides AEGN Acquirers and Issuers the information necessary to provide the Authorization services required by the AEGN. It provides details on Authorization processes, services provided by the Network, requirements for requesting Authorizations and responding to Authorization Requests, as well as Authorization features such as Automated Address Verification. In addition, the AEGNS Stand-In service is detailed in this chapter.

5.2 Authorization Processing

This section defines the types of Authorizations available on the Network. For technical information regarding the processing of Authorizations, including message formats and descriptions and other related information, refer to the *Network Specifications - Authorization* manual.

5.2.1 Online Authorization Processing

5.2.1.1 Online Authorization Request

There are two (2) types of Online Authorization processes that an Acquirer may make available to an S/E:

- Submission of an Authorization Request via transmission from a POS terminal
- Resolution of a verbal Authorization Request through an Acquirer Authorization call center

Transactions under the Network Floor Limit do not require Authorization by an Issuer unless required by the Service Code (refer to Section 4.2.7.2, "Service Code Interrogation Requirements," on page 217), or in the case of an AEIPS Transaction where either an Offline Authorization or an Online Authorization will be performed (refer to Section 5.2.2, "Chip Card (Offline) Authorizations," on page 246), or when the Transaction occurs at any Customer Activated Terminal (CAT) (refer to Section 4.2.14, "Customer Activated Terminals," on page 224).

5.2.1.2 Online Authorization Response

An Authorization Response is provided by the Issuer, an Issuer Processor, or via Stand-In to the Acquirer who forwards the message on to the S/E to inform the S/E how to conclude the Transaction. A list of response messages and their descriptions can be found in Table 5-2, "POS Online Response Messages," on page 256.

5.2.1.3 Online Authorization Process

The following steps detail how the Online Authorization process works for a single Transaction processed by a POS device in which an Authorization Response is needed prior to completing the Transaction.

1. A Cardmember presents a Card, Mobile Device, or Account number to an S/E. If the Cardmember is present, the Card or Mobile Device must be presented.
2. The Card information is entered by swiping the Card in the POS device, manually keying the information into the device, inserting a Chip-Card into a Chip-Enabled Device, tapping/waving an Expresspay-enabled Chip Card or Mobile Device over an Expresspay-enabled POS Device, or tapping/waving a Mobile Device over a magnetic swipe POS device.
3. The POS device relays the Transaction data (including the Card number, purchase amount, and other information) to the Acquirer.
4. The Acquirer's system formats and transmits this data to the AEGN as an Authorization Request message.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5. When the AEGN receives this request, it identifies the Issuer by comparing the Card prefix with Network resident lookup tables and forwards the data to the Issuer's host system for Authorization.
6. The Issuer's Authorization decisioning system reviews the Transaction and Cardmember Information.
7. If the Authorization Request is approved, the Issuer's Authorization system returns an approval response message (indicated by an Action Code of "000" or "001"). If the Authorization Request is not approved, the Issuer may provide another response as described in Section 5.7.1, "POS Online Response Messages," on page 255.
8. The Network forwards the response to the Acquirer.
9. The Acquirer system relays the appropriate Action Code to the S/E's POS device.

5.2.2 Chip Card (Offline) Authorizations

In a Chip Card Transaction, the Chip-Enabled Device performs risk management checks that determine whether the device will send a request to the Chip Card to perform an Offline Authorization or whether the device will have to obtain an Online Authorization. If the Chip Card receives the request for Authorization, the Card uses parameters loaded by the Issuer during the Card personalization process to decide how to decision the Offline Authorization. Otherwise, the Chip-Enabled Device must obtain an Online Authorization.

Note: For Transactions within the EU/EEA & UK, all Transactions should go online for Authorization.

5.2.2.1 Chip Card (Offline) Authorization Process

The following steps detail how the Offline Authorization process works at a Chip-Enabled Device for a single Transaction.

1. A chip-enabled Card or Expresspay Mobile is inserted/tapped against a Chip-Enabled Device.
2. The Chip-Enabled Device collects information from the Chip Card or Expresspay Mobile.
3. The terminal interrogates the data and decides whether to do the following:
   - Send a request to the Card or Expresspay Mobile to obtain an Offline Authorization decision, or
   - Send a request to the Issuer to obtain an Online Authorization. See Section 5.2.1.3, "Online Authorization Process," on page 245 for information regarding the Online Authorization process.
4. The chip evaluates the data from the device based upon information loaded onto the Chip Card or Expresspay Mobile during the personalization process.
5. The chip responds to the terminal with a decline or approval decision and a cryptogram.

5.2.2.2 Chip Card Fallback

Fallback occurs when an AEIPS-enabled Chip Card POS device cannot initiate a Transaction by using the chip on the Card and must process the Transaction utilizing the magnetic stripe. Prior to initiating Fallback, an S/E must attempt to process the Authorization utilizing the chip multiple times. AEGNS recommends a total of three (3) attempts. After the final unsuccessful attempt, the AEIPS-enabled Chip Card POS device must prompt the S/E to revert to reading the magnetic stripe as the Fallback option.

When Fallback occurs, the S/E must follow standard S/E Card acceptance practices detailed in Section 4.2.7, "In-Person Charges," on page 216. Fallback may not take place under the following conditions:

- When the Card is blocked
- When the applications present are blocked
- When the Authorization has already been declined offline

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

When Fallback occurs, the Acquirer must indicate that the Transaction is a Fallback Transaction within the Point of Service Data Code in the POS Authorization Request (1100) message.

If the Transaction cannot be completed offline via the chip or online via a magnetic stripe-read, the Transaction may be completed by key entering the Transaction into the POS device subject to agreement with the local Acquirer.

An S/E processing a Fallback Transaction must obtain an Online Authorization from the Issuer. All Fallback Transactions have a Network Floor Limit of zero (0).

5.3 AEGNS Authorization Services

The following services are provided to Acquirers and Issuers conducting business on the Network. Some services provided by the Network are optional and are indicated as such in the sections below.

5.3.1 ATM and POS Authorization Message Routing

AEGN supports the authorization of both POS Transactions and ATM Transactions twenty-four (24) hours per day, seven (7) days per week. For all American Express licensed BINs, Acquirers must ensure that all Authorization Request messages (except for On-Us, or U.S. Multi-Network Debit Card or U.S. Multi-Network Prepaid Card Transactions) are routed to the AEGN. The AEGN is solely responsible for routing all Online Authorization Requests from the Acquirer to the appropriate Issuer, based on the Issuer's licensed BIN, and returning the Authorization Response from the Issuer to the appropriate Acquirer. The message routing is accomplished by identifying the transmitted American Express Bank Identification Number (BIN) and referencing this number in the AEGNS routing tables.

An Issuer or Acquirer may designate a third-party processor to provide its Authorization service. Participants must ensure that Authorized Processors comply with all Authorization message routing requirements of this section.

5.3.2 Activity Logging

All authorization-related messages, either received by or transmitted from the AEGN, are recorded in log files. The length of time these logs are maintained is determined in accordance with AEGNS Chargeback policies (see the "Chargeback Policies Overview" chapter beginning on page 280), Fair Credit Billing Act (FCBA) regulations in the U.S., and any international laws pertaining to Chargebacks.

5.3.2.1 Authorization Log Records

Various log records are generated within the Acquirer, Issuer, and AEGN application environments for use in performance reporting, research, and Settlement file validation. These records contain application environment data and Transaction-specific data (e.g., Authorization decisioning results and time stamps).

The AEGN log records are created from Acquirer and Issuer messages as they flow through the Network, as well as any AEGN actioning performed. As a result, the AEGN log records contain detailed Authorization message information.

In instances for which log records or log record data are required to resolve questions, issues, or problems related to specific Authorization transactions, the AEGN log record, and associated data will take precedence over all other provided information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.3.3 Prepaid Card Authorization Processing

AEGNS supports the following Authorization-related services for Prepaid Cards:

- Prepaid Card Partial Authorization with Balance Return (with or without Balance Return) allows S/Es to obtain an Authorization for the remaining balance on a Prepaid Card, that is less than the requested purchase amount. The Cardmember, then, has the option to pay for the outstanding amount of the purchase by other means.
- Prepaid Card Authorization with Balance Return allows S/Es to obtain the remaining balance on a Prepaid Card when an Authorization Request is declined as a result of insufficient funds to cover the full amount of a purchase. The S/E then has the option of resubmitting a Partial Authorization Request for an amount less than or equal to the Prepaid Card balance.
- Prepaid Card Balance Inquiry allows S/Es to obtain the remaining balance on a Prepaid Card either as part of the Prepaid Card Partial Authorization with Balance Return and the Prepaid Card Authorization with Balance Return functionality, or as a stand-alone request submitted to the Issuer.

Acquirers in the countries listed in Table 5-1, "Designated Acquirer Countries to Support Prepaid Card Authorization-Related Services," on page 248 must be certified for and support the Prepaid Card Authorization-related services described above. Acquirers should work with S/Es wishing to use Prepaid Card Partial Authorization with Balance Return and/or Prepaid Card Authorization with Balance Return to ensure their POS devices are enabled to support this functionality.

Issuers of Prepaid Cards certified to support this functionality are required to respond, as described in Section 3.2.5.4, "Prepaid Card Functionality," on page 131, by returning the appropriate Authorization Response. Refer to the Network Specifications manuals for additional technical information regarding the Prepaid Card functionality.

Table 5-1 Designated Acquirer Countries to Support Prepaid Card Authorization-Related Services

Australia	Canada	France
Germany	India	Italy
Mexico	Portugal	Puerto Rico
Singapore	South Africa	Spain
United Kingdom	United States	

5.3.4 Authorization Reversals

Authorization Reversal is a message that can be system-generated or initiated by S/Es.

System-generated Authorization Reversals are initiated when either the Acquirer or the Network receives an approval from the Issuer but was unable to complete the Transaction. System-generated Authorization Reversals are generally due to late arriving approvals or problems after receipt of the approval.

S/E initiated Authorization Reversals allow S/Es to reverse a previously authorized amount. Acquirers and Issuers can identify a reversal initiated by an S/E by a unique Processing Code in the POS Authorization Reversal Advice (1420) and the POS Authorization Reversal Advice Response (1430) messages. Refer to the *Network Specifications - Authorization* manual and *Codes Reference Guide* for additional information.

The reversed Transaction must not be submitted to the Network for Settlement.

Upon receipt of a POS Authorization Reversal Advice (1420) message, either system-generated or S/E initiated, Issuers must use all relevant means to locate the original Transaction and release the funds held on the Cardmember account.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The Acquirer must accept the POS Authorization Reversal Advice (1420) message from the S/E and forward it to the Network. The Acquirer must not submit a previously reversed Transaction to the Network for payment. If the Acquirer submits the Transaction after the reversal was performed, the Network will consider this Transaction not authorized.

S/Es must initiate POS Authorization Reversals within the timeframes specified below or as soon as possible after the initial Authorization and never after the Transaction has been submitted for Settlement:

- Twenty-four (24) hours from the original Authorization Request for Card Present environment
- Seventy-two (72) hours from the original Authorization Request for Card Not Present environment
- For estimated Charges at lodging, cruise line, and car rental S/Es, POS Authorization Reversals should be made within twenty-four (24) hours of the check out, end of the cruise, or car rental.

5.3.5 Authorization on Credit

Authorization on Credit is functionality that allows Acquirers to send refund-specific Authorization Request messages to Issuers.

An Authorization on Credit may allow Issuers to display a pending credit to a Cardmember. It is recommended that Acquirers enable the Authorization on Credit functionality to provide a better Cardmember experience during refunds.

It also is recommended that Issuers enable the Authorization on Credit functionality, and display associated information pertaining to the pending credits on Cardmember-facing applications.

Issuers may decision an Authorization on Credit request according to their internal metrics, which may result in a decline. An S/E utilizing the Authorization must:

- Send a refund Authorization request for an amount that is equal or less than the original Transaction amount
- Provide the Cardmember a receipt for the refund initiated with an Authorization on Credit

5.3.6 Authorization Adjustments

Authorization Adjustments allow Acquirers and their S/Es to adjust the Transaction amount when the final Transaction amount is lower than the amount previously authorized. This allows the Issuer to release any hold on available funds on a Cardmember's account for excess amounts authorized without waiting to receive the Presentment message containing the final Transaction amount.

Upon receipt of a POS Authorization Adjustment Financial Advice (1220) message, certified Issuers must use all relevant means to locate the original POS Authorization Request (1100) message and release any excess funds held on the Cardmember's account.

Certified Acquirers must accept POS Authorization Adjustment Financial Advice (1220) messages from S/Es and forward them to the Network.

Once an Acquirer has sent an Authorization Adjustment, they must not submit a Presentment for the Transaction amount authorized in the original POS Authorization Request (1100) message. If the Transaction is presented for the original amount, the Network will consider the difference between the original authorized amount and the final Transaction amount not authorized.

S/Es must initiate Authorization Adjustments within the timeframes specified below, or as soon as possible after the initial Authorization and never after the Transaction has been submitted for Settlement:

- Twenty-four (24) hours from the original Authorization Request for Card Present environment
- Seventy-two (72) hours from the original Authorization Request for Card Not Present environment
- For estimated Charges at lodging, cruise line, and car rental S/Es, Authorization Adjustment should be made within twenty-four (24) hours of the check out, end of the cruise, or car rental.

Refer to the Network Specifications manuals and *Codes Reference Guide* for additional information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.3.7 Address Verification

Address Verification is an optional feature requiring Certification on the Network. AEGNS supports two (2) methods of Address Verification for Acquirers:

- Automated Address Verification (AAV)
- Name and Address Verification (NAV) (U.S. and Canada only)

Both methods will allow an S/E to obtain the verification of Cardmember address information as an added measure of protection against fraud. See Section 5.10.1, "Address Verification," on page 261 for more information.

5.3.8 Authorizations Support

AEGNS provides a Help Desk staffed twenty-four (24) hours per day, seven (7) days per week to assist Participants with all Authorization issues.

5.3.9 BIN Blocking

AEGNS provides Issuers the ability to block Authorization activity on inactive BINs as a means to mitigate fraud. Following the placement of a BIN block, Global Network Services Authorization System (GNSAS) will generate an "Invalid Account" or "Deny" Authorization Response on any Authorization Requests on a Card Account number within the blocked BIN or sub-range. Blocking a BIN will provide the Card Issuer protection from liability for fraudulent Transactions at or above the Network Floor Limit on the blocked BIN. Issuers will remain liable for Transactions under the Network Floor Limit.



Issuers may request BIN Blocking through their AEGNS representative.

5.3.10 Currency Conversion

The Authorization amount is forwarded to the Issuer in the Issuer's requested currency. The Issuer may request the Authorization amount of the Transaction be represented in the Issuer's Settlement currency. The amount the Issuer receives in the Authorization Request may not be the same as the Transaction amount in the First Presentment as there could be a difference due to the conversion of the amount from the Acquirer currency to the Issuer currency. See Section 6.4.2.3, "Foreign Exchange Conversion Rate Establishment," on page 274.

5.3.11 Deferred Payment Plan (DPP)

The Deferred Payment Plan (DPP) is an optional feature requiring Certification that allows Cardmembers to pay for products and services in installments. The Service can be initiated by the Issuer or the Acquirer via additional information supported in the Authorization Request. For more information see Section 5.10.3, "Deferred Payment Plan (DPP)," on page 263.

5.3.12 Fraud and Risk Scoring Service

To improve the POS credit Authorization process and detection of fraudulent charging, AEGNS offers Dynamic Fraud Management Network Services (DFMNS). Refer to Section 8.10.3.1.2, "Dynamic Fraud Management Network Services," on page 394 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.3.13 Cash Disbursements

Cash Disbursements are manual disbursements of cash to Cardmembers by a Cash Disbursement Provider. Cash Disbursement Transactions are identified by Merchant Category Code (MCC) 6010 - Financial Institutions, Manual Cash Disbursement. Additional Card acceptance requirements for Authorization must be followed at the Point of Sale. Refer to Section 4.5, "Cash Disbursements," on page 240 for additional information. All Card Issuers are required to ensure that they are able to process Cash Disbursement Transactions.

5.3.14 Participant Reporting

Authorization reports are available to Participants. Examples of these reports are available in the *Network Specifications - Instructions* manual.

5.3.15 Stand-In Authorization Service

When Network connectivity is unavailable between the Network and the Issuer (or the Issuer's Processor), the Network must Stand-In to provide the Acquirer with a response to the Authorization Request. The Stand-In Authorization service is an optional service that allows an Issuer to select Transaction criteria by which the Network will stand in on behalf of the Issuer and Approve a Transaction if the Transaction meets the Issuer's pre-defined criteria. The Network records all Stand-In Authorizations and provides the Issuer (or the Issuer's Processor) with a record of each Stand-In Authorization decision once the Issuer (or Issuer's Processor) has come back online. Should connectivity between the Network and the Issuer (or Issuer's Processor) be unavailable and the Issuer has not elected to utilize the AEGN Stand-In Authorization service, all Authorizations will be declined by the Network. See Section 5.8, "Stand-In Processes," on page 256 for more information regarding the Stand-In Process.

5.3.16 System Outage Resolution

System Outages are interruptions in service that prevent connectivity between AEGNS and Participants. The Participant must cooperate with AEGNS to resolve the problem.

AEGN will initiate Stand-In processing for Authorization Requests on behalf of the Issuer when no alternate routing path can be established.

5.4 Issuer Authorization Requirements

AEGNS Issuing Participants, or AEGNS authorized Issuer processors providing Authorization services on behalf of the Issuing Participant, must provide Authorization services that comply with the Network policy as set forth in this edition of the *Business and Operational Policies* manual. An Authorized Processor's failure to perform shall not relieve that Participant of its obligations under its Participant Agreement.

In addition to accepting responsibility for Transactions under the Network Floor Limit, the Issuer accepts responsibility and liability for all Transactions within its licensed BIN range that are Authorized as follows:

- The Issuer Authorizes the Transaction, or
- The Issuer's Authorized Processor Authorizes the Transaction, or
- The Authorization is performed on behalf of the Issuer in Stand-In, provided that the Stand-In parameters submitted by the Issuer for Host Stand-In (or remote system parameters for Remote Stand-In) are used correctly by the Network.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.4.1 Hours of Operation

The Issuer is responsible for responding to all Authorization Requests twenty-four (24) hours per day, seven (7) days per week in accordance with the policies set forth in this edition of the *Business and Operational Policies* manual. The Issuer may fulfill this requirement through one (1) or more of the following means:

- Direct electronic Authorization by the Issuer's Authorization system
- Indirectly, through the use of an Authorized Processor
- Indirectly, through utilization of the AEGN Stand-In service

5.4.2 Notification of Scheduled Outages

Participants must call the AEGNS Help Desk at +1-602-794-9903 to notify the Network of a scheduled outage. AEGNS requests thirty (30) days advance notice from Participants scheduling an outage.

To invoke specific scheduled Stand-In parameters, an Issuer must certify to send an ISO 1804 message to the AEGN and to receive an ISO 1814 network management response message from the AEGN. The scheduling process is as follows:

- The Issuer contacts the AEGNS Help Desk to schedule an outage preferably thirty (30) days in advance.
- At the time of the outage, the Issuer must send an 1804 'sign off' message to the Network to invoke Stand-In. The Network will respond with an 1814 acknowledgment message.
- Once connectivity has been re-established, the Issuer must send an 1804 'sign-on' message to allow Authorizations to be routed to the Issuer. The Network will respond with an 1814 acknowledgment message.

The Network maintains an Authorizations log that is stored and forwarded to the Issuer's system when the Issuer returns to active status.

The AEGN will not Stand-In for ATM Transactions.

5.4.3 Notification of Unscheduled Outages

An Issuer, upon experiencing an unscheduled outage, must immediately notify the AEGNS Help Desk**.** The appropriate support personnel within the Network will work with the Issuer to restore service.

5.4.4 Issuer Authorization Response Standards

Issuers are required to respond to Authorization Requests within specific timeframes to ensure the authorization process is completed in a timely manner. The timeframes are as follows:

- For POS Authorizations, the Network must receive the Authorization Response within eight (8) seconds, inclusive of transmission time, after the Authorization Request was sent to the Issuer or Stand-In will be invoked.
- For ATM Authorizations, the Network must receive the Authorization Response within ten (10) seconds, inclusive of transmission time, after the Authorization Request was sent to the Issuer or a "No Response" message will be sent back to the Acquirer.

For more information regarding Authorization Response timeframes required for POS and ATM Transactions, see Section 5.7, "Authorization Responses," on page 255.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.5 Acquirer Authorization Requirements

Acquirers operating on the AEGN are responsible for enabling S/Es to obtain Authorization for POS and ATM Transactions. An Acquirer must also ensure that S/Es comply with Network policy as set forth in this edition of the *Business and Operational Policies* manual.

5.5.1 Hours of Operation

Acquirers are responsible for routing Authorization Requests from S/Es twenty-four (24) hours per day, seven (7) days per week. This requirement may be fulfilled by Acquirers through one (1) or more of the following means:

- Direct interface to AEGN, or
- Indirectly, through the use of an Authorized Processor.

5.5.2 Authorization Systems for S/Es

Acquirers must supply their S/Es the means of obtaining Authorization for Transactions. The Acquirer is responsible for providing Authorization services for the S/E (or the S/E's processor) and must submit, and must require the S/E's processor to submit, the Authorization Request messages directly and solely to the Network.

In the case of On-Us Transactions, the Authorization Request will not be submitted to the Network. Where manual card imprinters are to be used as backup for failure of a primary electronic method, Acquirers must support requests for Authorizations through an Authorization call center and must follow the requirements described in Section 5.6.3, "Voice Authorization," on page 255.

Note: AEGNS prohibits the retention of track data by Acquirers or their S/Es following the authorization of a Transaction. See Section 2.4, "Participant Data Security Policy," on page 38.

5.5.3 Cancelled S/E Policy

Acquirers are responsible for ensuring that Authorization Requests submitted by cancelled S/Es are rejected by the Acquirer's Authorization system. These Authorization Request messages should not be sent to AEGNS. Acquirers that do not comply may be subject to non-compliance fees.

5.5.4 System Outage Notification

In the event that the AEGN fails to respond to an Authorization Request, the Acquirer should immediately notify the AEGNS technical Help Desk. A representative at AEGNS will escalate the issue to the appropriate support personnel within the Network to restore service.

5.6 POS Authorization Requests

A POS Authorization Request is an attempt by an S/E to obtain an Authorization from the Issuer of the Card to complete a sale. There are two (2) distinct environments in which an Authorization may be requested.

- Card Present - Any Transaction in which the Cardmember and Card are present at the Point of Sale (e.g., a retail store).
- Card Not Present - Any Transaction in which the Cardmember and Card are not present at the Point of Sale (e.g., Internet, mail order).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.6.1 Card Present Authorization Requests

For Card Present Authorizations, when the Cardmember and Card or Mobile Device are present at the Point of Sale, an S/E must obtain an Authorization unless the Transaction is under the Floor Limit or the Service Code does not require an Authorization.

5.6.1.1 Magnetic Stripe Authorization

Magnetic stripe Authorization occurs when the Card is swiped through a POS device and the track data included on the magnetic stripe is forwarded to the Issuer in the Authorization message. The track data must be sent exactly as captured.

5.6.1.2 Key-Entered Authorization

Key-entered Authorization occurs when the Merchant keys the Account number and Expiration Date from the Card into the POS device. An Imprint of the Card is required when an Authorization is key entered except when the Transaction meets any of the conditions for exclusion for "ISO 4527 - Missing Imprint" on page 326.

5.6.1.3 AEIPS Authorization

AEIPS Authorization occurs when a Chip Card with an AEIPS application is used to initiate a Transaction at an AEIPS-enabled POS device, and the Chip Card Transaction is performed as defined in the AEIPS Chip Card Specifications and *AEIPS Terminal Technical Manual*.

5.6.1.4 Expresspay Authorization

Expresspay Authorization occurs when a Chip Card or Mobile Device with an Expresspay Application is used to initiate a Transaction at an Expresspay-enabled POS Device, and the Chip Card or Expresspay Mobile Transaction is performed as defined in the following:

- Expresspay Card Specifications
- Expresspay Mobile Specifications
- *Expresspay Terminal Specifications*
- Live Terminal Parameters AEIPS & Expresspay Guide

5.6.2 Card Not Present Authorization Requests

For Card Not Present Authorizations, when the Cardmember is not present at the Point of Sale, an S/E must always perform an Online Authorization.

5.6.2.1 Key-Entered Authorization

Key-entered Authorization occurs when transaction data is keyed into a POS device when the Cardmember and the Card are not present (e.g., Internet, mail order) at the Point of Sale.

5.6.2.2 Card Not Present Recurring Billing Authorizations

S/Es must obtain an Authorization for each Transaction in a Recurring Billing series. After the initial transaction has been Authorized, the S/E must also obtain an Authorization for any subsequent transactions. If the Cardmember is not present, then the S/E must submit these transactions as Card Not Present Transactions. See Section 4.2.15, "Recurring Billing," on page 225 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.6.3 Voice Authorization

S/Es lacking electronic Authorization terminals or whose POS terminals are temporarily down must prepare the ROC manually or use a Preprinted ROC and include an Imprint of the Card. An S/E must obtain a valid Authorization by contacting the Acquirer's Authorization call center by telephone when:

- The S/E lacks an electronic Authorization terminal and the Transaction amount is above the Network Floor Limit, or
- The POS terminal is unable to send or receive a POS Authorization Request (1100) message and a POS Authorization Response (1110) message, respectively, and the Transaction is above the Network Floor Limit.

When the S/E calls the Acquirer's Authorization call center for an Authorization, the call will be answered by either a Voice Response Unit (VRU) or by Authorization call center personnel. The S/E will be asked to provide the S/E number and the following Card details:

- Account number
- Transaction amount
- Expiration Date
- Printed Card Security Code (PCSC) or One-Time Password (OTP)

5.7 Authorization Responses

An Issuer's Authorization system must be capable of responding to Authorization Request messages with, at a minimum, "Approve" (Action Code 000 or 001) or "Deny." A complete list of the Authorization Response Action Codes designed to minimize financial exposure, reduce fraud, and to recover stolen or lost Cards are available to Issuers and can be found in the *Codes Reference Guide.*

5.7.1 POS Online Response Messages

Issuers must respond to each POS Authorization Request (1100) message within eight (8) seconds from the time the Network transmits the message to the Issuer. The eight (8) seconds is inclusive of the time required to transmit the Authorization Request to the Issuer and the Authorization Response back to the Network. The elapsed response time is measured from the point at which the Network sends the Authorization Request to the Issuer and stops when the Network receives a response to the request from the Issuer.

Upon receipt of the POS Authorization Request (1100) message, the Issuer (or its designee) will log the request and arrive at a response based upon a set of decision criteria. Each individual Issuer, according to its own business requirements and assessment of risk, determines these criteria. The Issuer system must respond with a disposition for the Authorization Request as listed in Table 5-2, "POS Online Response Messages," on page 256. In some instances, either the Acquirer system or the POS device may be programmed to convert Approve with ID, Pick Up, and Please Call responses into a Deny response. The AEGN has no way of informing the Issuer when this conversion occurs.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

If AEGNS does not receive a response from the Issuer within eight (8) seconds, the Authorization will be routed to Stand-In for decisioning. The Issuer will receive a POS Authorization Advice (1120) message notifying the Issuer of the disposition of the Authorization Request.

Table 5-2 POS Online Response Messages

Issuer Response	Message Relayed	Action Taken
Transaction Approved	"Approve"	The Transaction is Authorized as requested and details are recorded in the Issuer Authorization system to include the Action Code and Approval Code. The Authorization Response is returned to the Network. An "Approval" is indicated by an Action Code of 000 in the POS Authorization Response (1110) message.
Transaction Approved with Cardmember ID	"Approve with ID"	The Transaction is Authorized as requested and details are recorded in the Issuer Authorization system along with the Action Code and Approval Code. As an additional step in the Authorization process, the S/E must establish positive Cardmember identification (photo ID). See the "S/E and ATM Standards" chapter for information regarding acceptable forms of identification. An "Approval with ID" is indicated by an Action Code of 001 in the POS Authorization Response (1110) message.
Transaction Denied	"Deny"	The Issuer refuses to Authorize the Transaction and an Action Code indicating the Authorization has been declined is returned to the Network. The S/E must decline the sale based upon this response or may request a different form of payment.
Transaction Denied, Pick Up Card	"Pick-Up"	The Issuer requests that a Card be captured at the S/E. If the S/E's POS system displays a Pick Up Card response, the S/E is not obligated to perform this action if it is against the S/E's company policy or deemed unsafe by the S/E. The AEGN and American Express Entities have no responsibility or liability for Cards that are or are not picked up. See Section 4.3.3, "Card Capture," on page 239.
Error detected (several Action Codes are available)		Refer to the *Codes Reference Guide*.

5.8 Stand-In Processes

The Stand-In Authorization service is provided to all Issuers on the AEGN. An Issuer may provide Stand-In criteria for AEGN Stand-In Tables that allow the Network to Stand-In and Approve Authorizations when an Issuer (or the Issuer's Processor) is unable to respond to an Authorization Request due to scheduled or unscheduled downtime. If an Issuer chooses not to provide Stand-In criteria to the Network, the AEGN reserves the right to decline all Transactions that default to Stand-In. See the following sections for Stand-In criteria forms:

- "Exhibit 8. Single Charge and VIP Stand-In Parameter Table" on page 464
- "Exhibit 9. Velocity-Based Stand-In Parameter Table" on page 467

For more information on response times required by Issuers, see Section 5.7.1, "POS Online Response Messages," on page 255.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

An Authorization Response may not be received within timeframes by the Network for the following reasons:

- The Issuer's or its designee's system responds too slowly to an Authorization Request
- The Issuer's or its designee's system suffers unexpected failure
- Communications loss prevents the Issuer or its designee from receiving or responding to an Authorization Request
- Regularly scheduled downtime of the Issuer's or its designee's Authorization system.

There are two (2) types of Stand-In Authorization Service:

- Host Stand-In
- Remote Stand-In

5.8.1 Host Stand-In

Host Stand-In is a Network service that provides Authorization services on behalf of the Issuer, based on Issuer parameters, when the Issuer is unavailable to the host.

Host Stand-In can occur as scheduled or unscheduled and unique Authorization parameters can be set based upon whether the outage is scheduled or not.

5.8.1.1 Types of Host Stand-In Tables

The following Stand-In Tables are available to Participants in Host Stand-In:

- Single Charge
- Velocity-Based
- VIP

All incoming Authorizations routed to Host Stand-In will be checked against all three (3) tables. If an Authorization fails to meet the table criteria on any one (1) table the Authorization Request will be declined.

5.8.1.2 Unsupported Functions and Features

The following are not supported by the Host Stand-In Authorization service:

- ATM Authorization Requests
- Issuer Based Deferred Payment Plan (DPP) Authorization Requests (see Section 5.10.3, "Deferred Payment Plan (DPP)," on page 263)
- Automated Address Verification (AAV)
- American Express Verification Value (AEVV) validation where the Issuer generated the AEVV
- Prepaid Card Partial Authorization with Balance Return
- Prepaid Card Balance Inquiry and Prepaid Card Balance Return
- OTP
- Online PIN Transactions

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.8.1.3 Mandatory Host Stand-In 5-Digit Card Security Code (5CSC) Requirements

In an effort to minimize fraud on the AEGN during Stand-In, the following requirements for the Host Stand-In Tables have been mandated by the Network:

- All AEGNS Issuers must exchange Card Security Code (CSC) keys with the AEGN.
- All AEGNS Issuers must have CSC keys loaded to the AEGN Host Stand-In Tables.
- All AEGNS Issuers must set the 5CSC validation indicator in the Velocity Stand-In Tables to "Y" for Card Present industry segments to allow the Network to validate the 5CSC value during the Stand-In Authorization process. See the *Codes Reference Guide* for a complete list of valid Merchant Category Codes (MCCs) and their associated industry segments.

5.8.1.4 Optional Host Stand-In Features

An Issuer may request that AEGNS validate the 3-digit Card Security Code (3CSC) and/or 4-digit Card Security Code (4CSC) during Host Stand-In. The Network will only validate the 3CSC/4CSC when a Transaction is key entered and no track data has been submitted in the POS Authorization Request (1100) message. The Network will use the PCSC in Stand-In as follows:

- If the PCSC cannot be validated by the Network because the Participant CSC key could not be obtained due to a technical error, the Authorization Request will be approved, provided no other decline reason exists.
- If the PCSC validation result by the Network is invalid, the Authorization Request will be denied.

The Host Stand-In Authorization Service will validate the Integrated Circuit Card Security Code (iCSC) value during Stand-In using the Encryption keys supplied by the Issuer.

A single CSC key is used to generate the 3CSC, 4CSC, 5CSC, and iCSC values. Once the CSC key has been provided to the Network, the CSC values can be validated in Host Stand-In by the Network.

Note: 4-digit Data Batch Code (4DBC) and OTP validation are not supported in Stand-In. If an Issuer has any Cards with 4DBC in circulation or has provided an OTP to their Cardmember, the Issuer should choose not to have the Network validate 4CSC in Stand-In, as Authorization Requests submitted with a 4DBC or OTP will be declined due to a 4CSC mismatch.

5.8.2 Remote Stand-In

If the AEGN Host Stand-In service is unavailable, the Network will switch to the Remote Stand-In service.

Remote Stand-In is a Network service that provides Authorization services to the Issuer via a remote system, based on Issuer parameters, when the AEGN host system is unavailable. Remote Stand-In service is available to all Network Issuers.

5.8.2.1 Types of Remote Stand-In Tables

The following Stand-In Tables are available to Participants in Remote Stand-In:

- Single Charge
- VIP

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.8.2.2 Unsupported Functions and Features

The following are excluded from the Remote Stand-In Authorization Service:

- ATM Authorization Requests
- All Deferred Payment Plan (DPP) Authorization Requests (see Section 5.10.3, "Deferred Payment Plan (DPP)," on page 263)
- All CSC validation
- Velocity Stand-In Tables
- Automated Address Verification (AAV)
- AEVV validation
- Prepaid Card Partial Authorization with Balance Return
- Prepaid Card Balance Inquiry and Prepaid Card Balance Return
- OTP
- Online PIN Transactions

5.8.3 Scheduled Stand-In

An Issuer may invoke Stand-In parameters by submitting a Network Management Request (1804) message informing the Network that the Issuer (or Issuer's Processor) will be unavailable. The Issuer will receive a Network Management Response (1814) message confirming the notification.

To end scheduled Stand-In, the Issuer must send a Network Management Request (1804) message to the Network Authorization system. Refer to the *Network Specifications - Authorization* manual for message layouts. Failure to receive the response will cause the AEGN to assume that the Issuer system is still incapable of Transaction Authorization and the Network will continue to perform Stand-In according to the Issuer specified parameters and resident file specifications.

5.8.4 Unscheduled Stand-In

Stand-In may be invoked due to unscheduled interruptions in connectivity between the Participant and AEGN. Unscheduled Stand-In Authorization service can occur because:

- The Issuer's or its designee's system does not respond to Authorization Requests and/or referrals within the eight (8) second timeframe. See Section 5.7, "Authorization Responses," on page 255.
- The Issuer or its designee's experiences unexpected system failure.
- Communications loss prevents the Issuer or its designee from responding to Authorization Requests.

5.8.5 Stand-In Authorization Parameters

The AEGN Stand-In Authorization Service is provided seven (7) days per week, twenty-four (24) hours per day. Under normal processing, all Authorization Requests will be routed to the Issuer (or the Issuer's Processor). When an Issuer invokes Scheduled Stand-In by submitting a Network Management Request (1804) message, the data will include a Stand-in number that is an index to the Stand-In parameter table indicating to the Network which parameters should be utilized for the Stand-In period. Authorization decisions during these scheduled periods will be made based upon Issuer-set criteria specifically designated for scheduled Stand-In. At all other times, non-response or late response from the Issuer's (or the Issuer Processor's) Authorization system will be handled using a set of unscheduled Stand-In parameters.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.8.6 Stand-In Table

If the Issuer is unable to fulfill an Authorization Request due to scheduled or unscheduled downtime, the Network will access the appropriate Stand-In parameter table to determine which Authorization Response to send. All Stand-In limits will be maintained in U.S. Dollars and the Transaction Amount in the Authorization Request will be converted to U.S. Dollars. See "Exhibit 8. Single Charge and VIP Stand-In Parameter Table" on page 464 and "Exhibit 9. Velocity-Based Stand-In Parameter Table" on page 467 to access the forms used to provide the Stand-In parameters to the Network.

5.8.7 Exception File

The Exception File and the Batch Exception Update Request (9344) messages contain negative Recurring Billing cancellation and VIP status Account numbers. The files allow the Issuer to specify special responses based upon a specific Account number.

During Stand-In:

- Accounts with a "negative" status will be declined due to fraudulent activity or credit reasons.
- Accounts that have been given special "VIP" status may have different Stand-In criteria than that specified in the Single Charge tables.

Issuers participating in the Recurring Billing Cancellation Service may utilize the Exception File and Batch Exception Update Request (9344) message to provide Card Account numbers, and other information, which will be used by AEGNS to block cancelled Recurring Billing Transactions. Refer to Section 1.6.13, "Recurring Billing Cancellation Service," on page 9 and Section 2.10.9, "Recurring Billing Cancellation Service Requirements," on page 117 for more information.

Expresspay Issuers must also provide a Card Type Indicator to the Exception File and the Batch Exception Update Request (9344) messages for Expresspay-enabled Card/device account numbers.

For more information, refer to the Network Specifications manuals.

5.8.8 Network Authorization Decision Making Process During Issuer Stand-In

When the Network must decision an Authorization Request due to an Issuer's (or an Issuer Processor's) inability to decision the Authorization Request, the Network will initiate the following process:

- If there is an Account number match against the Exception File, the Authorization decision will be based upon whether the Account number matched for negative or VIP status.
- If there is no Account number match against the Exception File, the amount of the Charge will be checked against the Stand-in parameter table number specified by the Issuer. If the Transaction amount is over the specified limit, the Charge will be declined. If the Transaction amount is below the specified limit, the Charge will be authorized with an Approval Code assigned by the Network. The Issuer accepts liability and responsibility for all Transactions that are authorized pursuant to this section.

The Remote Stand-In service will only utilize the Single Charge and VIP Stand-In Tables.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.8.9 Store and Forward Process

Transactions that have been Authorized during AEGNS Stand-In processing will be forwarded to the Issuer once the Issuer system returns online (after scheduled or unscheduled interruption). The Issuer must send an 1804 message (Network Management Request) to the AEGN to end scheduled Stand-In. The AEGN will send the Issuer a POS Authorization Advice (1120) message and will expect a POS Authorization Advice Response (1130) message in return. Failure to receive the response will cause the AEGN to assume that the Issuer system is still incapable of Transaction Authorization and the Network will continue to perform Stand-In according to the Issuer specified parameters and resident file specifications. For more information regarding the message layout for the Network Management Request (1804) message and POS Authorization Advice Response (1130) message, refer to the *Network Specifications - Authorization* manual.

5.8.10 Stand-In Processing Legal Disclaimer

Stand-In Authorization provided by the Network on behalf of an Issuer will be binding on an Issuer to the same extent as an Authorization provided by an Issuer directly. The AEGN or American Express Entities have no liability for Authorization of Transactions via Stand-In Authorization performed on behalf of Issuers provided, that Stand-In parameters submitted by the Issuer are used correctly. In no event will the AEGN or American Express Entities be liable for incidental, special, indirect, exemplary, consequential, speculative, or punitive damages.

5.9 Network Floor Limits

Network Floor Limits allow an S/E to process a sale without obtaining an Authorization. Each S/E type has a monetary amount assigned to it by country for a single Transaction, at or above which the S/E must obtain an Authorization before completing the Transaction. This process reduces the time needed to process an Authorization Request and assists S/Es who cannot always dial out for an Online Authorization due to poor telecommunication access. "Exhibit 17. Floor Limit Table" on page 485 lists the Network Floor Limits by country and S/E category, as well as by Region and alphabetically. Additionally, "Exhibit 17. Floor Limit Table" on page 485 includes a category for "All Other Markets" for countries not listed.

Note: Network Floor Limits do not apply to Expresspay Transactions.

In the case of an AEIPS Card Transaction, an Offline Authorization or Online Authorization may be performed below the Network Floor Limit.

5.9.1 Chip Fallback Floor Limits

An S/E processing a Fallback Transaction must obtain an Online Authorization from the Issuer. All Fallback Transactions have a Floor Limit of zero (0). See Section 5.2.2.2, "Chip Card Fallback," on page 246 for more information.

5.10 Authorization Features

In addition to standard Authorization Processing, AEGNS offers many services and features that Participants may utilize to enhance processing on the Network.

5.10.1 Address Verification

The AEGN provides two (2) features that allow S/Es to verify Cardmember address information. The two (2) features are:

- Automated Address Verification (AAV)
- Name and Address Verification Program (NAV) (U.S. and Canada only)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.10.1.1 Automated Address Verification

Automated Address Verification (AAV) is a Network feature requiring Certification that enables Acquirers to reduce fraud losses by matching the Cardmember's address information to the shipping address on electronically transmitted Authorization Requests. An S/E may submit a request for AAV validation in two (2) ways:

- The AAV request may be submitted with a standard POS Authorization Request (1100) message, or
- The AAV request may be submitted as an AAV "validation only" request. For this type of request, the Issuer should return an AAV validation response with a "000" (Approved) Action Code and no Approval Code.

Issuers certified for AAV are required to match the first line of the Cardmember's address information and/or postal code on the POS Authorization Request (1100) message with the Issuer's Cardmember Account information on file. If an Issuer is not certified to receive AAV data, a response will be sent to the S/E indicating that the Issuer is not participating in the AAV program.

Certification for AAV is mandated for all U.S. and Canadian Issuers. For information regarding the technical requirements for AAV, refer to the *Network Specifications - Authorization* manual.

For details regarding the Chargeback liability shift for Issuers, refer to Excluded Transactions under "ISO 4540 - Card Not Present" on page 330.

AAV is not supported by the Stand-In Authorization Service.

5.10.1.2 Name and Address Verification (NAV) Program

The Name and Address Verification (NAV) Program is only available to S/Es in the U.S. and Canada. The program allows an S/E to contact a U.S. or Canadian Issuer (via the S/E's Acquirer) to confirm Cardmember information during the Authorization process. Issuer validation of the Cardmember information does not shift Chargeback liability in the event that the Cardmember disputes the First Presentment as fraudulent at a later date.

5.10.1.2.1 S/E Requirements

The NAV Program is optional for U.S. and Canadian S/Es. An S/E may call its Acquirer to facilitate a transfer to an Issuer call center to validate that the Cardmember information provided by the Cardmember during an Authorization is correct.

During an NAV call to the Issuer, an S/E may only present the following information for validation:

- Cardmember name
- Street address
- ZIP code/Postal Code
- Telephone number

5.10.1.2.2 Issuer Requirements

All U.S. and Canadian Issuers are required to provide access to a call center with a toll-free number to allow U.S. and Canadian S/Es to contact the Issuer (via the S/E's Acquirer) and confirm Cardmember information from an Issuer representative.

During an NAV call, the Issuer is only required to confirm the following information:

- Cardmember name
- Street address
- ZIP code/Postal code
- Telephone number

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.10.2 Cardholder Verification Methods

AEGNS supports the following Cardholder Verification Methods (CVMs) as provided in the following table:

Table 5-3 Cardholder Verification Methods

CVM	Transaction Type Supported
Signature[1]	All except MPQR
Online PIN[2,3,4]	AEIPS, Expresspay, Digital Wallet Programs, MPQR
Offline PIN	AEIPS
Mobile Passcode	Expresspay Mobile, CPQR, MPQR
Consumer Device Cardholder Verification Method (CDCVM)	Digital Wallet Programs, CPQR, MPQR

1. Obtaining Cardmember signature on Card Present Transactions is optional to complete a ROC, and at the discretion of the S/E, unless required by applicable law.
2. Online PIN is a feature that requires Certification by the Network. Online PIN is an optional feature for Issuers and a conditional feature for Acquirers. Refer to Section 4.2.20.8, "POS Online PIN Certification and Enablement Program," on page 234. For information regarding the technical requirements and supported PIN formats, refer to the Network Specifications manuals and/or contact your AEGNS representative for additional information.
3. Online PIN may not be supported across all Acquirers or their S/Es. Issuers should be aware of the acceptance impact to their Cardmembers when traveling to markets where Online PIN is not supported. Contact your AEGNS representative for more information.
4. Online PIN is not supported by the Host Stand-In Authorization and Remote Stand-In Authorization Services. Refer to Section 5.8.1.2, "Unsupported Functions and Features," on page 257 and Section 5.8.2.2, "Unsupported Functions and Features," on page 259.

For details on the construct and use of the CVM, please refer to the AEIPS Chip Card Specifications and applicable Digital Wallet Program service guides including, but not limited to, the *Expresspay Mobile HCE Issuer Implementation Guide*.

5.10.3 Deferred Payment Plan (DPP)

The Deferred Payment Plan (DPP) is an optional network feature requiring Certification that allows Cardmembers to pay for products and services in installments. Both the Issuer and the Acquirer of a Transaction must be certified for a DPP Transaction to be successful. For more information regarding the Deferred Payment Plan process, refer to the Network Specifications manuals.

5.10.3.1 Issuer-Based Deferred Payment Plan

The Issuer-based Deferred Payment Plan requires that the S/E send a Pre-Authorization Request to the Issuer requesting the available DPP. After receiving the terms in the Pre-Authorization Response, the S/E must submit an Authorization Request back to the Issuer for approval. The S/E must ensure that the number of installments is recorded on the Record of Charge (ROC). The terms of the Deferred Payment Plan must be acknowledged in writing by the Cardmember.

Upon Issuer approval, the Acquirer will submit the full Transaction amount and the Issuer will bill the Cardmember in installments.

The Host and Remote Stand-In Authorization services are not available for Issuer-based DPP.

5.10.3.2 Acquirer-Based Deferred Payment Plan

The Acquirer-based Deferred Payment Plan requires that the S/E send an Authorization Request to the Issuer with the suggested DPP criteria. The Issuer provides a response to the S/E with the Authorization decision which includes the confirmed terms of the Deferred Payment Plan if the Transaction has been approved. The

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

S/E must ensure that the number of installments is recorded on the Record of Charge (ROC). The terms of the Deferred Payment Plan must be acknowledged in writing by the Cardmember.

Upon Issuer approval, the Acquirer will release the first installment for Cardmember billing. The Acquirer will manage the release of subsequent installments per the terms of the DPP. The Issuer will bill the Cardmember as these installments are released.

The Host Stand-In Authorization Service is available for Acquirer-based Deferred Payment Plan requests. Authorizations are made using single charge and velocity values provided by the Issuer.

Voice Authorization and Remote Stand-In processing are not available for DPP.

Two (2) types of Authorizations may be used for DPP:

- POS pre-Authorization messages (Issuer DPP only)
- POS Authorization messages (both Issuer and Acquirer DPP)

The Network will send a "service not permitted" message to the Acquirer for pre-Authorization and Authorization Requests for Issuers that are not certified for DPP.

5.10.4 CSC Feature

AEGNS has a variety of Card security features that provide protection from fraudulent activity in both Card Present and Card Not Present environments. Detailed information regarding the encoding, Encryption, and validation of CSC values can be found in the Network Specifications manuals. AEGNS provides the following Card security features:

- 5CSC
- 4CSC
- 4DBC
- 3CSC
- iCSC
- OTP

5.10.4.1 5CSC

5CSC is a 5-digit value located on the magnetic stripe of the Card. Refer to Figure 5-1. When a Card is swiped through a POS device, this value is passed to the Issuer for validation in the POS Authorization Request (1100) message. The Issuer uses the 5CSC validation result as one (1) of the parameters in determining how to decision the Authorization Request.

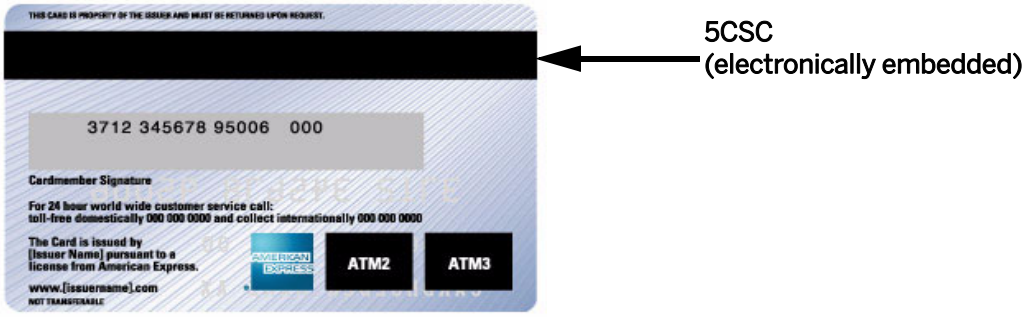


Figure 5-1 5CSC Location on Cards

See Section 8.10.2, "5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program," on page 392 for information regarding the 5CSC requirements for Issuers.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The Host Stand-In Authorization Service will validate the 5CSC value during Stand-In using the Encryption keys supplied by the Issuer. The Network will not validate 5CSC if the Authorization Requests are decisioned via Remote Stand-In.

5.10.4.2 4DBC and 4CSC

The 4DBC and 4CSC are 4-digit codes found on the front of Cards on the right side. Refer to Figure 5-2. An Issuer may only encode either 4DBC or 4CSC on the Card. The 4DBC/4CSC can be submitted for both Card Not Present Transactions and from Card Present POS devices as an added source of protection against fraud. The Issuer is required to validate the 4DBC/4CSC submitted in the Authorization Request and send an Authorization Response back to the S/E with the result of the validation. For more information regarding the technical requirements for 4DBC/4CSC, refer to the Network Specifications manuals.



Figure 5-2 4CSC/4DBC Location on Cards

Participant requirements:

- Issuers are required to have the 4DBC or 4CSC printed on the front of all Cards. Refer to the Network Specifications manuals for more information.
- Acquirers are required to certify to send the 4DBC/4CSC value in the POS Authorization Request (1100) message.

5.10.4.3 3CSC

The 3CSC is an encrypted 3-digit code derived from an algorithm that is printed on the signature panel on the back of the Card. Refer to Figure 5-3.

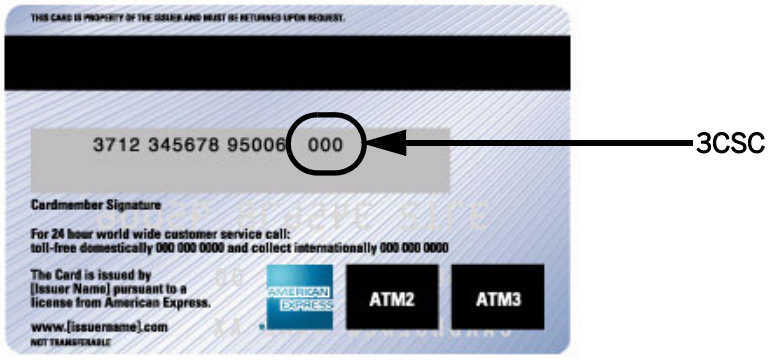


Figure 5-3 3CSC Location on Cards

Printing the 3CSC value on the signature panel is optional for Issuers.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.10.4.4 iCSC

iCSC is a 5-digit value generated with the CSC Version 2.0 algorithm located on the magnetic stripe equivalent on the Card's chip. Refer to Figure 5-4.

When the information on the chip is read by a Chip-Enabled Device, the iCSC value is passed to the Issuer for validation in the POS Authorization Request (1100) message. The Issuer uses the iCSC validation result as one (1) of the parameters in determining how to decision the Authorization Request.



Figure 5-4 iCSC Location on Cards

5.10.4.5 One-Time Password (OTP)

An OTP is a 4-digit dynamic code provided by the Issuer to the Cardmember. An OTP can be submitted for both Card Not Present and Card Present Transactions as an added means of protection against fraud. The Issuer is required to validate the OTP submitted in the POS Authorization Request (1100) message and provide the validation response in the POS Authorization Response (1110) message.

Issuers interested in providing OTPs to Cardmembers should contact their local AEGNS representative.

5.11 ATM Authorizations

ATM Authorization processing is available for all Participants on the Network. The following sections define the ATM Authorization processes and the requirements of Participants.

5.11.1 ATM Authorization Process - End to End

ATM operation varies according to the capabilities of the ATM and the software instructions which drive it. Although the sequence of steps may vary from ATM to ATM, all ATMs have the capability to dispense cash. ATM Authorizations follow these basic steps:

1. The Cardmember causes the Card's magnetic stripe or Chip data to be read by the ATM, either by inserting the entire Card into the ATM or by passing the Card through the ATM's stripe reader.
2. The ATM prompts the Cardmember to enter his/her PIN.
3. The Cardmember enters his/her PIN using the ATM's keypad.
4. The ATM screen displays one (1) or more options for dispensing cash.
5. The Cardmember selects a cash dispense option and amount.
6. The ATM relays the Transaction data (including the Card number, cash amount, encrypted PIN, and other information) to the ATM Acquirer.
7. The ATM Acquirer's system formats and transmits this data to the AEGN as an Authorization Request message.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8. When the AEGN receives this request, it identifies the Issuer by comparing the Card prefix with Network resident lookup tables and forwards the data to the Issuer's host system for Authorization.
9. The Issuer's Authorization decisioning system reviews the Authorization Request and Cardmember Information.
10. If the Authorization Request successfully passes this examination, the Authorization Request is approved without manual intervention, and the Issuer's Authorization system returns an "Approved" response message (indicated by an Action Code of 000) to the Network, which the Network forwards to the ATM Acquirer.
11. The ATM Acquirer's system relays the "Approved" message to the ATM.
12. The ATM dispenses the cash and optionally prints a Cardmember receipt. The actual Card Account number must not be printed in full on the receipt but may either be scrambled before printing or masked to allow only the last four (4) digits to be printed.
13. If the Issuer's decisioning system does not approve the Transaction, the Issuer may respond with another response as described in Section 5.11.4, "ATM Authorization Responses," on page 268.

If the Issuer fails to respond within the Authorization Response timeframe, the ATM will display the default timeout message.

5.11.2 ATM Acquirer Authorization Standards

ATM Acquirers operating on the AEGN are responsible for enabling Authorizations from ATMs they operate. ATM Acquirers must also ensure that these ATMs comply with Network policy as set forth in this edition of the *Business and Operational Policies* manual.

5.11.2.1 Hours of Operation

ATM Acquirers are responsible for routing all Authorization Requests, twenty-four (24) hours per day, seven (7) days per week, from ATMs that they operate. This requirement may be fulfilled by the ATM Acquirer through one (1) or more of the following means:

- Direct interface to the AEGN, or
- Indirectly, through the use of an Authorized Processor.

5.11.2.2 Authorization Systems

ATM Acquirers are responsible for providing Authorization routing to the Network from ATMs that they operate and/or from those ATMs for which the ATM Acquirer provides access.

AEGN Cardmember Transactions taking place at Acquirer operated ATMs must be transmitted through the Network.

5.11.2.3 Authorization Message Content

When an ATM device captures magnetic stripe content and PIN, the ATM Acquirer must forward the data to the Issuer (via the Network) as part of any Online Authorization Request message. The requirements for an ATM Authorization message are contained in the *Network Specifications - Authorization* manual.

5.11.2.4 System Outage Notification

In the event that the AEGN fails to respond to an Authorization Request, the Acquirer should immediately notify its AEGNS technical Help Desk. A representative at AEGNS will escalate the issue to the appropriate support personnel within the Network to restore service.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5.11.3 ATM Authorization Requests

All ATMs where Cards are accepted must be connected through Acquirers or networks which can forward Authorization Requests to the AEGN. ATM Authorization Messages must be online and will not be routed to Stand-In for decisioning should connectivity be unavailable.

5.11.3.1 ATM Location Requirements

Participants must ensure that their ATM dispensing machines:

- Do not rewrite the magnetic stripe on any Card or attempt to validate the magnetic stripe data,
- Do not make any attempt to validate the PIN (PINs are validated on the Issuer's Authorization system),
- Do not capture the Card unless requested to do so by an Action Code.

5.11.3.2 Personal Identification Number (PIN)

Cardmember PIN entry is required and the encrypted PIN must be forwarded to the Issuer as part of the Authorization Request message to enable verification. For details of supported PIN formats, refer to the Network Specifications manuals.

5.11.4 ATM Authorization Responses

Issuers are solely responsible for providing Authorization Responses to ATM Authorization Request Messages. Authorization Responses must comply with the Network Specifications manuals. Issuers must respond to ATM Authorization Request Messages within two (2) seconds of the time the Network transmits the Authorization Request to the Issuer. The round-trip time, from the initiation of the request at the ATM until the response is received at the ATM, will not exceed eight (8) seconds, as per the Network Specifications manuals.

Issuers log and respond to ATM Authorizations in the same manner as that described for POS Transactions. Referral responses are not permitted for ATM Authorization Requests.

In some instances, the Acquirer system may be programmed to convert a Pick Up message into a Deny response. The AEGN has no way of informing the Issuer when this conversion may be occurring. The Network and American Express Entities accept no responsibility or liability for Cards that are or are not captured by the ATM.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6 Clearing and Settlement

6.1 Introduction

The purpose of this chapter is to supply AEGNS Participants with the information necessary to clear and settle Transactions. The chapter begins with an overview of the Clearing and Settlement process including Transaction flows and definitions. The Clearing, Settlement, and Funds Exchange processes are explained, concluding with information on Acquirer, Issuer, and Network Rates.

For each Participant, the terms under which Transactions are settled are set out separately in agreements between each Participant and AEGNS.

6.2 Overview

All Financial and Non-Financial Transactions on American Express Cards that are submitted by Participants must flow through the Network Clearing process. Clearing is the process of editing, routing, and calculating Transactions submitted by Participants. The AEGN performs Clearing for Participants including First Presentments, any Transactions which may result from Chargeback processing, Second Presentments, and fee Transactions. Participants may submit Transactions to the AEGN at any time during the day. In order for Transactions to be included in financial Settlement, they must be submitted and cleared in accordance with the Network cutoff schedules as referenced in Section 6.3.3, "Settlement Schedule," on page 271. The cleared Transaction detail and summary records created by the AEGN are forwarded to Participants.

Settlement and Funds Exchange are the financial processes of computing Settlement totals and moving funds between Participants based on the Transactions cleared for the Settlement period. Funds Exchange occurs each Settlement Day. Funds Exchange includes the Settlement period's accumulated Transactions that have been cleared and forwarded to the Participant. The Network applies the fees associated with Acquirer's Rate/Issuer's Rate/Network Rate and foreign exchange to arrive at a Settlement position for each Participant. If funds are due to the Participant, the Network sends payment instructions to the Network's Settlement Bank instructing it to transfer the Settlement amount to the Participant's Settlement account. If funds are due to the Network, the Network sends payment instructions to each Participant's designated Settlement Bank or authorized agent instructing them to transfer the Settlement amount to the Network's Settlement Bank account.

6.2.1 The Transaction Life Cycle

The Transaction Life Cycle describes all the steps involved in processing Charge or Credit Transactions as viewed from the perspective of the AEGN. These steps are described in Section 1.7, "The Transaction Life Cycle," on page 10.

6.2.2 Time Usage in the *Business and Operational Policies* Manual

Unless otherwise noted in this chapter, all reference to "time" is stated in Eastern Time (ET in the United States). The use of "day" or "days" refers to calendar days.

6.3 Clearing Procedures

This section covers processing procedures for the AEGN Clearing system.

Participants that have contractually agreed to issue Cards and/or to acquire the Card Transactions and/or ATM Transactions must submit the Transactions through the Clearing process in order to exchange Transaction data. Outclearing is the movement of data from the Participant to the AEGN. Inclearing is the movement of data from the AEGN to the Participant.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The AEGN Clearing process edits all data received from Participants, verifies data accuracy, reorganizes the data by the Issuer's IIN (Issuer Identification Number) or the Acquirer's AIN (Acquirer Identification Number) and then sends the records to the appropriate Participant.

All Participants have certain rights and obligations in the processing of Clearing Transactions. Participants must submit and accept specific Transaction records through the AEGN Clearing processes as defined in this chapter. An Issuer, upon receiving a First Presentment through the Clearing process that is not in conformance with Network policies, may have specific rights to return the Transaction to the Acquirer via the Chargeback process. Acquirers, then, may have specific rights to resubmit the Transaction via a Second Presentment. This exchange of Transactions is described in more detail under the guidelines set forth in the "Chargeback Policies" chapter beginning on page 280.

6.3.1 Presentment and Acceptance of Transaction

All Transactions on an Issuer's Cards shall, after acceptance by AEGNS or its designee, be cleared and presented by AEGNS to, and accepted by, such Issuer without recourse to American Express, American Express Entities or any Acquirers (except in accordance with the "Chargeback Policies" chapter beginning on page 280), as follows:

1. In the case of Charges, at a price equal to the face amount less the applicable Issuer's Rate as set out in the applicable Participant Agreement; or
2. In the case of ATM Transactions on the Amex Shared ATM Network, at a price equal to the face amount plus the applicable ATM Transaction fee(s), as set out in the applicable Participant Agreement (or a separate ATM Access Agreement as the case may be); and
3. In both cases, plus any applicable Foreign Currency Factor, as set out in the applicable Participant Agreement.

All Charges presented by an Acquirer shall, after acceptance by an Issuer or its designee, be settled by AEGNS without recourse against the Acquirer (except in accordance with the "Chargeback Policies" chapter beginning on page 280), at the face amount less the applicable Network Rate as set out in the applicable Participant Agreement.

6.3.2 Submission Process

All POS Transactions are outcleared to the AEGN by Participants as specified in the *Network Specifications - Financial/Non-Financial* manual. Submission can occur at any time. For each Transaction between the Acquirer and the Issuer, the AEGN procedures allow for the submission of the original Presentment (by the Acquirer), a Retrieval Request (by the Issuer), a Fulfillment (by the Acquirer), a First Chargeback (by the Issuer), a Second Presentment (by the Acquirer), and a Final Chargeback (by the Issuer).

6.3.2.1 Message Type

For each Transaction between Acquirers and Issuers, AEGNS requires the Participant to use a specific message type. If a message is submitted by a Participant that is not valid for that Participant or for that Transaction, the message will be rejected. Refer to the Network Specifications manuals for further information.

6.3.2.2 Message Order

The Network will ensure that all financial message types are submitted in the correct order:

1. A First Presentment must occur before a First Chargeback may be processed.
2. A First Chargeback must occur before a Second Presentment may be processed.
3. A Second Presentment must occur before a Final Chargeback may be processed.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.3.2.3 Message Outclearing

Outclearing is the movement of data from Participants to the AEGN. The data is related to a single Cardmember Transaction or group of Transactions and is contained in a specific message type. Refer to the *Network Specifications - Financial/Non-Financial* manual for more information about message types.

Participants may outclear files multiple times throughout the day. The AEGN will receive and edit files from a Participant for format, content, and policy compliance. The Clearing process includes the following:

1. File Acknowledgment - Upon receiving a file, the AEGN will accept, reject or partially accept the file. Once editing is completed, the AEGN will send a File Acknowledgment to the Participant. AEGNS will initiate processing and settlement for all messages that have passed all edit rules. Refer to the *Network Specifications - Financial/Non-Financial* manual for the File Acknowledgment message layout.
2. Rejects - Rejects (partial or entire) can occur at a message level or at a file level. The AEGN will send back all rejects to the Participant with corresponding reject reason codes (maximum of ten (10) per message). In addition, an entire file reject will also occur if a file level error is detected. For example, all duplicate files will be rejected by the Network and the originating Participant will be notified of the reject and provided with the reject reason codes.
3. Error threshold - Each Participant chooses an error threshold that is utilized by the AEGN to determine if a file should be rejected due to excessive rejected messages. If the number of errors found in a file meets or exceeds the error threshold for a Participant, the AEGN will reject the entire file.

6.3.2.4 Cancelled S/E Submissions

Acquirers are responsible for ensuring that submissions by cancelled S/Es are not outcleared to the Network.

6.3.2.5 Message Inclearing

Inclearing is the movement of data from the AEGN to a Participant. Once all Transactions have been processed from an outcleared file, the Network will create and route files of accepted Transactions with the message types that are specific to the receiving Participant.

1. A Retrieval Request, Chargeback, or Final Chargeback submitted by an Issuer will be incleared to the designated Acquirer.
2. A First Presentment, Fulfillment Notification, or Second Presentment submitted by an Acquirer will be incleared to the designated Issuer.

Acknowledgment of accepted and rejected Transactions or files created and transmitted to Participants must be provided by the Participant.

6.3.3 Settlement Schedule

A Participant may outclear files multiple times throughout the day. Files are processed according to the transmittal date and time stamp on the header record during the file capture process. A single Settlement process will occur once each Settlement Day between the AEGN and Participants.

6.3.4 Scheduled Outages

AEGNS will attempt to communicate and manage planned system outages in timeframes that minimize impact to both the AEGN and Participants.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.3.5 Clearing and Settlement Financial Life Cycle and Processing Times

The required AEGNS financial life cycle and processing timeframes are described in Section 6.4.3.2, "Participant Failure to Settle on a Timely Basis," on page 275 through Section 6.4.3.8, "Delays," on page 277.

Participants must comply with the Clearing and Settlement timeframes process. It is the Participant's responsibility to control and monitor the submission process until an acknowledgment is received from the AEGN.

For additional information regarding processing timeframes and file acknowledgments, refer to the *Network Specifications - Financial/Non-Financial* manual.

6.3.6 Bank Holidays - Clearing

The Clearing data files will continue to be processed on Bank Holidays by Participants and the AEGN. Participants may outclear files and receive inclear files seven (7) days per week.

6.4 Settlement and Funds Exchange

Settlement is the process by which the Network computes and advises Participants of the net totals that will be used for Funds Exchange. Funds Exchange is the process by which Participants transfer funds based on the net value of the financial Transactions cleared for a given day or period. The AEGN notifies Participants of their Net Settlement for Clearing Transactions. Funds Exchange is performed based on the Net Settlement.

For the most common Transaction type, a Charge, the Acquirer will have a net credit position and the Issuer will have a net debit position. However, due to disputes, fees and the fact that some Participants act as both an Acquirer and Issuer, the Net Settlement will depend on the number and the value of Transactions as calculated for the Participant during the Clearing process. The AEGN calculates the Net Settlement for all Participants involved in the Clearing process for a given Settlement period. Participants may use either the Daily Activity Process (DAP) or Daily Settlement Advisement for Settlement and Funds Exchange.

The obligation of a Participant to make payment to AEGNS for Transactions presented to such Participant is absolute and unconditional. A Participant must not withhold or attempt to withhold full payment from AEGNS for any reason, including without limitation, an S/E's commencement (voluntarily or involuntarily) of bankruptcy or similar proceedings or an S/E's complete or partial cessation of operations. If a Participant fails to make payment to AEGNS when due or fails to provide adequate collateral pursuant to its Participant Agreement, in addition to AEGNS' other rights and remedies under contract, law and equity, AEGNS shall be entitled immediately to enforce any guaranty of the Participant's obligations, to setoff and recoup any amounts owed by AEGNS to the Participant under its Participant Agreement, and immediately suspend or terminate acceptance of such Participant's Cards, as applicable.

6.4.1 Settlement Process

The following rules establish the policies regarding Settlement of funds between Participants and the AEGN. Participants may utilize the Daily Activity Reports and/or Daily Settlement Advisements to facilitate the Settlement of funds.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.4.1.1 Daily Activity Process

The Daily Activity Process provides Participants with the ability to facilitate their own reporting needs with a single consolidated source of information. All activity will be reported in a single, mandatory report and an optional file allowing the Participant to create custom reporting and to post data to their internal reconciliation systems. The Participant's daily activity will be available in two (2) formats:

1. A Daily Activity Report (DAR) containing consolidated information of Participant's activity for purposes of financial and daily activity reconciliation. Receipt of this report is mandatory.
2. A Daily Activity File (DAF) containing consolidated information of a Participant's daily transaction activity. Receipt of this file is optional. Participants can use the DAF to automate reconciliation processes, create customer reporting or segment activity for other purposes.

The Daily Activity Report (DAR) may include details of financial activity that were not received via a submitted Transaction. In these cases, the Participant may not have been certified to receive the financial message. The financial activity will be identified on the Daily Activity Reports and Daily Activity File, from which the Participant is required to settle with the Network. Refer to the *Network Specifications - Instructions* manual for more information.

The Daily Activity Report (DAR) may include daily or monthly occurring manual transactions and fees. Settlement detail for these Transactions will be included in the Fee Detail Section. Participants are required to settle with AEGNS for these fees on the 26th of each month or another day designated and duly notified by AEGNS to Participants. Transactions and fees are identified by use of Valid Billing Unit Codes. Refer to the *Codes Reference Guide* for additional information.

6.4.1.2 Settlement Advisement

AEGNS prepares and sends a Settlement Advisement to certain Participants detailing the net value due to/from the Participant in the event the Net Settlement needs to be recalculated due to specific Participant requirements.

6.4.2 Funds Exchange

The following rules establish the policies regarding the Funds Exchange between Participants and the AEGN.

Participants use the incleared files and the various detailed reports reflected in the Settlement process to reconcile their net settlement with the Daily Activity Report and/or Daily Settlement Advisement. The Participants are required to transfer funds in the same settlement currency as that used on the Daily Activity Reporting and/or Daily Settlement Advisements, to or from the AEGN Settlement account via an authorized funds transfer vehicle. The Participant is responsible for settling the full Net Settlement amount with AEGNS. Any fees associated with the funds transfer (for example, bank charges) are the responsibility of the Participant.

6.4.2.1 Automated Funds Exchange

Participants must settle with AEGNS by use of Automated Funds Exchange where the Net Settlement amount is determined by the consolidated Daily Activity Reporting. Automated Funds Exchange will occur for every day financial activity results in a Net Settlement. Participants must settle the Net Settlement amount with AEGNS on the same day as receipt of the Daily Activity Report, unless the banking cut-off time in the local market restricts same-day settlement, in which case, the Participant must settle with AEGNS by the following Business Day.

Note: Funds Exchange will not occur on a Participant Settlement Bank Holiday and/or AEGNS Settlement Bank Holiday but will be made on the next scheduled Settlement Day. Refer to Section 6.4.3.1, "Bank Holidays - Settlement," on page 275 for more information.

Participants unable to utilize Automated Funds Exchange will be subject to a Manual Funds processing fee. See Section 10.5.7, "Manual Funds Exchange Processing Fee," on page 408.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.4.2.2 Manual Funds Exchange

Participants will settle with AEGNS by use of Manual Funds Exchange, where a settlement advisement is required. See Section 6.4.1.2, "Settlement Advisement," on page 273.

6.4.2.3 Foreign Exchange Conversion Rate Establishment

All amounts due from a Participant to AEGNS (or vice versa) must be paid in the agreed currency set out in the applicable Participant Agreement. Different or multiple AEGNS-approved Settlement currencies, or at AEGNS' option, U.S. Dollars, may be utilized for Settlement.

All Cardmember Transactions made in a currency different from the currency in which the Cardmember's Card is denominated will be converted by the AEGN to the Acquirer's and Issuer's settlement currency at a rate(s) selected by AEGNS.

Unless otherwise agreed between the Issuer and AEGNS, when a Cardmember's Transaction is in a currency different from the currency in which the Cardmember's Card is denominated or in a country other than the country in which the Card was issued, AEGNS reserves the right to add a Foreign Currency Factor, respectively, for the benefit of AEGNS into the value of the final Settlement amount when processing such Transactions. Such Foreign Currency Factors shall be settled in accordance with the process set out in the "Clearing and Settlement" chapter beginning on page 269.

Prior to assessment of the Foreign Currency Factors, AEGNS will notify Issuers, in writing, of the rate of the applicable factor, and Issuers are required to make disclosure to Cardmembers and prospective Cardmembers of the Foreign Currency Factor in accordance with Section 3.9.1.6, "Cardmember Agreement/Solicitation Materials," on page 207.

6.4.2.3.1 Foreign Exchange on Chargebacks

Foreign exchange gain or loss on a Chargeback Transaction will remain the responsibility of the AEGN. Issuers will Chargeback the amount they received on the original Presentment in their Settlement currency and Acquirers will receive the amount in the currency in which they originally presented.

When processing a Chargeback, Second Presentment, or Final Chargeback, the applicable Transaction settlement calculation factors will be the same as the First Presentment.

A Participant must provide the correct Transaction currency applicable to the original Presentment.

Rejected Transactions are sent back to the originator if Chargeback messages do not meet the following criteria:

1. Full Chargeback amounts must be equal to the original Presentment amount, except for debit or credit Presentment error. See "ISO 4752 - Credit/Debit Presentment Error" on page 343.
2. A partial Chargeback amount must be less than 100% of the original Presentment amount.
3. Second Presentments must be equal to or less than the original Chargeback amount.
4. Final Chargebacks must be equal to or less than the Second Presentment amount.

Only one (1) Chargeback, one (1) Second Presentment, and one (1) Final Chargeback are allowed per Presentment in the Disputes Process Transaction Life Cycle. See Section 7.3.3, "Disputes Process Transaction Life Cycle," on page 286.

6.4.3 Settlement Exceptions

The following rules establish the policies regarding Settlement of funds between Participants and the AEGN in exception situations.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.4.3.1 Bank Holidays - Settlement

Funds Exchange will not occur on a Participant Settlement Bank and/or AEGNS Settlement Bank Holiday, but will be made on the next scheduled Settlement Day. When this occurs, more than one (1) Funds Exchange will be made on the same day. For example, when Monday is a Bank Holiday for either Settlement Bank, Transactions that would normally be settled on Monday will instead be settled on Tuesday. In addition, Transactions due to be settled on Tuesday will still be settled on Tuesday.

Table 6-1. Settlement Exception Processes

If Funds Exchange is due to occur on the following Bank Holidays:	Then Funds Exchange will occur on:
Monday	Tuesday
Tuesday	Wednesday
Wednesday	Thursday
Thursday	Friday
Friday	Monday

6.4.3.2 Participant Failure to Settle on a Timely Basis

If a Participant has a net debit position, the Participant is required to do the following:

- Honor the automated funds exchange message, or
- Honor the Net Settlement amount from the Daily Activity Reporting, or
- Honor the Daily Settlement Advisement, and
- Transfer the requested funds within the timeframes required in Section 6.4.3.1, "Bank Holidays - Settlement," on page 275

If a Participant fails to adhere to these requirements, the Participant must honor an AEGN draft submitted to acquire the funds.

The Participant will honor both the amount of the debit and any compensation for each day the transfer was not effected as determined in Section 6.4.3.6.2, "Compensation from the Participant," on page 277.

If a Participant has a net credit position and is in any way unable to receive such funds, AEGNS will hold these funds until the Participant is able to receive such funds. The Participant will be required to explain the failure of the process and the actions taken to avoid future recurrence of the events. In such an event, the Participant will not be entitled to any compensation from AEGNS.

6.4.3.3 AEGNS Failure to Settle on a Timely Basis

If AEGNS fails to settle on a timely basis in accordance with Section 6.4.3.1, "Bank Holidays - Settlement," on page 275, and if the Participant is in a net credit position, AEGNS will promptly pay the difference upon recognizing the error or upon notification of the error by the Participant. AEGNS will be liable for the amounts owed according to the Daily Activity Reporting and for compensation as determined in Section 6.4.3.6.1, "Compensation to the Participant," on page 277. AEGNS will settle the credit position as part of the daily Settlement process.

If AEGNS fails to settle on a timely basis in accordance with Section 6.4.3.1, "Bank Holidays - Settlement," on page 275 with Participants in a net debit position, the Participants will promptly pay the difference upon recognizing the error or upon notification of the error by AEGNS. The Participant will be liable for the amounts owed according to the Daily Activity Reporting and for the cost of funds as calculated by AEGNS in Section 6.4.3.6.2, "Compensation from the Participant," on page 277.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.4.3.4 Participant Liability for Net Settlement

AEGNS and American Express Entities shall not have any liability to any Participant or other Person for any loss, cost, or other damage arising out of the Settlement program whether caused by its failure to exercise ordinary care, any errors, delays in effecting Daily Activity Reporting, funds transfers, or Transaction billing date transmissions except in the following cases:

1. The AEGN clearing system Daily Activity Reporting errors or delays that results in a transfer to a Participant of an insufficient amount of funds or in a transfer from a Participant of an excess amount of funds, or
2. AEGNS, through its own systems' failure to perform, is unable to receive a Participant's Transaction data or, if received, the system's inability to process the data so as to include it in the Daily Activity Reporting, or
3. If AEGNS is responsible for an error meeting the criteria described in this section and subject to the Participant's compliance with Section 6.4.3.3, "AEGNS Failure to Settle on a Timely Basis," on page 275, the total liability of AEGNS and American Express Entities for the errors or delays will be the compensation as defined in Section 6.4.3.6.1, "Compensation to the Participant," on page 277. A Participant's sole and exclusive remedy against AEGNS or its Settlement Bank with respect to any and all damage incurred by the Participant shall be the payment by AEGNS of the principal and the amount of compensation due. In this respect, only the Participant and not the Settlement Bank, if different, may recover compensation from AEGNS. Under no circumstances will AEGNS or American Express Entities be responsible for any incidental, special, indirect, exemplary, consequential, speculative or punitive damages.

Should the submission of settlement transaction data after the 180-day Presentment period be caused by a failure of AEGNS' performance as described in this section, AEGNS will pay to the Acquirer the amounts representing Transactions that were not submitted on time and that were not subject to Chargeback for other reasons, provided:

1. The Acquirer has been unable to collect the Transaction amounts, limited to the extent that it has not been able to collect, and
2. The AEGNS-designated representative was notified by the Acquirer within seventy-two (72) hours after the time the Acquirer would have received confirmation of the processing of the Settlement Transaction data, that the Settlement Transaction data at issue was not, in fact, processed. Such a claim must be made within forty-five (45) days of the receipt by the Acquirer of the Chargeback to qualify for such reimbursement from AEGNS.

6.4.3.5 Delay in Daily Settlement Advisement

In the event a Daily Settlement Advisement is not received by a Participant using manual funds exchange in accordance with Section 6.4.1, "Settlement Process," on page 272, upon receipt of the delayed Daily Settlement Advisement a Participant must transfer funds on the same Settlement Day the delayed Daily Settlement Advisement is received in the amount of such Net Settlement, noting the date of the Net Settlement. Due to the delay, another Daily Settlement Advisement and funds transfer(s) may be occurring that same Settlement Day. Each Daily Settlement Advisement received must be treated separately for Settlement purposes.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6.4.3.6 Unjust Enrichment and Compensation Computation

Any Participant that does not transfer the appropriate funds per Section 6.4.2, "Funds Exchange," on page 273, will transfer the principal due immediately, upon discovery by the Participant or by AEGNS, to the AEGN Settlement account. In addition, the Participant must also separately transfer compensation, as defined in this section, to the AEGN Settlement account. In the event of the failure of a Participant to initiate the transfer of the funds and compensation described in this section, AEGNS has the right to draft the Participant's account for funds due and for compensation, and the Participant's Settlement Bank must honor the draft.

6.4.3.6.1 Compensation to the Participant

If AEGNS fails to settle on a timely basis in accordance with Section 6.4.3.1, "Bank Holidays - Settlement," on page 275, AEGNS will reimburse the Participant. All reimbursements paid to a Participant will be computed as follows:

(Principal x Cost of Funds x number of days)/360

6.4.3.6.2 Compensation from the Participant

Compensation will be paid for the period between the date the transfer was due in accordance with Section 6.4.2, "Funds Exchange," on page 273 and the date that the respective funds are transferred correctly to the AEGN Settlement account from the Participant. Compensation will be computed as follows:

(Principal x Cost of Funds x number of days)/360)

Note: "Number of days" includes the date a Participant or AEGNS fails payment of funds owed. It does not include the date the Participant or AEGNS pays the funds owed.

6.4.3.7 Funds Exchange Dispute Process

Should a Participant dispute the amount of a Funds Exchange of which it has been advised and seeks to hold AEGNS responsible under Section 6.4.2, "Funds Exchange," on page 273, the Participant must, upon discovery, notify their AEGNS-designated representative to further investigate the matter. Regardless of whether the amount is disputed, the Participant must process the timely transfer of funds in full as reflected in the Daily Activity Reporting. Upon request by the AEGNS-designated representative, the Participant must provide relevant clearing system records or other documents required to support their dispute of the amount involved.

6.4.3.8 Delays

If a Participant seeks to hold AEGNS responsible for any delays in Funds Exchange under Section 6.4.3.6.1, "Compensation to the Participant," on page 277, the Participant must notify its AEGNS-designated representative.

The Participant must give notice to AEGNS by the end of the next Business Day of the occurrence of the delay. AEGNS' liability under Section 6.4.3.6.1, "Compensation to the Participant," on page 277 will be limited to compensation to be paid from and including the day AEGNS receives the Participant's notice until and including the day that:

1. The Participant receives the data, or
2. AEGNS is able to receive the data and process the Transactions for inclusion in the Daily Activity Reporting.

If the data is received by the Participant or received and processed by AEGNS the day after it was due, only one (1) day of compensation will be paid.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Participants claiming compensation under this section must be prepared to support their claim with all Documentation requested by AEGNS including, without limitation, printed output from electronic transmission units. Failure to provide the relevant Documentation in a timely manner will be deemed to invalidate the Participant's claim.

For the purpose of this section, notice will be given by telephone or fax (fax must include confirmation) and will be effective when received by an AEGNS-designated representative, as specified in this section. In all cases, the Participant must confirm this notice in writing by certified mail or its equivalent before the end of the next Business Day of each notice to the AEGNS-designated representative.

6.4.3.9 Currency Restrictions and Exchange Controls

If the laws and/or regulations of the United States and/or any country in an Issuer's Territory are changed to restrict the international use of a Card issued by that Issuer and/or materially affect the buying or selling rates in that country used for conversions of local currency and/or U.S. Dollar, and/or prohibit the purchase of U.S. Dollars in that country for remittance abroad or the remittance of U.S. Dollars from that country abroad (all three (3) categories of such changes collectively "Changes"), the parties agree to follow the procedure set out below:

1. Notification specifying the exact nature of the Changes to be imposed must be provided in writing by the Issuer or by AEGNS to the other immediately following discovery of the occurrence of Changes. The recommendation by either the Issuer or AEGNS as to the necessary operational steps to be implemented must be provided in writing to the other before implementation of the recommendation.
2. Notwithstanding any other provision of the Participant Agreement, in the event of Changes, AEGNS may, based on reasonable judgment, require the suspension, in whole or in part, of the use of Cards issued by an Issuer inside and/or outside any country in such Issuer's Territory. AEGNS will use its reasonable best efforts, subject to the particular time constraints, to discuss with the Issuer the Changes and the extent of such suspension in order to try to reach an understanding as to what action should be taken.
3. The Issuer must comply with any bulletins or notices issued by AEGNS or another American Express Entity advising that, due to Changes, Cards issued by an Issuer are not to be accepted inside and/or outside any country in such Issuer's Territory ("Suspension of Card Acceptance Notification").
4. Any reasonable costs associated with giving Suspension of Card Acceptance Notifications throughout the world, aside from normal authorization and bulletin releases, will be borne by the Issuer whose Cards are the subject of the Notifications.
5. Any systems or operational changes necessitated by the Changes shall, at the Issuer's expense, be communicated and implemented by AEGNS on a top priority basis to and in all affected locations following issuance of a Suspension of Card Acceptance Notification.
6. The responsibility for losses resulting to AEGNS or American Express Entities and/or an Issuer from the "Changes" and relating to Charges by that Issuer's Cardmembers which:

   a. are dated at any time following the Suspension of Card Acceptance Notification, and

   b. are at or above the applicable Network Floor Limit,

   will be borne by the entity responsible for servicing S/Es in the country in which the S/E submitted the Charges in question.

   The responsibility for all other losses resulting from Changes will, except as otherwise provided in the Chargeback policy, be borne by that Issuer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7. Subject to obtaining appropriate consent of competent authorities, if necessary, if, on occurrence of any of the Changes, an Issuer is unable to purchase U.S. Dollars for remittance abroad, or to remit U.S. Dollars abroad, as necessary, to satisfy its obligations, then all provisions of this chapter relating to payments shall be superseded by this section insofar as they are inconsistent with this section, and American Express Entities shall have the right to set off any of their obligations to an Issuer against any and all obligations of that Issuer which exist or come into existence. If after all obligations of American Express Entities have been set off as described above, excess obligations of the Issuer exist or come into existence at any time, if AEGNS shall so request in writing, the Issuer shall pay all such obligations which it cannot remit according to AEGNS' instructions to an interest-bearing U.S. Dollar bank account at a bank in its Territory as designated by AEGNS. All future payments owed by American Express Entities to the Issuer shall be set off in U.S. Dollars from such account, and
8. When the Changes cease to exist, the parties will discuss in good faith whether and when to return to the conditions governing settlement, etc., in effect before the Changes were introduced.

6.4.3.10 Suspension of Settlement

In the event that AEGNS identifies a material risk of financial or brand exposure to AEGNS, daily Net Settlement funds due to a Participant may be withheld until AEGNS determines that such risk has been sufficiently mitigated. Material risk of financial or brand exposure could result from either or both of the following:

- Potential or actual deterioration of financial markets in the Territory; or
- Governmental actions restricting the transfer or payment of funds (whether domestically or internationally).

Payments that are subsequently approved by AEGNS will be settled to the Participant in the next scheduled payment. Any withheld payments will be settled separately from the Net Settlement due to the Participant for that day.

6.5 Double Byte Character (DBC) Support

Double Byte Character (DBC) Support is an optional feature that enables certified Acquirers to send the S/E name and address in a DBC format to certified Issuers for statementing in the Cardmembers' local language.

When all of the following circumstances occur, the DBC Addendum (9240) will accompany First Presentment and may accompany Second Presentment messages:

1. A Cardmember Transaction takes place in a market where the country code of the Acquirer and the domicile country code of the Issuer are the same.
2. An Acquirer is in a region that utilizes DBCs in their local language and that Acquirer has contracted with the AEGN to provide DBC data.
3. An Issuer is in a region that utilizes DBCs in their local language and that Issuer has contracted with the AEGN to receive DBC data.

The Acquirer must identify the language of the information contained in the DBC addendum. Refer to the Network Specifications manuals for the Double Byte Character message layout.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7 Chargeback Policies

7.1 Introduction

In this chapter, Participants[1] will find AEGNS policy guidelines, to include processing timeframes and individual requirements relating to Retrieval Requests, Fulfillments, First Chargebacks, Second Presentments, Final Chargebacks, Good Faith, Arbitration and Compliance. In addition, Participants will find information relating to document delivery as it relates to disputed Transactions

It is incumbent upon the Issuer to make every effort to resolve any dispute between itself and its Cardmember. Any Transaction which remains undisputed by the Cardmember, or for which the Issuer no longer has financial liability, is not eligible for Chargeback rights. Furthermore, Issuers should ascertain that their Cardmember has dealt directly, or attempted to deal directly with the Merchant before filing a Retrieval Request or First Chargeback with the Network.

Nothing in this policy shall be construed so as to permit an Issuer to refuse Presentment of Transaction data or a Participant to withhold payment via the Network.

All references to "day" or "days" in this chapter refer to calendar days, unless otherwise specified, and the Network Processing Date (NPD) of any individual Transaction is considered day zero for the purpose of counting Chargeback timeframes.

7.2 Chargeback Policies Overview

The AEGN Chargeback policy grants Participants the right to have all or part of the financial liability associated with certain disputed Transactions, as set forth in this policy, transferred to the Participant from which the Transaction originated.

The Chargeback process involves handling Transactions that are disputed by the Cardmember or by the Issuer in accordance with the applicable Chargeback rule. Certain conditions apply allowing an Acquirer to send a Second Presentment of a disputed Transaction to the Network following receipt of a First Chargeback.

The Chargeback policies in this chapter define the only conditions under which Participants may dispute a Transaction. Unless stated otherwise in a Chargeback rule, the *Business and Operational Policies* manual in effect as of the Transaction Date will determine a Participant's requirements for processing a dispute. No dispute rights other than those specified in the *Business and Operational Policies* manual in effect at the time of the Transactions and *Network Participant Updates* exist. Participants must therefore ensure that any dispute processed conforms to these conditions and any applicable rules relating to Documentation before filing any step in the dispute life cycle with the Network.

Issuers and Acquirers may submit a Good Faith request to the other providing all conditions are met. Refer to Section 7.11, "Good Faith," on page 364 for additional information.

If an Acquirer has grounds to dispute the Issuer's claim made when the Issuer filed a Final Chargeback, the Acquirer may submit an Arbitration Filing with the Network. These details are described in Section 7.12.1.1, "Arbitration Filing Procedures," on page 367. A pre-Arbitration attempt prior to submitting an Arbitration Filing is not required, but is encouraged.

Issuers and Acquirers may be able to submit a Compliance Filing to the Network at any step during the dispute life cycle, providing all appropriate conditions have been met. See Section 7.12.2, "Compliance," on page 369 for more information.

All documents submitted by either a Participant or AEGNS to the other shall be in the English language. Where an "original" document is not in the English language, it shall be submitted in its original language and accompanied by an English translation.

1. For the purposes of Chapter 7 of the *Business and Operational Policies* manual, references to Participants means Issuers, Acquirers or Authorized Processors handling Dispute Transactions on behalf of the Issuer or the Acquirer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.2.1 Handling of Disputed Transactions

Participants are required to comply with applicable law when handling disputed Transactions.

In addition, both Issuers and Acquirers are required to monitor the number of disputed Transactions they handle, reviewing for trends and patterns. For example, a pattern may suggest to an Issuer where a review of their Authorization procedures is warranted, while Acquirers may look for trends indicating inappropriate Card acceptance procedures or Merchants not fulfilling Retrieval Requests.

Issuers are required to notify AEGNS if (a) there is an unusual increase in the number of Retrieval Requests or Chargebacks, or (b) they have reason to believe that an unusual increase in the number of such Transactions is likely, and to appoint a dedicated Person or team to work with AEGNS on an agreed plan to handle any such unusual increase.

Participants are under an obligation to make appropriate usage of the dispute process (e.g., Chargebacks or Retrieval Requests are not intended nor should they be used by a Participant for purposes of making submissions the Participant knows or should know are not likely to succeed on the merits), and are required to use the Chargeback right that most closely fits the circumstances of the situation. Issuers are required to ensure Cardmembers do not authorize usage of their Card by anyone other than the Cardmember him/herself. In the event that AEGNS becomes aware of a Participant abusing these processes, or of an unusual increase in the number of disputed Transactions being submitted by Participants, AEGNS may, at its discretion, intercede and take appropriate action including, but not limited to, adjusting the timeframes to act as set out in the applicable Chargeback rule and/or levying penalties.

Issuers may not charge back Acquirers for losses incurred through the use of counterfeit Cards or Cards issued on Fraudulent Applications that appeared to be, and were accepted as, legitimate Cards, providing all other Card acceptance procedures were followed by the S/E except when the Transaction qualifies under Section 7.10.8.1, "AEIPS Fraud Liability Shift (FLS)," on page 359. "ISO 4763 - Fraud Full Recourse" on page 348 continues to allow Issuers the right to transfer liability of eligible fraud types to the Acquirer for Transactions that meet the requirements of this Chargeback.

7.3 The Transaction Life Cycle

The Transaction Life Cycle describes all the steps involved in processing Charge or Credit Transactions as viewed from the perspective of the Network. These steps are illustrated in the "Introduction" chapter beginning on page 1, and those steps involved in the disputes process are described in Section 7.3.3, "Disputes Process Transaction Life Cycle," on page 286 in more detail.

7.3.1 Authorization Processing

The two (2) processes that follow are described fully in the "Authorizations" chapter beginning on page 245 and take place utilizing the AEGN Authorization system.

7.3.1.1 Authorization Request

Transactions under the Network Floor Limit do not require Authorization. In cases where the S/E is suspicious of the Cardmember, the Card, or the conditions of the purchase, the S/E shall request Authorization in order to meet all the requirements described in the "Authorizations" chapter beginning on page 245. Request for Authorization may be made electronically through transmission from a POS device to the Acquirer's computer systems or verbally via telephone connection to the Acquirer's Authorization center.

Where a Chip Card is used in a Chip Card-enabled POS terminal or ATM, and the LCOL (Lower Consecutive Offline Limit) has been set to a number higher than zero (0), Authorization may be granted by the Chip Card application without recourse to Online Authorization. In such circumstances this shall be considered an Authorized Transaction under all Chargeback Reasons if the terminal accurately followed Card instructions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.3.1.2 Authorization Response

To allow completion of Transactions, Authorization is provided by one (1) of the following:

- The Issuer, or
- The Network if done during the Stand-In process, or
- An AEIPS-compliant and/or Expresspay-compliant application for Chip Card Transactions or Mobile Device in an AEIPS and/or Expresspay-compliant POS device

7.3.2 Clearing and Settlement Processing

The following Transaction Life Cycle steps are processed using the Clearing and Settlement functions of the AEGN infrastructure and/or AEGNS Network Disputes Manager. Only Presentment takes place for all Transactions. Retrieval Request and Fulfillment may be performed even though a Transaction is not charged back by the Issuer. All of these processes are described in detail in the "Clearing and Settlement" chapter beginning on page 269.

7.3.2.1 Presentment

After the S/E submits the paper or electronic Record of Charges (ROC(s)) to the Acquirer, the ROCs are sent to the Network to enter the Clearing and Settlement process in order to transfer the financial liability from the Acquirer to the Issuer and ultimately to the Cardmember. Presentment is the first time all the details of a Transaction move from Acquirer to Issuer.

7.3.2.2 Retrieval Request

When the Issuer requires a copy of the ROC or other Documentation, the Issuer sends a Retrieval Request Notification (1642) message to the Network, which then passes it on to the Acquirer for Fulfillment. The Retrieval Request Notification (1642) message must provide sufficient details of the Transaction to allow the Acquirer to identify it and must indicate the Document Type being requested.

The three (3) most common reasons for an Issuer to initiate a Retrieval Request are to:

- Satisfy a Cardholder inquiry
- Substantiate a Chargeback
- Support a legal or fraud investigation

Issuers may not initiate a Retrieval Request for a Transaction Certificate on a Chip Card Transaction if the Data was sent as an addenda to the First Presentment.

7.3.2.3 Fulfillment

Fulfillment is the transfer of Documentation from the Acquirer to the Issuer in support of the Issuer's Retrieval Request.



Refer to Section 7.3.2.14, "Documentation Delivery," on page 285 for additional information regarding delivery of Documentation.

The Acquirer must send a Fulfillment Notification (1640) message in response to all Retrieval Requests. If the Acquirer cannot provide Documentation, the Acquirer must notify the Issuer that it cannot fulfill by using the appropriate response in the Fulfillment Notification (1640) message. Acquirers that do not send the required Fulfillment Notification in reply to a Retrieval Request will have limited Second Presentment rights.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.3.2.4 First Chargeback

When an Issuer identifies a Transaction that it determines does not comply with the policies of the AEGN, the Issuer may initiate the process to move the financial liability from itself to the Acquirer by filing a First Chargeback. Chargebacks may be filed only for those Transactions where financial liability resides with the Issuer at the time of the Chargeback. Any Transaction that the Cardmember or their agent has paid for and does not dispute may not be charged back to the Acquirer regardless of whether or not it was in violation of Network policies except for processing errors as defined in Section 7.9.3, "Processing Error Chargeback Types," on page 304. In addition, and unless the Cardmember specifically disputes all or part of the Transaction, it is incumbent upon the Issuer to make every effort within the bounds of applicable law to collect payment for any Transaction before filing a First Chargeback.

To file a First Chargeback, the Issuer must:

1. Act within the timeframes specified by the applicable Chargeback rule. It is the Issuer's responsibility to ensure that the Cardmember provides the specific information, when required, and within the applicable timeframes.
2. Retrieve supporting Documentation as specified for the applicable rule.
3. Pass to the Acquirer the required Documentation collected from the Cardmember or prepared by the Issuer in support of the Chargeback.
4. Pass to the Acquirer the specific details which cause the Transaction to be in violation of the AEGN policies.

Issuers must file a First Chargeback within 120 days from the Network Processing Date of the First Presentment of the disputed Transaction, unless otherwise specified in the applicable rule. Failure to comply with the Documentation timeframes specified in Table 7-16, "Process Timeframes," on page 303 will allow the Acquirer to file a Second Presentment.

Refer to Table 7-16, "Process Timeframes," on page 303 for additional details regarding submission of Documentation via AEGNS Network Disputes Manager.

7.3.2.5 Second Presentment

If the Acquirer determines (based on a review of the item, any further supporting Documentation provided by the S/E, and the relevant Network policies) that there is sufficient justification to dispute the First Chargeback, a Second Presentment may be filed with the AEGN by the Acquirer, thereby moving the financial liability from the Acquirer back to the Issuer. The Second Presentment amount must be equal to or less than the original Chargeback amount.

The Acquirer may also make a Second Presentment if the Issuer, when sending the First Chargeback, failed to comply with Network policies for one (1) of the following reasons:

1. The Documentation required to support the First Chargeback was incomplete, incorrect, or not received within the required timeframe.
2. The First Chargeback was improper; i.e., did not comply with the Network policies.
3. The Acquirer's Reference Number or Cardmember Account number was invalid or not the same as in the original Presentment.

Refer to Table 7-16, "Process Timeframes," on page 303 for additional details regarding submission of Documentation via AEGNS Network Disputes Manager.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

When an Acquirer submits a Second Presentment to an Issuer, a Message Reason Code is required to indicate why the Second Presentment is being sent. Refer to Table 7-14, "Second Presentment Message Reason Codes," on page 300. Acquirers must file a Second Presentment within forty-five (45) days from the Network Processing Date of the First Chargeback. Failure to comply with the Documentation timeframes specified in Table 7-16, "Process Timeframes," on page 303 will allow the Issuer to file a Final Chargeback.

7.3.2.6 Final Chargeback

Once the Second Presentment is received, the Issuer determines (based on a review of the Second Presentment, First Chargeback supporting Documentation, and any further supporting Documentation provided by the Acquirer, and the relevant Network policies) if there is sufficient justification to dispute the Second Presentment. The Final Chargeback amount must be equal to or less than the Second Presentment amount.

A Final Chargeback is processed in the same manner as was the First Chargeback. The Issuer must do the following to file a Final Chargeback:

1. File a Final Chargeback with the Network within forty-five (45) days from the Network Processing Date of the Second Presentment.
2. Retrieve supporting Documentation as specified for the applicable rule.
3. Pass to the Acquirer the required Documentation collected from the Cardmember or prepared by the Issuer in support of the Chargeback.
4. Pass to the Acquirer the specific details which cause the Transaction to be in violation of the AEGN policies.
5. Ensure that the Final Chargeback complies with AEGN policies.

The Chargeback Policies reason code used for a Final Chargeback does not have to be identical to that used for the First Chargeback, but restrictions may apply to modifications of the reason code if changing from a non-fraud type to a fraud type. If the Documentation supplied with the Second Presentment reveals a more appropriate and better supported reason for charging back the Transaction, the Issuer may use that reason. In all cases, the Issuer must comply with the conditions defined in this chapter.

The Issuer may also file a Final Chargeback if the Acquirer, when sending the Second Presentment, failed to comply with Network policy for one (1) of the following reasons:

1. The Documentation required to support the Second Presentment was incomplete, incorrect, or not received within the required timeframe. Refer to Table 7-16, "Process Timeframes," on page 303 for additional information regarding the submission of Documentation via AEGNS Network Disputes Manager.
2. The Second Presentment was improper (i.e., did not comply with the Network policies).
3. The Issuer identifies a different Chargeback reason based on the Documentation supplied in support of the Second Presentment.

The Issuer must provide a Transaction Data Certificate on a Final Chargeback when data elements in the Transaction Data Certificate are required as proof of Issuer claim (e.g., no Authorization). For additional information related to the Transaction Data Certificate, refer to the Chip Card (9240) message in the *Network Specifications - Financial/Non-Financial* manual.

7.3.2.7 Dispute Transaction Fees

Dispute Transactions processed through the Network are subject to a processing fee. This processing fee will be charged to the sending Participant for each Retrieval Request, First Chargeback, and Second Presentment processed. Refer to Section 10.2.6, "Dispute Transaction Fees," on page 402 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.3.2.8 Dispute Message Reject Fee

Dispute Transaction messages that are rejected by the Network are subject to a processing fee. This processing fee will be charged to the sending Participant for each dispute message that is rejected by the Network. Refer to Section 10.2.7, "Dispute Message Reject Fee," on page 403 for more information.

7.3.2.9 Good Faith

The Good Faith process enables Participants to acknowledge a financial liability shift and associated funds exchange in instances where both Participants agree on the resolution. Details of Good Faith processing requirements can be found in Section 7.11, "Good Faith," on page 364.

7.3.2.10 Pre-Arbitration

Acquirers are strongly encouraged, but not required, to pursue a pre-Arbitration (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information) attempt prior to submitting an Arbitration Filing.

7.3.2.11 Arbitration Filing

An Acquirer may submit an Arbitration Filing with the AEGNS Arbitration Committee if they determine (based on a review of the Final Chargeback, any further supporting Documentation provided by the Issuer, and the relevant Network policies) that there is sufficient justification to dispute the Final Chargeback. An Arbitration Filing must be received by the AEGNS Arbitration Committee as specified in Section 7.12.1.1, "Arbitration Filing Procedures," on page 367 and Section 7.12.1.2, "Arbitration Submission Timeframe," on page 368.

7.3.2.12 Pre-Compliance Requirement

AEGNS requires that Participants attempt pre-Compliance (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information) prior to submitting a Compliance Filing with the AEGNS Arbitration Committee. Timeframes that Participants must follow prior to submitting a Compliance Filing are described in Section 7.12.2, "Compliance," on page 369.

7.3.2.13 Compliance Filing

An Acquirer or Issuer may submit a Compliance Filing to the AEGNS Arbitration Committee where a violation of the policies in the *Business and Operational Policies* manual, in effect at the time of the violation, can be documented. Issuers and Acquirers must meet specific criteria in order to submit a Compliance Filing. Details of these criteria and conditions are found in Section 7.12.2, "Compliance," on page 369. A Compliance Filing may be submitted only by the party (i.e., the Acquirer or the Issuer) who has the financial liability for the Transaction(s) in question.

7.3.2.14 Documentation Delivery

Participants must use AEGNS Network Disputes Manager (NDM) to send Documentation to other Participants.

When using NDM, Participants can prove Documentation has been sent by providing a copy of the Network Disputes Manager Sent report.

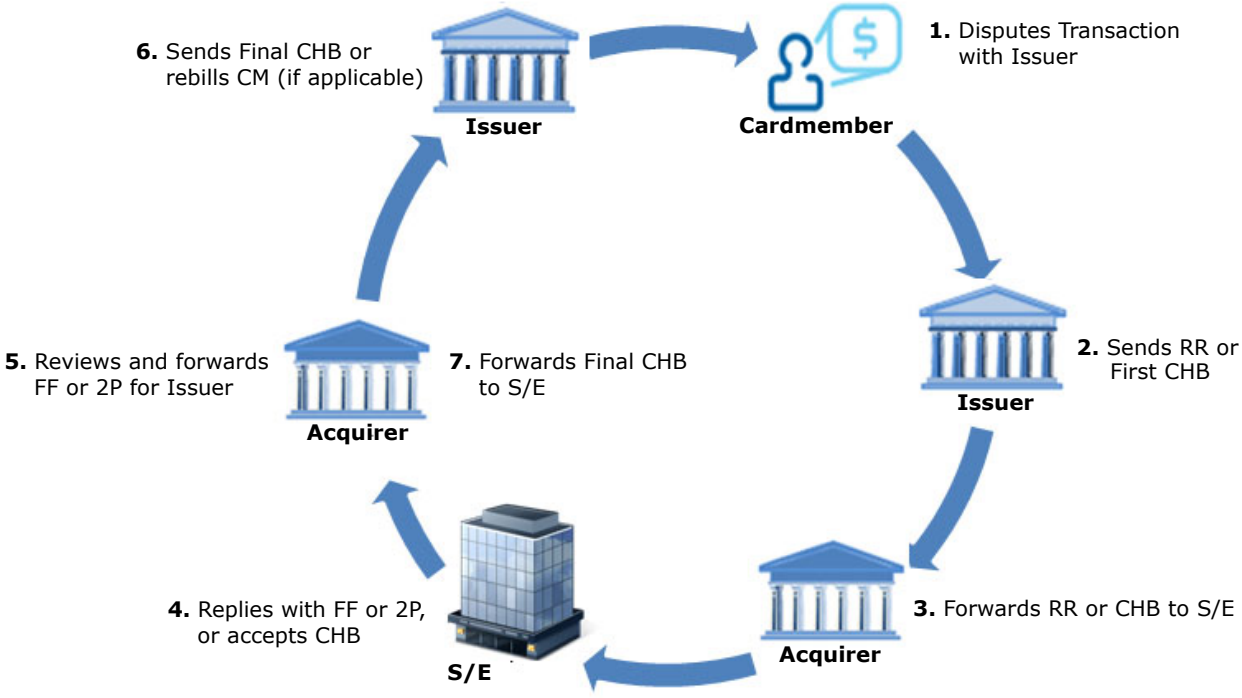
Note: Refer to Section 7.12.1.1, "Arbitration Filing Procedures," on page 367 and Section 7.12.2.1, "Compliance Filing Procedures," on page 370 for information relating to Documentation delivery for Arbitration and Compliance.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.3.3 Disputes Process Transaction Life Cycle

Only Transactions that have been disputed by the Issuer or Cardmember will require any Network processing beyond the Presentment defined in Section 7.3.2.1, "Presentment," on page 282. For those Transactions, the next few steps are referred to as the Disputes Process Transaction Life Cycle.

Most disputes begin when a Cardmember contacts the Card Issuer with a question or problem with a specific Transaction. Figure 7-1 illustrates the Network dispute life cycle and may not apply to all Participants.



- 2P - Second Presentment
- CHB - Chargeback
- CM - Cardmember
- FF - Fulfillment
- RR - Retrieval Request
- S/E - Service Establishment

Note: Steps 2 through 5 occur through the Network.

Figure 7-1 Disputes Process Transaction Life Cycle Flow

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The following table provides a description of the steps of the Disputes Process Transaction Life Cycle:

Table 7-1 Disputes Process Transaction Life Cycle Steps

Step	Who	Does What	Additional Action
1	Cardmember	Contacts the Issuer and disputes the Transaction	
2	Issuer	Gathers the information from the Cardmember and: • Sends a Retrieval Request to the Acquirer, or • Sends a First Chargeback to the Acquirer	
3	Acquirer	• Receives the Retrieval Request and forwards the information to the S/E, or • Receives the First Chargeback and debits the S/E	
4	S/E	• Responds to the Retrieval Request with a Fulfillment Notification supporting the Transaction, or • Accepts the First Chargeback, or • Disputes the First Chargeback with a Second Presentment providing supporting Documentation to validate the Transaction	If the S/E accepts the First Chargeback, no further action is required.
5	Acquirer	• Reviews the Fulfillment Notification and forwards to the Issuer, or • Reviews the support and creates the Second Presentment and forwards to the Issuer	
6	Issuer	• Receives the Fulfillment Notification and reviews the support, or • Receives the Second Presentment and reviews the support, or • Receives no reply or a response from the Acquirer of "Not Fulfilling" and sends a Chargeback to the Acquirer	• If the Cardmember accepts the Transaction, no further action is required. • If the Cardmember still disputes the Transaction and the supporting Documentation does not validate the Transaction, the Issuer sends a Final Chargeback to the Acquirer.
7	Acquirer	Receives the Final Chargeback and debits the S/E	

Additional steps may occur when there is no agreement to the validity of the Transaction. Refer to Section 7.11, "Good Faith," on page 364 and Section 7.12, "Arbitration and Compliance," on page 366 for further information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.4 Retrieval Request and Fulfillment

Issuers send Retrieval Requests through the Network to obtain Documentation from Acquirers. In order for the Issuer to fulfill its obligation to have in its possession Documentation supporting the Transaction, the Issuer may have to request Documentation from the Acquirer before a Chargeback may be filed. The Issuer must allow the Acquirer sufficient time for Fulfillment of the request in accordance with the schedule defined in Section 7.8, "Process Timeframes," on page 303. The Issuer must also review the received Documentation to ensure the intended Chargeback Reason is still appropriate. Refer to Table 7-2, "Retrieval Request - Description for Use," on page 288 for additional information.

If the applicable Chargeback policy rule requires a Retrieval Request and Documentation is requested by the Issuer and is not received from the Acquirer within the timeframes set forth in this chapter or, if the Documentation received is illegible or missing vital information, the Issuer may file a Chargeback under the Retrieval Chargeback rules. When time allows and the Issuer's Chargeback rights are not in danger of expiring, the Issuer may contact the Acquirer via the Network processes in an attempt to resolve issues surrounding the Documentation receipt or quality before filing a Retrieval Chargeback.

In the Retrieval Request Notification, the Issuer must specify the Retrieval Request Notification Message Reason Code and the Function Code (Document Type). See Table 7-3, "Retrieval Request Notification Reasons," on page 289 or the *Codes Reference Guide*. Fulfillment data required for each function code is described in Section 7.5, "Fulfillment Data Requirements," on page 294.

Documentation codes required to support an Acquirer's Fulfillment are described in Section 7.4.1, "Fulfillment Notification Reason Codes," on page 293.

Refer to Table 7-16, "Process Timeframes," on page 303 for additional information regarding submission of Documentation via AEGNS Network Disputes Manager.

Certain limitations to Chargeback and Retrieval Request rights exist for AEIPS-compliant Integrated Circuit Cards (ICCs).

The Issuer must use Transaction Certificate information to determine the circumstances of a Transaction. The details of the Card/Terminal interaction must be reviewed to determine what additional information or Documentation is necessary.

Retrieval Request rights are limited to request for information not contained in the Transaction Certificate (i.e., a copy of the ROC confirming the Transaction was "PIN verified").

Table 7-2 Retrieval Request - Description for Use

ISO Message Reason Code	Retrieval Request Notification Reason	Description for Use
6003	Chargeback Documentation	Issuer is requesting Documentation to validate that the Transaction qualifies for a First Chargeback
6006	Legal Request or Fraud Analysis	Issuer is requesting Documentation in support of a fraud investigation or as a result of a legal request.
6008	Cardmember Requests Copy of ROC	Issuer is requesting Documentation on behalf of the Cardmember. Cardmember is requesting a copy of the ROC.
6013	Repeat Documentation Request	Issuer submitted previous Retrieval Request and is repeating the original request for Documentation.
6014	Cardmember does not recognize Transaction or Transaction Amount	Issuer is requesting Documentation on behalf of the Cardmember. The Cardmember does not recognize the Transaction or Transaction amount and is requesting Documentation to validate his/her authorization of the Transaction.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-2 Retrieval Request - Description for Use (continued)

ISO Message Reason Code	Retrieval Request Notification Reason	Description for Use
6016	Cardmember needs for personal records	Issuer is requesting Documentation on behalf of the Cardmember. The Cardmember is not disputing the Transaction, but needs Documentation for his/her records.
6304	ATM Journal Roll/Audit Tape Request	Issuer is requesting Documentation on behalf of the Cardmember. Cardmember is requesting a copy of the ATM Journal Roll/Audit Tape Request.

Table 7-3 Retrieval Request Notification Reasons

ISO Message Reason Code	Retrieval Request Notification Reason	Document Type - Function Code					
		Original ROC 600[13]	Copy ROC 603[13]	Substitute ROC 601	Itemized Documentation 602[3,7,8,11,10,14,15,16,17]	Transaction Log 606	Proof of Govt. ID Validation[5] 640
6003	Chargeback Documentation[1,3,6,7,12,14,15,16,17]	✓	✓	✓	✓	✓	✓
6006	Legal Request or Fraud Analysis[4,6,12,14,15,16,17]	✓	✓		✓	✓	✓
6008	Cardmember Requests Copy of ROC[3,6,7,8,9,10,12,14,15,16,17]		✓				✓
6013	Repeat Documentation Request[2,6,12,14,15,16,17]	✓	✓	✓	✓	✓	✓
6014	Cardmember does not recognize Transaction or Transaction Amount[6,9,12,14,15,16,17]	✓	✓	✓	✓	✓	✓
6016	Cardmember needs for personal records[11,12,17]			✓			✓
6304	ATM Journal Roll/Audit Tape Request	✓	✓	✓	✓	✓	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-3 Retrieval Request Notification Reasons (continued)

ISO Message Reason Code	Retrieval Request Notification Reason	Document Type - Function Code					
		Original ROC 600[13]	Copy ROC 603[13]	Substitute ROC 601	Itemized Documentation 602[3,7,8,11,10,14,15,16,17]	Transaction Log 606	Proof of Govt. ID Validation[5] 640

✓Document Type Required

1. If this reason is used, the intended Chargeback Reason must be indicated on the Retrieval Request Notification.
2. Retrieval Request Notification Reason Code 6013 may be used only if a prior Retrieval Request was done and Document Type is required.
3. For Transactions that qualify for the No Signature/No PIN Program, the following Retrieval Request Notification Reason Codes are invalid:
   - Retrieval Request 6003 when used with Chargeback "ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-Received" on page 352
   - Retrieval Request 6008 - Cardmember requests copy of ROC
   - Any Retrieval Request Message Reason Code when Itemized Documentation Code 01 "Signed Support" is requested through Function Code 602 Itemized Documentation
4. For Transactions that qualify for the ZIP Code Verification (ZCV) Program, Retrieval Request Notification Reason Code 6006 is invalid.
5. For Cash Disbursement Transactions, the Function Code (Document Type) Proof of Government ID Validation must be used.
6. For Expresspay Transactions performed by a Chip Card or Mobile Device, any Retrieval Request Notification Message Reason Code is invalid when used with the following Chargeback ISO Codes:
   - "ISO 4527 - Missing Imprint" on page 326
   - "ISO 4540 - Card Not Present" on page 330
   - "ISO 4544 - Cancellation of Recurring Goods/Services" on page 332
7. For Transactions that qualify for the American Express SafeKey Fraud Liability Shift (FLS), the following Retrieval Request Message Reason Codes are invalid:
   - Retrieval Request 6003 is invalid when used with Chargeback ISO Codes:
     - "ISO 4540 - Card Not Present" on page 330
     - "ISO 4763 - Fraud Full Recourse" on page 348
   - Retrieval Request 6008 - Cardmember requests copy bearing signature (signed support)
   - Any Retrieval Request Message Reason Code when Itemized Documentation Code 01 "Signed Support" is requested through Function Code 602 Itemized Documentation
8. For PIN-Authenticated Transactions, the following Retrieval Request Notification Reasons are invalid:
   - Retrieval Request 6008 - Cardmember requests copy of ROC
   - Any Retrieval Request Message Reason Code when Itemized Documentation Code 01 "Signed Support" is requested through Function Code 602 Itemized Documentation
   - Retrieval Request 6014 - Cardmember does not recognize Transaction or Transaction Amount
     - Issuers may use Retrieval Request Message Reason Code 6003 with Chargeback "ISO 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented" on page 309 to investigate Cardmember inquiries related to Transaction amounts.

     Note: For purposes of this Retrieval Request exclusion, a PIN Authenticated Transaction is defined as:

     - EMV Transactions - ICC Chip/PIN Indicator is "YY = Chip and PIN", or "YO = Transaction was Chip and Online PIN was used" in the POS First Presentment (1240) message
     - Magstripe Transactions - Point of Service Data Code Position 8 with a value of '1' in the POS Authorization Request (1100) message

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-3 Retrieval Request Notification Reasons (continued)

ISO Message Reason Code	Retrieval Request Notification Reason	Document Type - Function Code					
		Original ROC 600[13]	Copy ROC 603[13]	Substitute ROC 601	Itemized Documentation 602[3,7,8,11,10,14,15,16,17]	Transaction Log 606	Proof of Govt. ID Validation[5] 640

9. For Mail Order/Telephone/Internet Transactions, the following Retrieval Request Notification Reasons are invalid:
   - Retrieval Request 6008 - Cardmember requests copy of ROC
   - Any Retrieval Request Message Reason Code when Itemized Documentation Code 01 "Signed Support" is requested through Function Code 602 Itemized Documentation

     Note: For purposes of this Retrieval Request exclusion, a Mail Order/Telephone/Internet Transaction is defined as a Transaction where the Point of Service Data Codes in the POS First Presentment (1240) message indicate that both the Cardmember (Point of Service Data Code Position 5) and Card (Point of Service Data Code Position 6) were not present for the Transaction. Refer to the *Codes Reference Guide* for specific Point of Service Data Code values.
10. For Customer Activated Terminals (CAT) Transactions, the following Retrieval Request Notification Reasons are invalid:
    - Retrieval Request 6008 - Cardmember requests copy of ROC
    - Any Retrieval Request Message Reason Code when Itemized Documentation Code 01 = "Signed Support" is requested through Function Code 602 Itemized Documentation

      Note: For purposes of this Retrieval Request exclusion, a CAT Transaction is defined as a Transaction with a Point of Service Data Code Position 4 with a value of '2, 4,or 5' in the POS First Presentment (1240) message.
11. Retrieval Request Notification Reason 6016 - Cardmember needs for personal records is invalid with all Chargeback ISO Code Messages.
12. Any Retrieval Request Message Reason Code is invalid when used with the following Chargeback ISO Codes:
    - 4516 - Request for Support Not Fulfilled
    - 4517 - Request for Support Illegible/Incomplete
13. An Acquirer may provide either the original or a copy of the Record of Charge (ROC) in response to a request for an original ROC 600 or in response to a request for a copy ROC 603.
14. For all Digital Wallet Contactless-Initiated Transactions, the following Retrieval Request Notification Reason Codes are invalid:
    - Retrieval Request 6008 - Cardmember requests copy of ROC
    - Retrieval Request 6014 - Cardmember does not recognize Transaction or Transaction Amount
      - Issuers may use Retrieval Request Message Reasons Code 6003 with Chargeback ISO Code 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented to investigate Cardmember inquiries related to Transaction Amount.
    - Any Retrieval Request Message Reason Code is invalid when used with the following Chargeback ISO Codes:
      - 4527 Missing Imprint
      - 4540 Card Not Present
      - 4544 Cancellation of Recurring Goods/Services
      - 4798 Fraud Liability Shift – Counterfeit
      - 4799 Fraud Liability Shift – Lost/Stolen/Non-received

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-3 Retrieval Request Notification Reasons (continued)

ISO Message Reason Code	Retrieval Request Notification Reason	Document Type - Function Code					
		Original ROC 600[13]	Copy ROC 603[13]	Substitute ROC 601	Itemized Documentation 602[3,7,8,11,10,14,15,16,17]	Transaction Log 606	Proof of Govt. ID Validation[5] 640

15. For Digital Wallet Application-initiated Transactions, the following Retrieval Request Notification Reason Codes are invalid:
    - Retrieval Request 6008 - Cardmember requests copy of ROC
    - Retrieval Request 6014 - Cardmember does not recognize Transaction or Transaction Amount
        - Issuers may use Retrieval Request Message Reasons Code 6003 with Chargeback ISO Code 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented to investigate Cardmember inquiries related to Transaction Amount.
    - Any Retrieval Request Message Reason Code when Itemized Documentation Code 01 "Signed Support" is requested through Function Code 602 Itemized Documentation
    - Any Retrieval Request Message Reason Code is invalid when used with the following Chargeback ISO Codes:
        - 4527 Missing Imprint
        - 4540 Card Not Present
        - 4544 Cancellation of Recurring Goods/Services
        - 4798 Fraud Liability Shift – Counterfeit
        - 4799 Fraud Liability Shift – Lost/Stolen/Non-received
16. For Digital Wallet Magnetic Secure Transmission (MST) or Expresspay Mobile Transactions, the following Retrieval Request Notification Reason Codes are invalid:
    - When the Transaction qualifies for the No Signature/No PIN Program:
        - Retrieval Request 6008 - Cardmember requests copy of ROC
        - Any Retrieval Request Message Reason Code when Itemized Documentation Code 01 "Signed Support" is requested through Function Code 602 Itemized Documentation
    - Any Retrieval Request Message Reason Code is invalid when used with the following Chargeback ISO Codes:
        - 4527 Missing Imprint
        - 4540 Card Not Present
        - 4544 Cancellation of Recurring Goods/Services
        - 4798 Fraud Liability Shift – Counterfeit
        - 4799 Fraud Liability Shift – Lost/Stolen/Non-received
17. For MPQR Transactions, all Retrieval Request Notification Reason Codes are invalid.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.4.1 Fulfillment Notification Reason Codes

The following table lists available Fulfillment Notification reason codes and their corresponding descriptions:

Table 7-4. Fulfillment Notification Reason Codes

Fulfillment Notification Reason Code	Fulfillment Notification Reason Description
2700	Per Local Regulation, Proof of Government ID Validation Cannot be Provided (valid for Cash Disbursement Transactions only)
6300	Documentation Being Provided/To Follow (see below)
6301	Invalid Acquirer Reference Number
6302	Not Fulfilling
6303	Credit Previously Issued
6305	ATM Journal Roll Provided

Note: The purpose of the previous table is to facilitate the communication between the Issuer and Acquirer during the Retrieval Request process.

The AEGNS Network Disputes Manager user must also indicate if additional supporting Documentation is to follow, and the manner in which it is to be delivered (email, mail, facsimile, etc.). See the *Network Disputes Manager - User Guide.*



Refer to Section 7.3.2.14, "Documentation Delivery," on page 285 for additional information regarding delivery of Documentation.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.4.2 Itemized Documentation Codes

Itemized Documentation Codes must be used whenever a Retrieval Request or Fulfillment is done for Itemized Documentation (Function Code 602). The appropriate Itemized Documentation Code and its description must be input in the Comments field on the appropriate screen or Transaction form. If no Documentation is required, leave the Comments field blank.

Table 7-5. Itemized Documentation Codes

Code	Itemized Documentation Code Description
2 spaces	No Documentation required
00	Reserved
01	Signed support
02	Itemized support
03	Proof of delivery
04	Lodging folio
05	Copy of rental agreement
06	Copy of S/E's return policy
07	Copy of S/E's cancellation policy
08	Imprint
09	Acknowledgment of responsibility for car rental capital damages
10	Copy of membership contract
11	Chip Card Transaction Certificate
12	ATM Audit Tape/Journal Roll

Note: For Card Present Transactions, a Cardmember signature is not required in the Fulfillment, unless required by applicable law.

An Acquirer's failure to provide the Documentation requested through the Itemized Documentation code is not, in and of itself, grounds for an Issuer to submit a Chargeback ISO Code 4517 Request for Support Illegible/Incomplete. Refer to "ISO 4517 - Request for Support Illegible/Incomplete" on page 319 for processing requirements.

7.5 Fulfillment Data Requirements

The following tables indicate the data required on each type of Fulfillment Notification provided by the Acquirer. Failure to provide the indicated data may result in a Chargeback for "ISO 4517 - Request for Support Illegible/Incomplete" on page 319. See the *Codes Reference Guide* for Function Codes starting with series 600.

The Cardmember's Account number, which may be truncated and, if available the Card Expiration Date must be provided on all Fulfillments. See Section 4.2.21.1, "Completing Charge ROCs," on page 237.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.5.1 Fulfillment Data Requirement Tables

Table 7-6 Data Required on all Fulfillments, Regardless of Industry

All Industries	✓ Indicates Required Data ∗ Indicates if available				
Data Field	**Document Type - Function Code**				
	Original ROC 600[1]	**Copy ROC 603[1]**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Card Account number used to initiate Transaction (May be truncated)	✓	✓	✓	✓	✓
Cardmember Name	∗	∗	∗	∗	
Expiration Date	∗	∗	∗	∗	∗
Signature (Optional for Card Present, non-PIN-based Transactions, unless otherwise noted[2,3])	∗	∗		∗	
S/E Number	∗	∗	∗	∗	∗
S/E Name	✓	✓	✓	✓	✓
S/E Location	✓	✓	✓	✓	✓
Location Code (Store Number)	∗	∗	∗	∗	∗
Transaction Date	✓	✓	✓	✓	✓
Transaction Amount	✓	✓	✓	✓	✓
Approval Code	∗	∗	∗	∗	∗
Description of Merchandise/Services	∗	∗	∗	∗	∗
Merchandise Itemization				✓	
Transaction ID	∗	∗	∗	∗	∗
Proof of Government ID Validation[4]	✓	✓			

1. An Acquirer may provide either the original or a copy of the Record of Charge (ROC) in response to a request for an original ROC 600 or in response to a request for a copy ROC 603.
2. Transactions that qualify for the No Signature/No PIN Program do not require a signature.
3. Obtaining Cardmember signature on Card Present Transactions is optional to complete a ROC, and at the discretion of the S/E, unless required by applicable law. Signature must be obtained for the following Merchant Category Codes (MCCs):
   4829 - Wire Transfers and Money Orders
   6010 - Financial Institutions - Manual Cash Disbursements
   6051 - Non-Financial Institutions - Foreign Currency, Money Orders (not Wire Transfer), Scrip and Travelers Checks
4. Transactions that qualify for Cash Disbursements contain all information specified above for Original Record of Charge (ROC) (Function Code 600) together with Proof of Government ID Validation (Function Code 640), in accordance with local regulation.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-7 Data Required for Airline Industry

Documentation Data-Airline Industry					✓ Indicates Required Data
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Carrier IATA (by leg)	✓	✓	✓	✓	
Fare Basis (by leg)	✓	✓	✓	✓	
Ticket Number (by leg)	✓	✓	✓	✓	
Departure Date (by leg)	✓	✓	✓	✓	
Airport Code (by leg)	✓	✓	✓	✓	
Travel Agency (IATA, ARC)	✓	✓	✓	✓	
Ticket "Mailed To" Address			✓	✓	

Table 7-8 Additional Data Required for Car Rental Industry

Documentation Data-Car Rental Industry					✓ Indicates Required Data
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Rental Agreement Number	✓	✓	✓	✓	
Rental Agent ID Number				✓	
Cardmember Address				✓	
Pick-Up Location (City, State)			✓	✓	
Pick-Up Date			✓	✓	
Return Location (City, State)			✓	✓	
Return Date			✓	✓	
Type of Vehicle				✓	
Mileage				✓	
Refueling Charge				✓	
Insurance Charge				✓	
Rental Rate				✓	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-8 Additional Data Required for Car Rental Industry (continued)

Documentation Data-Car Rental Industry	✓ Indicates Required Data				
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Actual Rate Charges				✓	
Charge Adjustments			✓	✓	
Tax				✓	
Method of Billing				✓	
Parking Ticket/Moving Violation				✓	

Table 7-9 Additional Data Required for Lodging Industry

Documentation Data-Lodging Industry	✓ Indicates Required Data				
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Guest Name	✓	✓	✓	✓	
Folio Number	✓	✓	✓	✓	
Check-In Date			✓	✓	
Checkout Date			✓	✓	
Room Rate			✓	✓	
Tax			✓	✓	
Incidental Charges			✓	✓	
No Show Reservation Indicator			✓	✓	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-10 Additional Data Required for Restaurant Industry

Documentation Data-Restaurant Industry				✓ Indicates Required Data	
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Food/Beverage Total Amount	✓	✓	✓	✓	
Tip Amount	✓	✓	✓	✓	

Table 7-11 Additional Data Required for Communication Industry

Documentation Data-Communication Industry				✓ Indicates Required Data	
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Call From City, State/ Country			✓	✓	
Call From Number			✓	✓	
Call To City, State/ Country			✓	✓	
Call To Number			✓	✓	
Duration of Call			✓	✓	
Time of Call			✓	✓	
Rate Class			✓	✓	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-12 Additional Data Required for ATM Transactions

Documentation Data-ATM Transactions	✓ Indicates Required Data				
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Network Route and Transit Number					✓
Network Name					✓
Transaction Time					✓
Transaction Audit Tape Detail					✓
ATM Location (City, State)					✓
Terminal ID					✓

Table 7-13 Additional Data Required for Mail Order/Telephone Order/Internet Order

Documentation Data-Mail Order/Telephone Order/Internet Order	✓ Indicates Required Data				
Data Field	**Document Type - Function Code**				
	Original ROC 600	**Copy ROC 603**	**Substitute ROC 601**	**Itemized Documentation 602**	**Transaction Log 606**
Shipping Date	✓	✓	✓	✓	
Shipping Address	✓	✓	✓	✓	
AAV Response Code	✓	✓	✓	✓	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.6 Second Presentment Data Requirements

When an Acquirer submits a Second Presentment to an Issuer, a Message Reason Code is required to indicate why the Second Presentment is being sent.

Table 7-14 Second Presentment Message Reason Codes

ISO Message Reason Code	Reason for a Second Presentment
2000	General - invalid Chargeback
2001	Invalid Acquirer Reference Number on Chargeback
2002	Non-receipt of required Documentation to support Chargeback
2003	Correct Transaction Date provided
2004	Correct Merchant description provided (DBA)
2005	Correct Merchant location provided
2006	Incorrect Transaction Date provided on Chargeback
2007	Transaction did not exceed Network Floor Limit
2008	Transaction Authorized by Issuer
2009	No error in addition of sale - amount correct in original Transaction
2010	No proof of altered amount (customer stated in Chargeback that amount had been altered)
2011	Credit previously issued
2012	Original Transaction was valid
2700	Per Local Regulation, Proof of Government ID Validation Can Not Be Provided (valid for Cash Disbursement Transactions only)
2701	Valid ATM Journal Roll/Audit Tape Provided

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.7 Compelling Evidence

The Acquirer can file a Second Presentment if the Acquirer can demonstrate that the Cardmember engaged in the Transaction by providing one (1) of the following:

Table 7-15 Compelling Evidence as a Second Presentment Responsibility

Chargeback ISO Code	Compelling Evidence
ISO 4540 - Card Not Present	1. For Transactions involving the shipment of Goods or Services, proof that the Transaction contains a shipping address that matches a previously used shipping address from an undisputed Transaction. 2. For airline or passenger transportation Transactions, one (1) of the following: a. Evidence the Cardmember participated in the flight or transportation (e.g., scanned boarding pass or passenger manifest) b. Credits of frequent-flier miles or loyalty point program for the flight or travel in question, showing a direct connection to the Cardmember c. Proof of receipt of the flight or transportation ticket at the Cardmember's billing address d. Proof that the Transaction contains the designated passenger name that matches a previously used passenger name from an undisputed Transaction 3. For E-commerce Transactions involving the sale of Digital Goods or Services, provide all of the following: a. Cardmember name linked to the account with the Merchant b. Description of the Goods or Services, and the date/time they were purchased and downloaded, accessed by, or provided to the Cardmember c. Proof that the device and Card used for the disputed Transaction was used in a previous, undisputed Transaction. In addition, provide the following information that is currently linked to the Cardmember account with the Merchant: i. Device ID ii. IP address and geographical location iii. Device name (if available) **Note:** In addition, provide three (3) or more of the following: d. Proof that the Merchant validated the Card and the Cardmember prior to or at the time of purchase (e.g., AAV (Automated Address Verification) verification response of "Y" or PCSC (Printed Card Security Code) verification response of "Y") e. Proof that the customer's account with the Merchant was accessed by the customer and successfully verified by the Merchant on or before the Transaction date f. Proof that the Cardmember password or CDCVM was captured by the Merchant in order to complete the Transaction g. Cardmember phone number and/or email address linked to the customer profile held by the Merchant 4. For Recurring Billing Transactions, all of the following must be provided: a. Proof of a legally binding contract held between the Merchant and the Cardmember b. Proof the Cardmember accessed the Merchant's website or application to establish Services on or before the Transaction date c. Proof the Cardmember received the Goods or Services d. Proof of a previous Transaction that was not disputed. *ISO 4540 is continued on the next page.*

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-15 Compelling Evidence as a Second Presentment Responsibility (continued)

Chargeback ISO Code	Compelling Evidence
ISO 4540 - Card Not Present (cont'd)	5. For Transactions involving the sale of website search and/or advertising Services to promote consumer products or Services, all of the following must be provided: a. Proof of a legally binding contract held between the Merchant and the Cardmember b. Details of the initial ad-service setup, including at least two (2) of the following items: i. Purchaser's IP address and geographical location at the date and time of the initial ad-service setup ii. Email address of purchaser iii. Company name or purchaser name c. Proof the Cardmember has accessed the Merchant's website to establish Services on or before the Transaction date d. Proof that the device and Card used for the disputed Transaction was used in a previous, undisputed Transaction. In addition, provide the following information that are currently linked to the Cardmember account with the Merchant: i. Device ID ii. IP address and geographical location iii. Device name (if available) e. Proof that the Cardmember received the Goods or Services f. Description of the Goods or Services and the date they were provided.
ISO 4554 - Goods and Services Not Received	1. For Transactions involving the shipment of Goods or Services, evidence to prove that there is a link between the Person who received the Goods or Services and the Cardmember (e.g., photographs, emails). 2. For airline or passenger transportation Transactions, one (1) of the following: a. Evidence the Cardmember participated in the flight or transportation (e.g., scanned boarding pass or passenger manifest) b. Credits of frequent-flier miles or loyalty point program for the flight or travel in question, showing a direct connection to the Cardmember c. Proof the flight in question was available during airline bankruptcy proceedings d. Additional Transactions related to the original Transaction, such as seat upgrades, baggage payment, or purchases made on board the aircraft or transportation vehicle e. Itemized invoice for associated charges 3. For E-commerce Transactions representing the sale of Digital Goods or Services downloaded, accessed by or provided to the Cardmember, one (1) of the following must be provided: a. Proof that the Cardmember's IP address at the time of the purchase matches the IP address where the Digital Goods were downloaded b. Proof the Cardmember's email address provided at the time of the purchase matches the email address used to deliver the Digital Goods c. Proof that the S/E's website was accessed by the Cardmember for Digital Services after the Transaction date **Note:** In addition, the Acquirer can also provide one (1) of the following: a. Description of the Digital Goods b. Date and time the Digital Goods were downloaded or accessed. 4. For Card Not Present Transactions where the Goods are picked up at the S/E Location, the Acquirer must provide the Cardmember or authorized third-party signature on the pick-up form as well as additional proof to demonstrate that the identity of the Cardmember or authorized third party was verified at the time of pick-up.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.8 Process Timeframes

All timeframes that follow are measured in calendar days unless otherwise specified. The Network Processing Date is day zero for the purpose of counting Chargeback timeframes.

Table 7-16 Process Timeframes

Process Step	Associated Timeframes
Authorization	The life span of an Authorization is seven (7) days. If held longer than seven (7) days after the date the original Authorization was obtained, the Transaction must be re-Authorized to avoid possible Chargeback consequences. This Authorization life span does not apply to lodging, cruise line, or car rental Transactions, and Expresspay Transactions at Transit Access Terminals (TATs). For more information, refer to: • Section 4.2.19.1, "Lodging," on page 227 • Section 4.2.19.2, "Cruise Lines," on page 227 • Section 4.2.19.3, "Car Rental," on page 227 • Section 4.2.9.1.2, "Authorization Requirements for Expresspay Transactions at TATs," on page 219 • If the original Authorization was granted by an AEIPS or Expresspay-compliant application on a Chip Card, a new Authorization must be obtained directly from the Issuer
Presentment	Presentment must be made within timeframes specified in this manual. Refer to Section 2.9.12, "Acquirer Transaction Processing Requirements," on page 102. **Note:** Exceeding the specified timeframes alone is not grounds for Chargeback.
Retrieval Request	The Acquirer must accept and fulfill requests for Documentation for a period of one (1) year (or as required by local law) following the Network Processing Date of the Presentment. To meet this requirement, the Acquirer is required to fulfill for a maximum of 395 days from the Network Processing Date of the Transaction. A Retrieval Request for a Transaction Certificate may not be initiated on a Transaction for which a Chip Card Addendum (9240) message was submitted with the First Presentment. **Note:** Failure of an Acquirer to fulfill requests for Documentation within a one (1) year period is not a basis for a Chargeback or Compliance Filing unless all the criteria for a Chargeback or Compliance Filing are met.
Documentation	For Transactions processed via AEGNS Network Disputes Manager, supporting Documentation must be attached to the Transaction at the time it is submitted through AEGNS Network Disputes Manager. When providing supporting Documentation, Participants should ensure that the supporting Documentation is legible and contains full details as requested by AEGNS or the other Participant. Participants must use the AEGNS Network Disputes Manager Documents Only function to send supporting Documentation for disputed Transactions processed via the AEGNS infrastructure. Supporting Documentation must be sent through AEGNS Network Disputes Manager within twenty-four (24) hours from the time that the Transaction is sent through the AEGNS infrastructure.
Fulfillment Notification	Fulfillment Notification must be provided by the Acquirer within thirty (30) days from the Network Processing Date of the Retrieval Request Notification. Acquirers that do not send the required Fulfillment Notification in response to a Retrieval Request will have limited Second Presentment rights (refer to "ISO 4516 - Request for Support Not Fulfilled" on page 317).
First Chargeback	A First Chargeback must be sent within the timeframes specified in the individual ISO Chargeback Codes.
Second Presentment	A Second Presentment must be sent to the Network within forty-five (45) days from the Network Processing Date of the First Chargeback.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-16 Process Timeframes (continued)

Process Step	Associated Timeframes
Final Chargeback	A Final Chargeback must be sent to the Network within forty-five (45) days from the Network Processing Date of the Second Presentment.
Good Faith	Good Faith Transactions, by their nature, are not subject to normal Transaction life cycle timeframes.
Arbitration	An Arbitration Filing must be submitted through AEGNS Network Disputes Manager with all related Documentation within forty-five (45) days from the Network Processing Date of the Final Chargeback.
Pre-Compliance	All pre-Compliance correspondence and Documentation must be sent to the receiving Participant at least thirty (30) days prior to submitting a Compliance Filing.
Compliance	For violations involving a Transaction, the Compliance Filing must be submitted through AEGNS Network Disputes Manager within 180 days from the Network Processing Date of the Presentment. For any violations not involving a Transaction, the Compliance Filing must be submitted through AEGNS Network Disputes Manager within 180 days from the date the violation occurred.

7.9 Chargeback Policy Rules

Issuers and Acquirers are required to adhere to all applicable Chargeback policy rules. This section details the following:

- A description of Chargeback Types, including specific requirements relating to Fraud Chargebacks.
- Chargeback Reasons "At A Glance." See Table 7-17, "Chargeback Reasons," on page 306.
- A description of the Chargeback format, followed by Chargeback ISO Message Reason Codes listed in numerical order.

7.9.1 Retrieval Chargeback Types

Retrieval Chargebacks provide the Issuer rights to transfer liability to an Acquirer when Documentation requested by the Issuer in support of an intended Chargeback is unfulfilled, illegible, or missing vital data. Refer to:

- "ISO 4516 - Request for Support Not Fulfilled" on page 317
- "ISO 4517 - Request for Support Illegible/Incomplete" on page 319

7.9.2 Authorization Chargeback Types

The Authorization Chargeback provides the Issuer rights to transfer liability to an Acquirer when there are discrepancies between the Network's Authorization policies and the manner in which Authorization was carried out. Refer to:

- "ISO 4521 - Invalid Authorization" on page 321

7.9.3 Processing Error Chargeback Types

Processing Error Chargebacks provide the Issuer rights to transfer liability to an Acquirer when errors occur at the POS or at the Acquirer's data processing center. Refer to:

- "ISO 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented" on page 309
- "ISO 4512 - Multiple Processing" on page 311
- "ISO 4523 - Unassigned Cardmember Account Number" on page 325

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- "ISO 4530 - Currency Discrepancy" on page 327
- "ISO 4536 - Late Presentment" on page 329
- "ISO 4752 - Credit/Debit Presentment Error" on page 343

7.9.4 Cardmember Dispute Chargeback Types

Cardmember Dispute Chargeback types provide the Issuer rights to transfer liability to an Acquirer where the Cardmember has raised issues that either cause the Cardmember to withhold payment for such Transactions or claim that Credit is due to the Cardmember's Account. Refer to:

- "ISO 4513 - Credit Not Presented" on page 312
- "ISO 4515 - Paid Through Other Means" on page 316
- "ISO 4544 - Cancellation of Recurring Goods/Services" on page 332
- "ISO 4553 - Not as Described or Defective Merchandise" on page 334
- "ISO 4554 - Goods and Services Not Received" on page 337
- "ISO 4750 - Car Rental Charge Non-Qualified or Unsubstantiated" on page 341
- "ISO 4754 - Local Regulatory/Legal Dispute" on page 344

7.9.5 Fraud Chargeback Types

Fraud Chargebacks provide the Issuer with rights to transfer liability to an Acquirer according to the specific conditions of the applicable Chargeback rule, and after reporting the incident of Confirmed Fraud to AEGNS. Refer to:

- "ISO 4527 - Missing Imprint" on page 326
- "ISO 4534 - Multiple ROCs" on page 328
- "ISO 4540 - Card Not Present" on page 330
- "ISO 4755 - No Valid Authorization" on page 345
- "ISO 4763 - Fraud Full Recourse" on page 348
- "ISO 4798 - Fraud Liability Shift - Counterfeit" on page 350
- "ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-Received" on page 352

7.9.5.1 Fraud Data Entry Requirement

If an Issuer experiences an instance of Confirmed Fraud, the Issuer must manually enter the fraud Transaction into the WFIS or electronically transmit it into the GNS Fraud Repository before filing a Fraud Chargeback. The GNS Fraud Repository is described in the "Security and Fraud" chapter beginning on page 375.

7.9.5.2 Counterfeit Card Chargeback Restriction

Issuers may not Chargeback Acquirers for losses incurred through the use of counterfeit Cards or Cards issued on Fraudulent Applications that appeared to be, and were accepted as, legitimate Cards, providing all other Card acceptance procedures were followed by the S/E except when the Transaction qualifies under Section 7.10.8.1, "AEIPS Fraud Liability Shift (FLS)," on page 359. "ISO 4763 - Fraud Full Recourse" on page 348 continues to allow Issuers the right to transfer liability of eligible fraud types to the Acquirer for Transactions that meet the requirements of this Chargeback.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.9.6 Chargeback Reasons "At A Glance"

The ISO Message Reason Code is utilized to process Chargebacks on the Network. Table 7-17, "Chargeback Reasons," on page 306 lists each Chargeback reason and indicates whether the Chargeback may be used with POS or ATM Transactions, whether a Retrieval Request is required, and if Issuer Support is required.

Additional information includes the page number for easy reference, Minimum Chargeback Amount, in U.S. Dollars, applicable to the Chargeback, and Chargeback timeframes.

Table 7-17 Chargeback Reasons

ISO Message Reason Code	Page No.	POS	ATM	Retrieval Required	Issuer Support	Minimum Amount	Time Frames (Days)
Retrieval Chargeback Types							
ISO 4516 - Request for Support Not Fulfilled	317	✓	✓	✓		$0	120
ISO 4517 - Request for Support Illegible/Incomplete	319	✓	✓	✓	✓	$0	120
Authorization Chargeback Types							
ISO 4521 - Invalid Authorization	321	✓			✓	$0	120
Processing Error Chargeback Types							
ISO 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented	309	✓			✓	$25	120
ISO 4512 - Multiple Processing	311	✓			✓	$25	120
ISO 4523 - Unassigned Cardmember Account Number	325	✓				$25	120
ISO 4530 - Currency Discrepancy	327	✓	✓		✓	$25	120
ISO 4536 - Late Presentment	329	✓			✓	$25	120
ISO 4752 - Credit/Debit Presentment Error	343	✓			✓	$25	120
Cardmember Dispute Chargeback Types							
ISO 4513 - Credit Not Presented	312	✓			✓	$25	120
ISO 4515 - Paid Through Other Means	316	✓			✓	$25	120
ISO 4544 - Cancellation of Recurring Goods/Services	332	✓			✓	$0	120
ISO 4553 - Not as Described or Defective Merchandise	334	✓			✓	$25	120
ISO 4554 - Goods and Services Not Received	337	✓	✓	For ATM Dispense Only	✓	$25	POS 120 ATM 45
ISO 4750 - Car Rental Charge Non-Qualified or Unsubstantiated	341	✓			✓	$25	120
ISO 4754 - Local Regulatory/Legal Dispute	344	As prescribed by the applicable law.			✓	$25	120

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 7-17 Chargeback Reasons (continued)

ISO Message Reason Code	Page No.	POS	ATM	Retrieval Required	Issuer Support	Minimum Amount	Time Frames (Days)
Fraud Chargeback Types							
ISO 4527 - Missing Imprint	326	✓			✓	$25	120
ISO 4534 - Multiple ROCs	328	✓			✓	$25	120
ISO 4540 - Card Not Present	330	✓		1	✓	$25	120
ISO 4755 - No Valid Authorization	345	✓			✓	$0	120
ISO 4763 - Fraud Full Recourse	348	✓			✓	$0	120
ISO 4798 - Fraud Liability Shift - Counterfeit	350	✓			✓	$0	120
ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-Received	352	✓			✓	$0	120

1. A Retrieval Request is not required if the Issuer can comply with applicable Issuer Support requirements.

7.9.7 Description of the Chargeback Format

ISO Code - A 4-Digit Message Reason Code for the Chargeback

Chargeback Type	A description of the type of Chargeback.
Chargeback Reason	The specific Network policy violated or the reason for Cardmember complaint.
Description	A detailed description of the issue or circumstance which caused the dispute by the Issuer or Cardmember.
POS/ATM Eligibility	Specifies whether ATM, POS, or both types of Transactions may be processed under this rule.
Excluded Transactions	The circumstances that would exclude certain POS or ATM Transactions from being processed under this rule.
Minimum Amount	The smallest amount in U.S. Dollars that may be disputed.
Chargeback Maximum Time to File	Total number of days following the Network Processing Date of the original Transaction (or other timeframe where specified) during which time the Issuer may file the Chargeback with the Network. The Network Processing Date is day zero for the purpose of counting Chargeback timeframes.
Conditions	If multiple conditions are listed and prefaced by "The Issuer must meet all of the following conditions," all conditions must be met. Otherwise, only one (1) single condition applies.
Retrieval Required	Specifies if a Retrieval Request is necessary before the Chargeback may be processed.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO Code - A 4-Digit Message Reason Code for the Chargeback

Issuer Support	Denotes legible (e.g., typed) Documentation and/or information that must be submitted by the Issuer to the Acquirer as support for a Chargeback. Cardmember Documentation or Issuer Declaration are common terms found in the Issuer Support sections. These terms are defined in the "Definitions" chapter beginning on page 495, however, examples of Cardmember Documentation or Issuer Declaration include: Cardmember Documentation: • Letters, facsimiles, or emails from the Cardmember to the Issuer, or • Letters, facsimiles, or emails from the S/E to the Cardmember, or • Attestations made by the Cardmember to the Issuer in a secure online environment that is maintained by the Issuer. Issuer Declaration: • A statement by the Issuer that attests to certain actions that were taken by that Issuer or Cardmember, or • Notes or logs from Issuer case management systems.
Second Presentment Acquirer Responsibility	If multiple items are listed and prefaced by "One (1) or more of the following items must be provided," then the Acquirer must provide the appropriate items to support its claim that the Chargeback is invalid.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented

Chargeback Type	Processing Error Chargeback
Chargeback Reason	Either of the following: • The Presentment amount differs from the original Transaction amount, or • The Issuer identifies the Primary Account Number (PAN) on the Transaction does not match the PAN on the Presentment.
Description	The Issuer may charge back a Transaction using this Chargeback ISO Code under one (1) of the following circumstances: 1. The Presentment amount: a. Differs from the original Transaction amount, or b. Contains an addition or transposition error and the Presentment was sent with the incorrect amount, or c. Differs from the Cardmember's copy of the ROC and the Cardmember denies authorizing any change to the Transaction Amount. 2. The Issuer receives a Presentment for a PAN that does not match the PAN on the Transaction. The PAN in the Presentment contains the Issuer's Identification Number and a valid check digit. 3. For MPQR Transactions, the Transaction amount differs from purchase amount (the cost of the Goods and Services).
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from being processed under this ISO Code: 1. For Chargebacks processed under Chargeback Description one (1) of this ISO Code: a. Legitimate Delayed Billing charges submitted by car rental, cruise line, and lodging S/Es. 2. For Chargebacks processed under Chargeback Description two (2) of this ISO Code: a. Authorized Transactions where the full magnetic stripe was sent to the Issuer with the Authorization Request, or b. Chip Card Transactions where the validated Transaction Certificate is provided in the First Presentment.
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.
Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. For Chargebacks processed under Chargeback Description one (1) of this ISO Code: a. A handwritten amount on the Cardmember copy of the ROC or Itemized Documentation will take precedence in determining the correct Transaction amount. b. The amount to be charged back is limited to the difference between the correct amount and the incorrect Presentment amount.
Retrieval Required	No

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4507 - Incorrect Transaction Amount or Primary Account Number (PAN)

Issuer Support	The Issuer must provide the following to support a Chargeback processed under this ISO Code: 1. For Chargebacks processed under Chargeback Description one (1), two (2), or three (3) of this ISO Code: a. An Issuer Declaration that indicates the Chargeback Description that the Chargeback is processed under. 2. As applicable, the Issuer must also provide the following for processed under: a. Chargeback Description 1c of this ISO Code - Cardmember Documentation describing the alteration and a copy of the Cardmember's ROC. b. Chargeback Description two (2) of this ISO Code - Documentation that confirms the PAN on the Transaction did not match the PAN in the Presentment. c. Chargeback Description three (3) of this ISO Code - Cardmember Documentation that shows the Transaction amount is different from the purchase amount. **Note:** While a Retrieval Request is not required for this ISO Code, a copy of the ROC may be necessary to satisfy the Issuer Support requirement number two (2).
Second Presentment Acquirer Responsibility	The Acquirer must provide one of the following in order to support a Second Presentment. 1. For Chargebacks processed under Chargeback Description one (1) or two (2) of this ISO Code, either: a. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed, or b. Proof that the Transaction falls into one (1) of the excluded Transaction types. 2. As applicable, the Acquirer can also provide one of the following to support a Second Presentment. For Chargebacks processed under: a. Chargeback Description one (1) of this ISO Code: Proof that the Transaction amount is correct (e.g., copy of the itemized ROC or the ROC combined with itemized Documentation showing the breakdown of charges). b. Chargeback Description one (1) of this ISO code. For instances where the Cardmember denies authorizing a change in the Transaction Amount, the Acquirer must provide either: i. Proof the Transaction amount was not altered, or ii. Proof the Cardmember approved the altered amount. c. For Chargebacks processed under Chargeback Description two (2) of this ISO Code, either: i. A copy of the imprinted slip, which confirms the PAN, or ii. A copy of the receipt from the POS terminal, which read the PAN from the magnetic stripe. d. For Chargebacks processed under Chargeback Description three (3) of this ISO Code: i. Proof that the Transaction amount is correct and the same as the purchase amount. **Note:** For Chargebacks processed under Chargeback Description two (2) of this ISO Code, the Acquirer may accept the Chargeback and send a new First Presentment with a corrected PAN if the Acquirer has the corrected PAN. This new Transaction will be subject to Late Presentment policy. See "ISO 4536 - Late Presentment" for additional information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4512 - Multiple Processing

Chargeback Type	Processing Error Chargeback
Chargeback Reason	A single Transaction for the same amount was sent for payment multiple times.
Description	1. The Cardmember claims that a single Transaction appears more than once on his/her statement. 2. The Issuer suspects that a single Transaction has been sent for payment more than once.
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Airline, cruise line, and lodging industry cases involving voided tickets that are pending Credit and which were reissued for a different itinerary. 2. Airline, cruise line, and lodging vouchers or tickets with different voucher or ticket numbers.
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.
Conditions	The Transaction that was sent first shall be considered the valid Transaction.
Retrieval Required	No
Issuer Support	If the Acquirer's Reference Number for each of the Transactions is provided in the Presentment it must be provided with the Chargeback. If one (1) Acquirer is involved, the Issuer supplies support for the multiple Transactions processed. If two (2) Acquirers are involved, then the Issuer supplies a copy of the valid Transaction to the Acquirer being charged back.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof to support multiple valid Transactions. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 3. Proof that the Transaction falls into one (1) of the excluded Transaction types (e.g., copy of airline tickets, scanned boarding passes, or passenger manifest(s) etc.).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4513 - Credit Not Presented

Chargeback Type	Cardmember Dispute Chargeback
Chargeback Reason	Any of the following: • Cardmember received written acknowledgment of a Credit due to the Card Account from the S/E, but the Issuer has not received a Credit that it can post to the Cardmember's Account, or • Goods or Services were cancelled, refused, or returned in compliance with the S/E's policy but a Credit was never received by Cardmember, or • The Cardmember was incorrectly billed for a No Show Reservation or Advance Deposit Transaction and a Credit was not received by the Cardmember. • For Installment Payment Provider Transactions, the Cardmember has received a written acknowledgment of a Credit due from the End Beneficiary, but has not been refunded installments or is charged additional installments.
Description	The Issuer may charge back a Transaction using this Chargeback ISO Code under one (1) of the following circumstances: 1. The Cardmember received written acknowledgment of a Credit due to the Card Account from the S/E, but the Issuer has not received a Presentment of Credit from the Acquirer that it can post to the Cardmember's Account. 2. In compliance with the stated policy of the S/E or any applicable laws or regulations, the Cardmember: a. Cancelled an order for Goods or Services, or b. Refused delivery for Goods or Services, or c. Returned Goods that have been received, and **Note:** The Issuer has not received a Presentment of Credit from the Acquirer that it can post to the Cardmember's Account. 3. The Cardmember was incorrectly billed for: a. A No Show Reservation Transaction[1], or b. An Advance Deposit or Payment[2], and **Note:** The Issuer has not received a Presentment of Credit from the Acquirer that it can post to the Cardmember's Account. 4. For Installment Payment Provider Transactions, the Cardmember has received a written acknowledgment of a Credit due from the End Beneficiary, but has not been refunded installments or is charged additional installments.
POS/ATM Eligibility	POS only
Excluded Transactions	None
Minimum Amount	$25
Chargeback Maximum Time to File	Either: • 120 days from the date Goods or Services were cancelled, refused, or returned by Cardmember, or • 120 days from the date of the S/E's written acknowledgment of credit due, or • 120 days from the Network Processing Date of the Presentment.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4513 - Credit Not Presented (continued)

Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. The Issuer must wait fifteen (15) days from the following before processing the Chargeback: a. The date of the S/E's written acknowledgment of credit, or b. The date the Cardmember returned, refused, or cancelled the Goods or Services. 2. The amount to be charged back is limited to the amount of the unprocessed credit of the No Show Reservation or Advance Deposit Transaction Amount or Goods and Services returned or cancelled. 3. In addition, and as applicable, the following conditions also exist for Chargebacks processed under: a. Chargeback Description two (2) of this ISO Code - The Issuer must ensure the Cardmember made a Good Faith attempt to: i. Return the Goods, or cancel the order(s) for Goods or Services, and receive Credit from the S/E. b. For Installment Payment Provider Transactions, the Cardmember has received a written acknowledgment of a Credit due from the End Beneficiary, but has not been refunded installments or is charged additional installments.
Retrieval Required	No

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4513 - Credit Not Presented (continued)

Issuer Support	The Issuer must provide the following: 1. For Chargebacks processed under Chargeback Description one (1), two (2), or three (3) of this ISO Code: a. Issuer Declaration that indicates the Chargeback Description that the Chargeback is being processed under, or b. Cardmember Documentation that a Presentment of Credit has not been received from the Acquirer that the Issuer can post to the Cardmember's Account. 2. As applicable, the Issuer must also provide the following for Chargebacks processed under this ISO code: a. Chargeback Description one (1) of this ISO Code: i. Documentation indicating that a Credit has been issued to the Cardmember (i.e., Credit ROC, S/E letter acknowledging credit, statement of credit), or ii. Documentation of S/E Authorization of Chargeback. b. Chargeback Description two (2) of this ISO Code: i. If the order for Goods or Services were cancelled - The Issuer must provide cancellation details including the cancellation date and any cancellation reference number, or ii. If the Goods or Services were refused - The Issuer must provide the Cardmember's Documentation or Issuer Declaration that the Cardmember refused the Goods or Services in accordance with the S/E's stated cancellation policy or applicable laws or regulations. The Cardmember Documentation or Issuer Declaration must state the date of refusal and method of refusal, or iii. If the Goods or Services were returned - The Issuer should provide proof that Cardmember returned Goods to S/E. If proof of return is not available, provide specific details of the return or attempted return including date, method, and any other relevant information (e.g., mode of return, return address, tracking number, etc.). c. Chargeback Description three (3) of this ISO Code: i. Cardmember Documentation that proves the Cardmember cancelled a reservation but was charged for either the No Show Reservation or Advance Deposit Transaction. For example, a valid cancellation number or contact name or phone bill as evidence of contact with the S/E. **Note:** The Cardmember's cancellation must be in compliance with the cancellation policy of the S/E. ii. Cardmember Documentation that proves the Cardmember received Services at either the same location or a different location within the specified timeframe of the No Show Reservation Transaction[1]. iii. Proof of Services refused by the S/E but Advance Deposit or Payment charged[2].

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4513 - Credit Not Presented (continued)

Second Presentment Acquirer Responsibility	The Acquirer must provide the following for Chargebacks processed under this Chargeback ISO Code to support a Second Presentment. For Chargebacks processed under: 1. Chargeback Description one (1), two (2), or three (3) of this ISO Code: a. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed, or b. Proof that instead of the Credit the S/E provided substitute Goods or Services that were accepted by the Cardmember. 2. As applicable, the Acquirer can also provide the following to support a Second Presentment. For Chargebacks processed under: a. Chargeback Description two (2) or four (4) of this ISO Code - One (1) of the following must be provided: i. If the Goods are claimed to be returned - The Acquirer must provide proof refuting Cardmember's claim that Goods were returned to the S/E or End Beneficiary, or ii. If the Goods or Services are claimed to be cancelled, refused, or returned - The Acquirer must show in writing: • That the S/E provided its cancellation/return policy to the Cardmember at the time of the purchase, and, • That the Cardmember did not comply with the S/E's clearly documented cancellation or return policy which was provided to the Cardmember at the time of the purchase. b. Chargeback Description three (3) of this ISO Code - One (1) of the following must be provided: i. Proof that the Cardmember-supplied evidence is incorrect or inaccurate, or ii. Proof that otherwise supports the validity of the No Show Reservation or Advance Deposit claim.

1. Refer to Section 4.2.20.1, "No Show Reservations Program," on page 229 for eligibility requirements.
2. Refer to Section 4.2.20.3, "Advance Deposit or Payment Program," on page 231 for eligibility requirements.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4515 - Paid Through Other Means

Chargeback Type	Cardmember Dispute Chargeback
Chargeback Reason	Cardmember was billed for a Charge, which was settled through other means.
Description	The Issuer may charge back a Transaction using this Chargeback ISO code under one (1) of the following circumstances: 1. After having offered his/her Card for payment of a Transaction, the Cardmember later decided to settle the obligation through other means. The S/E provided a receipt to the Cardmember for the preferred payment method and the Cardmember assumed that the earlier Card Transaction would be cancelled. This same Transaction was sent for payment and appears on the Cardmember statement. 2. While trying to pay an End Beneficiary using an Indirect Acceptor, the Cardmember or End Beneficiary receive an error and, believing the Transaction was unsuccessful, the Cardmember decides to settle the obligation with the End Beneficiary though other means.
POS/ATM Eligibility	POS only
Excluded Transactions	None
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.
Conditions	None
Retrieval Required	No
Issuer Support	Proof of payment by other means, which can be clearly linked to the disputed Transaction.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Cardmember payment was not related to the disputed Transaction. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4516 - Request for Support Not Fulfilled

Chargeback Type	Retrieval Chargeback
Chargeback Reason	Either of the following: • The Issuer raised a Retrieval Request Notification (1642) message and the Acquirer did not provide Fulfillment Notification within thirty (30) days from the Network Processing Date of the Retrieval Request notification, or • The Issuer raised a Retrieval Request message and the Acquirer provided Fulfillment Notification indicating not fulfilling.
Description	Issuer may charge back a Transaction using this ISO Code under one (1) of the following circumstances: • The Acquirer has failed to provide the Issuer with a Fulfillment Notification within required timeframe, or • The Acquirer notified the Issuer in the Fulfillment Notification that the required Documentation will not be forthcoming.
POS/ATM Eligibility	POS and ATM
Excluded Transactions	The following Transactions are excluded from being processed under this ISO Code: 1. Transactions where the Retrieval Request was initiated using Reason Code 6016 Cardmember needs for personal records. 2. Transactions that qualify under the No Signature/No PIN Program. Refer to Section 4.2.20.4, "No Signature/No PIN Program," on page 232. 3. Expresspay, Expresspay Mobile, or Digital Wallet Contactless-Initiated Transactions, where the Transaction amount is less than or equal to the country threshold for Expresspay Transactions as indicated in the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide* available on Knowledge Base. 4. AEIPS PIN Digital Wallet Contactless-Initiated and Digital Wallet Application-Initiated Transactions where the Retrieval Request was initiated using Reason Code 6006 - Legal Request or Fraud Analysis. 5. SafeKey Transactions which were either Fully Authenticated or Attempted. 6. For POS Only Transactions - AEIPS-compliant Chip Card Transactions where a Transaction Certificate is provided in the First Presentment. 7. Consumer-Presented Quick Response (CPQR) Transactions. 8. Merchant-Presented Quick Response (MPQR) Transactions. 9. Transactions to fund a Stored Value Digital Facility (SVDF). 10. A Chargeback where fulfillment has already been received.
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment
Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. Cardmember must dispute the Charge, and 2. Issuer must wait the required timeframe for the Fulfillment Notification before filing the Chargeback unless the Acquirer has sent a Fulfillment Notification stating Not Fulfilling in which case the Chargeback may be filed upon receipt of this notification.
Retrieval Required	Yes. The Chargeback is the result of a previous Retrieval Request.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4516 - Request for Support Not Fulfilled (continued)

Issuer Support	None
Second Presentment Acquirer Responsibility	The Acquirer must provide one (1) or more of the following for Chargebacks processed under this ISO Code to support a Second Presentment: 1. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 2. Proof that the Chargeback is a result of an invalid Retrieval Request as established in Table 7-3, "Retrieval Request Notification Reasons," on page 289. 3. Correct, relevant information, where the Issuer has requested invalid information, e.g., a copy of a folio when the Transaction occurred at an airline S/E, the Acquirer must provide the correct S/E information. **Note:** If the Acquirer did not provide the correctly requested Documentation with a Fulfillment or did not use Network Disputes Manager to send Fulfillment Documentation to the Issuer, a Second Presentment right will not be available.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4517 - Request for Support Illegible/Incomplete

Chargeback Type	Retrieval Chargeback
Chargeback Reason	One (1) of the following: • Documentation necessary to investigate a Cardmember inquiry, substantiate a Chargeback, or support a legal or fraud investigation, • The Acquirer provided illegible or incomplete Documentation, or • The Acquirer submitted a Fulfillment Notification message, however, the Fulfillment Documentation was not provided to the Issuer.
Description	The Acquirer failed to provide the Issuer with Fulfillment data or Documentation requested as established in Section 7.5, "Fulfillment Data Requirements," on page 294. **Note:** A truncated PAN does not constitute incomplete Documentation or Fulfillment data.
POS/ATM Eligibility	POS and ATM
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Any Transaction where the Retrieval Request was initiated using ISO Message Reason Code 6008 Cardmember requests copy of ROC with one (1) of the following Transaction types: • "Card Not Present Charges" in Section 4.2.10, "Card Not Present Charges," on page 221 • "Aggregated Transactions" in Section 4.2.13, "Aggregated Transactions," on page 224 • "No Show Reservations Program" in Section 4.2.20.1, "No Show Reservations Program," on page 229 • "Advance Deposit or Payment Program" in Section 4.2.20.3, "Advance Deposit or Payment Program," on page 231 2. Transactions where the Retrieval Request was initiated using the ISO Message Reason Code 6016 Cardmember needs for personal records. 3. A Final Chargeback where a Retrieval Request was not requested for the disputed Transactions. 4. A Final Chargeback where the requested Documentation was provided in the Second Presentment. 5. Transactions that qualify under the No Signature/No PIN Program. Refer to Section 4.2.20.4, "No Signature/No PIN Program," on page 232. 6. Expresspay, Expresspay Mobile, or Digital Wallet Contactless-Initiated Transactions, where the Transaction amount is less than or equal to the country threshold for Expresspay Transactions as indicated in the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide* available on Knowledge Base. 7. AEIPS PIN Digital Wallet Contactless-Initiated and Digital Wallet Application-Initiated Transactions where the Retrieval Request was initiated using Reason Code 6006 - Legal Request or Fraud Analysis. 8. SafeKey Transactions which were either Fully Authenticated or Attempted. 9. For POS Only Transactions - AEIPS-compliant Chip Card Transactions where a Transaction Certificate is provided in the First Presentment. 10. Consumer-Presented Quick Response (CPQR) Transactions. 11. Merchant-Presented Quick Response (MPQR) Transactions. 12. Transactions to fund a Stored Value Digital Facility (SVDF).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4517 - Request for Support Illegible/Incomplete (continued)

Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment
Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. Cardmember must dispute the Charge, and 2. The Issuer submitted the Retrieval Request Notification within 105 days of the Network Processing Date of the Presentment, and 3. The required information for First Chargeback requested through the Retrieval Request and received in the Fulfillment Documentation is illegible or incomplete, and 4. The Issuer stated what required Documentation was illegible or incomplete **and** why the Documentation is necessary to satisfy a Cardmember inquiry, or substantiate a Chargeback, or support a legal or fraud investigation. 5. The required information for Final Chargeback requested through the Retrieval Request and received in the Second Presentment is illegible or incomplete.
Retrieval Required	Yes. The Chargeback is the result of a previous Retrieval Request. **Note:** For a Final Chargeback processed under this ISO Code, an Issuer must have requested a Retrieval Request for the disputed Transaction.
Issuer Support	The Issuer must provide the following for Chargebacks processed under this ISO code: 1. An Issuer Declaration that states the following: a. The Documentation that was illegible or incomplete, and b. A statement indicating why the Documentation is necessary to satisfy a Cardmember inquiry, substantiate a Chargeback, or support a legal or fraud investigation. **Note:** If the dispute relates to an airline Transaction, the Issuer must provide an Issuer Declaration or Cardmember Documentation that contains both Cardmember name and Card Account number. If available, Issuers should also provide applicable reference numbers (e.g., ticket number, passenger name(s), S/E number).
Second Presentment Acquirer Responsibility	The Acquirer must provide one (1) or more of the following for Chargebacks processed under this ISO Code to support a Second Presentment: 1. Proof that required Documentation was sent within the specified timeframes and was legible, complete and correct. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 3. Proof that the Chargeback is a result of an invalid Retrieval Request as established in Table 7-3, "Retrieval Request Notification Reasons," on page 289. 4. Documentation that either: • Refutes the Issuer's declaration regarding the necessity of the Documentation to support a Cardmember inquiry, substantiate a Chargeback, or support a legal or fraud investigation, or • Provides the Documentation stated in the Issuer's declaration. 5. Proof that Transaction falls into one (1) of the excluded Transaction types.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4521 - Invalid Authorization

Chargeback Type	Authorization Chargeback
Chargeback Reason	One (1) of the following: • The S/E either failed to obtain a valid Authorization for a Transaction that exceeded the Network Floor Limit, or • The S/E failed to obtain a single Authorization for the full amount of the Transaction, or • The Authorization was requested by the S/E, was declined or reversed, and the S/E submitted the Transaction for Payment, or • The Authorization for the Transaction is greater than seven (7) days before the Network Processing Date of the Presentment, or • The S/E failed to adhere to the policy requirements for Expresspay Transactions conducted at TATs as detailed in Section 4.2.9.1.2, "Authorization Requirements for Expresspay Transactions at TATs," on page 219. **Note:** S/Es that receive Authorizations for estimated Charge amounts may obtain additional Authorizations. Refer to Section 4.2.19, "Estimated Charge Amounts," on page 227 for additional information.
Description	The Issuer may charge back a Transaction using this Chargeback ISO Code under one (1) of the following circumstances: 1. The Issuer receives a Transaction that exceeds the Network Floor Limit and was not Authorized for the full amount in a single Authorization Request. The Authorization may be requested by one (1) of the following: a. The Issuer, or b. The Network if done during the Stand-In process, or c. By a Chip Card application. 2. The S/E requested an Authorization that was declined or reversed and the S/E submitted the declined Transaction for payment. The Authorization Request may be declined by either the Issuer, by the Network if done during Stand-In, or Offline by a Chip Card. 3. The S/E obtained Authorization for a Transaction, but the S/E or Acquirer waited more than seven (7) days to submit the Transaction for payment.
POS/ATM Eligibility	POS only

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4521 - Invalid Authorization (continued)

Excluded Transactions	The following Transactions are excluded from being processed under this ISO Code: 1. For Chargebacks processed under Chargeback Description one (1), two (2), or three (3) of this ISO code: a. Chargebacks that qualify for Fraud or Cardmember Dispute Chargeback Types. 2. As applicable, the following Transactions are also excluded. For Chargebacks processed under: a. Chargeback Description one (1) of this ISO Code - Transactions that have been correctly Authorized in accordance with requirements for estimated Charge amounts. b. Chargeback Description one (1) or two (2) of this ISO Code - Chip Card Transactions where the Transaction Certificate provided in the First Presentment shows that the Authorization was granted Offline by the Chip Card application. c. Chargeback Description three (3) of this ISO Code - Lodging, cruise line, and car rental Transactions where the Authorization is valid for the life of the lodging or cruise line stay or car rental agreement. Refer to Section 4.2.19.1, "Lodging," on page 227 and Section 4.2.19.3, "Car Rental," on page 227, and Section 4.2.19.2, "Cruise Lines," on page 227 for additional information. d. Chargeback Description three (3) of this ISO Code - Expresspay Transactions conducted at TATs where the Authorization is valid for the duration of the "Status check/cumulative spend interval to authorize (maximum contiguous days)" listed by the Transit S/E's market in Table 4-1, "Expresspay at TAT - Operational Parameters," on page 219. 3. Expresspay Transactions of less than or equal to the Cumulative Spend Protection Threshold listed in Table 4-1, "Expresspay at TAT - Operational Parameters," on page 219 or the Declined Authorization Protection amount listed Table 4-2, "Expresspay at TAT - Declined Authorizations," on page 220 completed at a TAT when the S/E has followed all requirements described in Section 4.2.9.1.2, "Authorization Requirements for Expresspay Transactions at TATs," on page 219. 4. Merchant-Presented Quick Response (MPQR) Transactions.
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment
Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. Chargeback Descriptions one (1), two (2), or three (3) of this ISO Code - The Issuer made an effort in good faith to collect payment from the Cardmember for the Transaction. 2. As applicable, the following conditions also exist for Chargebacks processed under: a. Chargeback Description one (1) of this ISO Code: i. If prior Authorization was provided for a lesser amount, the Chargeback amount is restricted to the difference of the Authorized amount and the Presentment Transaction amount. ii. For estimated Charge amounts the Chargeback amount is restricted to the difference of the Authorized amount plus the allowable percentage and the Presentment Transaction amount. (Refer to Section 4.2.19, "Estimated Charge Amounts," on page 227 for more information.)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4521 - Invalid Authorization (continued)

Retrieval Required	No
Issuer Support	The Issuer must provide the following to support a Chargeback processed under this ISO Code. For Chargebacks processed under: 1. Chargeback Description one (1), two (2), or three (3) of this ISO Code - An Issuer Declaration that: a. Indicates the Chargeback Description that the Chargeback is processed under, and b. Supports the Chargeback. 2. As applicable, the Issuer must also provide the following for Chargebacks processed under: a. Chargeback Description one (1) or two (2) of this ISO code - The Issuer must provide the following in the case of an AEIPS Transaction. The Issuer must provide a copy of the validated Transaction Certificate data to prove that Authorization was not provided by the AEIPS-compliant Chip Card. **Note:** This is only required for Final Chargebacks.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4521 - Invalid Authorization (continued)

Second Presentment Acquirer Responsibility	The Acquirer must provide the following in order to support a Second Presentment. For Chargebacks processed under: 1. Chargeback Description one (1), two (2), or three (3) of this ISO code - One (1) or more of the following must be provided: a. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. b. Proof that the Transaction falls into one (1) of the excluded Transaction types. 2. As applicable, the Acquirer can also provide the following to support a Second Presentment. For Chargebacks processed under: a. Chargeback Description one (1) of this ISO code - One (1) of the following must be provided: i. Proof that the original Transaction was improperly described when sent and did not exceed the Network Floor Limit; e.g., the S/E type was improperly designated resulting in a lower Network Floor Limit being applicable, or ii. Proof that Authorization was obtained for the same Transaction on the Transaction Date for a lesser amount which was not presented by the Acquirer. Only the Authorized Transaction amount can be submitted as a Second Presentment, or iii. Proof that a single Authorization for the full amount of the Transaction was obtained on the Transaction Date, or iv. Proof that Authorization was obtained in accordance with requirements for estimated Charge amounts. Only the Authorized amount plus the allowable percentage can be submitted as a Second Presentment. b. Chargeback Description two (2) of this ISO code: i. Proof of Authorization obtained on the Transaction Date for a lesser amount which was not subsequently charged to the Cardmember's Account. Only the approved amount can be a Second Presentment, or ii. Proof a valid Transaction was Authorized for the disputed Transaction. c. Chargeback Description three (3) of this ISO code: i. The Acquirer must provide proof that Authorization was obtained within seven (7) days of the Presentment Date of the disputed Transaction.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4523 - Unassigned Cardmember Account Number

Chargeback Type	Processing Error Chargeback
Chargeback Reason	Card Account number is not assigned to a Cardmember.
Description	The Issuer receives a Transaction for an Account number, which matches none of the Cards that it has issued. It contains the Issuer's Identification Number and a valid check digit, however, the number has never been assigned to a Cardmember.
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Transactions in which an Authorization has been obtained from the Issuer, the Issuer's agent or during Stand-In; or 2. Chip Card Transactions where a Transaction Certificate provided in the First Presentment bears the same Card number. 3. Merchant-Presented Quick Response (MPQR) Transactions.
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.
Conditions	None
Retrieval Required	No
Issuer Support	None
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Evidence that a Card carrying the disputed Account number was used at the POS: • Copy of imprinted slip, which confirms Account number. • Copy of receipt from POS terminal, which read the Account number from the magnetic stripe. 2. Proof that the Transaction falls into one (1) of the excluded Transaction types. 3. Proof that a correcting Transaction, which directly offsets the disputed Transaction has already been processed. The Acquirer may accept the Chargeback and send a new First Presentment with a corrected Card Account number if it can provide one (1). The new Transaction will be subject to Late Presentment policy. See "ISO 4536 - Late Presentment" on page 329.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4527 - Missing Imprint

Chargeback Type	Fraud Chargeback
Chargeback Reason	The Cardmember denies participation in a Transaction in which the S/E fails to obtain a physical or electronic Imprint of the Card.
Description	None additional
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Authorized Transactions where the full magnetic stripe was sent to the Issuer with the Authorization Request. 2. Mail/Telephone/Internet. 3. Chip Card Transactions where a Transaction Certificate is provided in the First Presentment. 4. Digital Wallet Program Transactions. 5. Merchant-Presented Quick Response (MPQR) Transactions. 6. Transactions to fund a Stored Value Digital Facility (SVDF). 7. Transactions using a flat-printed Card.
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment
Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. Before filing this Chargeback, the Issuer must manually enter the fraud Transaction into the WFIS or electronically transmit it into the GNS Fraud Repository. 2. The Cardmember Account must be added to the Exception File before filing this Chargeback. 3. For Final Chargeback - This Chargeback is only applicable if the First Chargeback was either a fraud type or one of the following: a. 4512 - Multiple Processing b. 4516 - Request for Support Not Fulfilled c. 4517 - Request for Support Illegible/Incomplete d. 4754 - Local Regulations/Legal Dispute
Retrieval Required	No
Issuer Support	Cardmember Documentation or Issuer Declaration that supports the Chargeback.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Transaction falls into one (1) of the excluded Transaction types. 2. Proof that the Card was present by providing an imprinted ROC or showing capture of the magnetic stripe. 3. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4530 - Currency Discrepancy

Chargeback Type	Processing Error Chargeback
Chargeback Reason	Acquirer sent Presentment in a currency different than the Transaction currency or a currency rate other than an approved rate was used to convert the Transaction into Presentment currency.
Description	The Cardmember transacted business at a foreign S/E or ATM in local currency. When the Transaction was sent, a currency other than the correct Transaction currency or currency rate selected by American Express was used to convert the Transaction into Presentment currency.
POS/ATM Eligibility	POS and ATM
Excluded Transactions	None
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the First Presentment.
Conditions	Chargeback must be made for the full original Presentment Transaction amount of the Transaction.
Retrieval Required	No
Issuer Support	Cardmember Documentation or Issuer Declaration that supports the Chargeback.
Second Presentment Acquirer Responsibility	The following must be provided: 1. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. The Acquirer may accept the Chargeback and send a new First Presentment with the correct Transaction currency and conversion rate. The new Transaction will be subject to Late Presentment policy. See "ISO 4536 - Late Presentment" on page 329.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4534 - Multiple ROCs

Chargeback Type	Fraud Chargeback
Chargeback Reason	The Cardmember denies participation in one (1) or more suspect Transactions at the same S/E where the Cardmember had previously used his/her Card.
Description	The Cardmember acknowledges having transacted business with the S/E either in the past or during the same timeframe as when the suspect Transactions were created. The Cardmember further denies knowledge of the suspect Transactions themselves. This Chargeback is not intended to remedy multiple processing of a single Transaction through a processing error. Utilize Chargeback reason "ISO 4512 - Multiple Processing" on page 311 for these types of errors.
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Purchases in separate store departments, Recurring Billing, Advance Deposits or Payment, Delayed Billing Charges, Delayed Delivery "balance" Transactions, Split Shipment Transactions, and carrier passenger policy Charges. 2. Eligible Transactions with an active Issuer Override Request status code in FraudNet. Refer to "Exhibit 15. Dynamic Fraud Management Network Services Terms and Conditions" on page 482 for more information on Eligible Transactions. 3. Merchant-Presented Quick Response (MPQR) Transactions.
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment
Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. Before filing this Chargeback, the Issuer must manually enter the fraud Transaction into the WFIS or electronically transmit it into the GNS Fraud Repository. 2. The Cardmember Account must be added to the Exception File before filing this Chargeback. 3. For Final Chargeback - This Chargeback is only applicable if the First Chargeback was either a fraud type or one of the following: a. 4512 - Multiple Processing b. 4516 - Request for Support Not Fulfilled c. 4517 - Request for Support Illegible/Incomplete d. 4754 - Local Regulations/Legal Dispute
Retrieval Required	No
Issuer Support	Cardmember Documentation or Issuer Declaration that supports the Chargeback.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Transactions were valid Charges. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 3. Proof that the Transaction falls into one (1) of the excluded Transaction types.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4536 - Late Presentment

Chargeback Type	Processing Error Chargeback
Chargeback Reason	Presentment was not submitted by the Acquirer and accepted by the AEGN within the required timeframe.
Description	The Network Processing Date of the First Presentment is: 1. More than thirty (30) days but less than 181 days after the Transaction Date, and the Account is blocked or closed, or 2. More than 180 days after the Transaction Date. The Transaction may or may not have been authorized by the Issuer, depending upon the Transaction amount and any applicable Network Floor Limit. Whether the Transaction was authorized or not, if the Issuer fails in its effort to collect from the Cardmember, the Transaction may be charged back.
POS/ATM Eligibility	POS only
Excluded Transactions	Transactions that could be charged back under reason "ISO 4521 - Invalid Authorization" on page 321.
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.
Conditions	1. A failed effort in good faith has been made by the Issuer to collect payment on the Transaction in dispute, and 2. For description one (1) above, the Card Account must be added to the Exception File no later than the Network Processing Date of the Chargeback.
Retrieval Required	No
Issuer Support	The Issuer must provide the Transaction Date contained in the original Presentment.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof the Transaction was submitted by the Acquirer and accepted by the AEGN within the required timeframe. 2. For description two (2) above, proof of a different, correct Transaction Date that is within the 180 day limit. 3. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 4. Proof that the Transaction falls into one (1) of the excluded Transaction types.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4540 - Card Not Present

Chargeback Type	Fraud Chargeback
Chargeback Reason	The Cardmember denies participation in a Mail/Telephone/Internet Transaction, which may or may not have been Authorized by the Issuer.
Description	A mail order, telephone order, or Internet type Transaction, was processed by an S/E without the permission of the Cardmember whose Account number was used.
POS/ATM Eligibility	POS only
Excluded Transactions	Any of the following that apply: 1. Card Present. 2. When the PCSC was provided to the Issuer in the POS Authorization Request (1100) message and the Issuer failed to provide a PCSC validation response of "Y" or "N" in the POS Authorization Response (1110) message. 3. When the Cardmember address information was provided to the Issuer in the POS Authorization Request (1100) message and either: a. The Issuer is located in the United States or Canada and does not participate in the AAV program, or b. The S/E shipped physical Goods to an address that the Issuer verified through the AAV program, where the Issuer provided either of the following responses: i. A street address match (for example, street address match is 123 Main Street and S/E shipped Goods to 123 Main Street), or ii. A street address and postal code match (for example, street address match and postal code match is 123 Main Street, 68796 and S/E shipped Goods to 123 Main Street, 68796). 4. Transactions that qualify for the American Express SafeKey Fraud Liability Shift. Refer to Section 7.10.8.3, "American Express SafeKey Fraud Liability Shift," on page 361 for additional information. 5. Digital Wallet Contactless-initiated Transactions, Digital Wallet MST Transactions, and Expresspay Mobile. 6. Digital Wallet Application-initiated Transactions that have been granted an exception as part of the AEGNS Risk Assessment described in Section 2.5.4.1, "General Requirements for Digital Wallet Programs," on page 58. For further information, please contact your AEGNS representative. 7. Eligible Transactions with an active Issuer Override Request status code in FraudNet. Refer to "Exhibit 15. Dynamic Fraud Management Network Services Terms and Conditions" on page 482 for more information on Eligible Transactions. 8. Consumer-Presented Quick Response (CPQR) Transactions. 9. Merchant-Presented Quick Response (MPQR) Transactions.
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the First Presentment

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4540 - Card Not Present (continued)

Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. Before filing this Chargeback, the Issuer must manually enter the fraud Transaction into the WFIS or electronically transmit it into the GNS Fraud Repository. **Note:** Issuers may not raise this Chargeback on Transactions originating from S/Es in the United States or Canada solely for the S/E's failure to obtain a signature from the Cardmember as Proof of Delivery. 2. The Cardmember Account must be added to the Exception File before filing this Chargeback. 3. For Final Chargeback - This Chargeback is only applicable if the First Chargeback was either a fraud type or one of the following: a. 4512 - Multiple Processing b. 4516 - Request for Support Not Fulfilled c. 4517 - Request for Support Illegible/Incomplete d. 4754 - Local Regulations/Legal Dispute
Retrieval Required	No
Issuer Support	Cardmember Documentation or Issuer Declaration that supports the Chargeback and demonstrates that both the Card and Cardmember were not present for the Transaction. For airline Transactions, the Issuer must ensure that the Issuer Declaration or Cardmember Documentation contains both Cardmember name and Card Account number. If available, Issuers should also provide applicable reference numbers (for example, ticket number, passenger name(s), S/E number). Additional Issuer Support Requirements for Final Chargebacks after Compelling Evidence was provided by the Acquirer during Second Presentment: The Issuer must provide one (1) of the following: • Documentation that demonstrates the Issuer contacted the Cardmember with the Second Presentment Compelling Evidence and an Issuer Declaration refuting the Second Presentment Compelling Evidence, or • Issuer Declaration indicating that the Second Presentment Compelling Evidence provided is not valid, or • Issuer Declaration attesting that the name and address provided in the Second Presentment Compelling Evidence does not match the Cardmember details.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Cardmember signed a carrier delivery receipt for Goods. **Note:** S/Es in the United States or Canada are not required to provide a signature from the Cardmember in order to qualify as valid Proof of Delivery. 2. Proof that the Transaction falls into one (1) of the excluded Transaction types. 3. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 4. Compelling Evidence as indicated in Table 7-15, "Compelling Evidence as a Second Presentment Responsibility," on page 301.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4544 - Cancellation of Recurring Goods/Services

Chargeback Type	Cardmember Dispute Chargeback
Chargeback Reason	A Cardmember selected the S/E's option to process Recurring Billing Transactions on the Card and the Cardmember revoked their consent to process Recurring Billing Transactions from the S/E on their Card.
Description	The Issuer may charge back a Transaction using this Chargeback ISO code when a Recurring Billing S/E submits Recurring Billing Transactions subsequent to: 1. The Cardmember's revocation of consent to process Recurring Billing Transactions from that S/E on the Card and either: • The Cardmember made a reasonable attempt to notify the Recurring Billing S/E that the Cardmember has revoked their consent to process Recurring Billing Transactions from that S/E on their Card, or • If local laws or regulations prohibit requiring the Cardmember to contact the Recurring Billing S/E, then the Cardmember's Issuer should make a reasonable attempt to notify the Recurring Billing S/E on behalf of the Cardmember.
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Any Transaction other than Recurring Billing Charges for Goods or Services, including Deferred Billing Charges. 2. Card Present Transactions. 3. Merchant-Presented Quick Response (MPQR) Transactions. 4. Installment Payment Provider Transactions.
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment of the recurring Transaction under dispute.
Conditions	The following conditions exist for Chargebacks processed under this ISO Code: 1. Either of the following may apply: a. The Chargeback is limited to Transaction(s) submitted by the Recurring Billing S/E after the notification of the revocation of the Cardmember's consent to process Recurring Billing Transactions on the Card, or b. The Chargeback is limited to the amount of Goods not received or Services unused after the Cardmember revoked their consent, and i. The Cardmember made a reasonable attempt to notify the Recurring Billing S/E that the Cardmember has revoked their consent to process Recurring Billing Transactions from that S/E on their Card, or ii. If local laws or regulations prohibit requiring the Cardmember to contact the Recurring Billing S/E, then the Cardmember's Issuer should make a reasonable attempt to notify the Recurring Billing S/E on behalf of the Cardmember.
Retrieval Required	No

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4544 - Cancellation of Recurring Goods/Services (continued)

Issuer Support	As applicable, the Issuer must provide the following for Chargebacks processed under this ISO code: 1. The Cardmember Documentation or Issuer Declaration that demonstrates: a. That the Cardmember made a reasonable attempt to notify the Recurring Billing S/E that the Cardmember revoked their consent to process Recurring Billing Transactions from that S/E on their Card, or b. If local laws or regulations prohibit requiring the Cardmember to contact the Recurring Billing S/E, that the Cardmember's Issuer made a reasonable attempt to notify the Recurring Billing S/E on behalf of the Cardmember.
Second Presentment Acquirer Responsibility	The Acquirer must provide one (1) or more of the following in order to support a Second Presentment for Chargebacks processed under this ISO code: 1. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed, or 2. Proof that the Transaction falls into one (1) of the excluded Transaction types. 3. Proof that the Cardmember has not cancelled and continues to use the Service or receive the Goods, and a copy of the Recurring Billing cancellation process and cancellation policy. For Transactions processed upon expiration of an Introductory Offer, proof that the S/E fulfilled the requirements stated in Section 4.2.15.1, "Introductory Offers," on page 225.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4553 - Not as Described or Defective Merchandise

Chargeback Type	Cardmember Dispute Chargeback
Chargeback Reason	Either of the following: • The Cardmember received Goods or Services that are different than the written description provided by the S/E at the time of the purchase, or • The Cardmember received damaged Merchandise or defective Merchandise or Services.
Description	The Issuer may charge back a Transaction using this ISO Code when the Cardmember attempted to return Goods or cancel Services and one (1) of the following: 1. The Goods or Services received by the Cardmember are different than the written description provided by the S/E at the time of purchase, including a dispute related to the quality of Goods or Services received by the Cardmember. 2. The Goods or Services purchased by the Cardmember were received in a damaged or defective state.
POS/ATM Eligibility	POS only
Excluded Transactions	Transactions to fund a Stored Value Digital Facility (SVDF).
Minimum Amount	$25
Chargeback Maximum Time to File	Either of the following: • 120 days from the Network Processing Date of the Presentment, or • 120 days from the date of receipt of Goods or Services.
Conditions	The Issuer must meet all the following conditions: 1. The Cardmember has failed in a good faith attempt with the S/E to return Goods or cancel Services, or otherwise resolve the issue directly with the S/E. 2. The Issuer must wait fifteen (15) days from the date of the attempted return before sending the Chargeback, unless the 120 day filing limit would be exceeded. 3. The Chargeback amount is limited to the disputed amount of the Transaction. For Chargebacks processed under Chargeback Description two (2) of this ISO Code, the Cardmember must comply with the S/E's return policy when attempting to return the Goods or cancel the Services.
Retrieval Required	No

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4553 - Not as Described or Defective Merchandise (continued)

Issuer Support	The Issuer must provide the following to support a Chargeback processed under this ISO code. For Chargebacks processed under: 1. Chargeback Description one (1) or two (2) of this ISO Code: a. An Issuer Declaration that indicates the Chargeback Description that the Chargeback is processed under. 2. As applicable, the Issuer must also provide the following for Chargebacks processed under: a. Chargeback Description one (1) of this ISO Code: i. The Cardmember's written Documentation or Issuer Declaration detailing: • The Cardmember's Good Faith attempt(s) to return the Goods or cancel the Services with the S/E, or otherwise resolve the issue directly with the S/E (including the date(s), Person(s) contacted, and communication method(s) used by the Cardmember), • A description of the expected Goods or Services, • A description of the received Goods or Services. ii. A detailed written description of the Goods or Service(s) purchased. For a Mail Order/Telephone Order/Internet purchase, other written description may be used, as applicable (e.g., catalog page, Web page). iii. Proof of return of Goods or cancellation of Services, when applicable. iv. Additional Issuer Support Requirements for Chargebacks based on the quality of the Goods or Services received by the Cardmember: • For First Chargebacks - The Issuer must provide Cardmember Documentation or an Issuer Declaration that describes how the quality of the Goods or Services received by the Cardmember was not as reasonably expected or did not match the description of the Goods or Services that were provided by the S/E. • For Final Chargebacks - The Issuer must provide Documentation from an expert or a professional that supports the Cardmember's dispute related to the quality of the Goods or Services. This Documentation must include information to demonstrate the expertise of the expert or professional. Examples include, but may not be limited to, a copy of the expert's license in the applicable field (e.g., gemologist), or copy of the expert's business card or company letterhead. b. Chargeback Description two (2) of this ISO Code - i. The Cardmember's written complaint or Issuer Declaration detailing: • The problem, disputed amount, date of receipt of Goods or Services, extent of damage, and date and details of notification to the S/E of damage or defect, and • The Cardmember's Good Faith attempt(s) to return the Goods or cancel the Services with the S/E (including the date(s), Person(s) contacted, and communication method(s) used by the Cardmember).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4553 - Not as Described or Defective Merchandise (continued)

Second Presentment Acquirer Responsibility	The Acquirer must provide the following in order to support a Second Presentment. For Chargebacks processed under: 1. Chargeback Description one (1) or two (2) of this ISO Code - a. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed, or b. Proof refuting Cardmember's claim that Goods were returned to the S/E, that the Services were cancelled, or that the Cardmember did not attempt to resolve the issue with the S/E. c. For Installment Payment Provider Transactions and Bill Payment Provider Transactions, proof that the Chargeback is not valid based on the Indirect Acceptor's terms and conditions agreed to by the Cardmember. 2. As applicable, the Acquirer can also provide the following to support a Second Presentment. For Chargebacks processed under: a. Chargeback Description one (1) of this ISO Code, the Acquirer must provide Documentation that refutes the Cardmember's claim. **Note:** If the Chargeback was based on the quality of Goods or Services received, then the Acquirer must provide Documentation to demonstrate that the quality of the Goods or Services provided by the S/E to the Cardmember matched the description of the Goods or Services that were provided by the S/E. b. Chargeback Description two (2) of this ISO Code, the Acquirer must provide one (1) or more of the following items: i. Show that an attempt was made by the S/E to repair or replace damaged or defective Goods or to provide replacement Services. ii. If returned, state how the Cardmember did not comply with the S/E's clearly documented cancellation, return policy or applicable law and regulations. iii. Show that the Cardmember agreed to accept the Goods or Services "as is." 3. Proof that the Goods or Services matched what was described at the time of purchase (e.g., emails, certificate of authenticity, photographs).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4554 - Goods and Services Not Received

Chargeback Type	Cardmember Dispute Chargeback
Chargeback Reason	Goods or Services were only partially delivered or not delivered at all. Included in this description are funds dispensed from an ATM or funds loaded to a Stored Value Digital Facility (SVDF).
Description	The Goods or Services purchased by the Cardmember were only partially received or not received at all. Where partial receipt makes the entire purchase unsuitable or unacceptable, the Cardmember must attempt to return the Goods received or cancel the Services before full Credit may be authorized. In the case of Transactions to fund an SVDF, the funds were not loaded to the SVDF or only partially loaded. In the case of funds dispensed from an ATM or funds loaded to an SVDF, no return of partially dispensed/loaded funds is necessary. The Chargeback amount is the amount of funds claimed not to have been received. Except in the case of ATM Transactions, Transactions to fund an SVDF, or Transactions where the Goods or Services were not received at all, the Issuer must request that the Cardmember make an attempt to contact the S/E to return the Goods or cancel the Services in compliance with both the S/E's return policy and local laws and regulations.
POS/ATM Eligibility	POS and ATM
Excluded Transactions	Transactions that could be charged back under "ISO 4513 - Credit Not Presented" on page 312.
Minimum Amount	$25
Chargeback Maximum Time to File	**POS**: Either of the following: 1. 120 days from the Network Processing Date of the Presentment, or 2. 120 days from one (1) of the below (whichever occurred first): • From the expected date of receipt of the Goods and Services (for example, airline flight date or entertainment performance date), or • From the date the Cardmember becomes aware that the expected Goods and Services would not be provided, not to exceed 540 days from the Network Processing Date of the First Presentment (for example, airline bankruptcy or entertainment performance cancellation) **SVDF**: 120 days from the Network Processing Date of the Presentment for Transactions used to fund an SVDF where the funds were not loaded to the SVDF or only partially loaded. **ATM**: Forty-five (45) days from the Network Processing Date of the Fulfillment Notification.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4554 - Goods and Services Not Received (continued)

Conditions	The Issuer must meet all the following conditions: 1. The Cardmember made a Good Faith attempt to either obtain or cancel the Goods or Services not received or return the partially received Good or Services in compliance with both the S/E's cancellation/return policy and local law and regulation. 2. Prior to sending the Chargeback, the Issuer must wait until: • The expected date of delivery, or • Fifteen (15) days from the Transaction Date if delivery is unscheduled, and within 120 days from the Network Processing Date of the Presentment, or • Fifteen (15) days from the date of the attempted return, unless the 120-day filing limit would be exceeded, or • If the S/E is no longer in business or if the Cardmember becomes aware that the expected Goods and Services would not be provided, the Issuer may file a Chargeback immediately. And one (1) or more of the following conditions is also met: 3. The amount to be charged back will either be for that part of the Goods or Services which were not received or for the entire Transaction amount when partially delivered shipments have been returned to the S/E. In the case of funds dispensed from an ATM, no return of partially dispensed funds is necessary. 4. The Cardmember ordered Goods or Services via mail/telephone/Internet means, to be delivered to the address specified by the Cardmember and the Goods or Services were not received. 5. In the case of Transactions to fund an SVDF, the funds were not loaded to the SVDF or only partially loaded. The amount to be charged back is limited to the difference between the Presentment Amount and the amount loaded to the SVDF. No return of partially loaded funds is necessary.
Retrieval Required	For ATM dispense only If the Issuer intends to file a Chargeback that requires a Retrieval Request, the Retrieval Request Notification must be made within 105 days from the Network Processing Date of the Presentment.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4554 - Goods and Services Not Received (continued)

Issuer Support	The Issuer must provide all the following: 1. The Cardmember's written Documentation or Issuer Declaration detailing one (1) of the following: a. Cardmember's attempt(s) to return the partially received Goods, or b. Cardmember's attempt(s) to cancel the partially received Services and receive credit from the S/E (including the date(s), Person(s) contacted, and communication method(s) used by the Cardmember), or c. Cardmember becomes aware that the expected Goods and Services would not be provided, or d. Non-receipt of Goods and Services. In the case of Transactions to fund an SVDF, Cardmember's claim that the funds were not loaded to the SVDF or only partially loaded. 2. A detailed written description of the Goods or Services purchased and expected date of delivery. For a Mail Order/Telephone Order/Internet purchase, other written description may be used, as applicable (e.g., catalog page, Web page). For Transactions to fund an SVDF, Documentation containing fund loading activity may be used. 3. Proof of return of Goods or cancellation of Services, when applicable. Additional Issuer support requirements for Chargeback conditions of this ISO code: • For airline Transactions covered under Chargeback Condition four (4) of this ISO code, the Issuer must provide support described in items one (1) through three (3) above and Cardmember name, Card Account number, and passenger name(s). If available, Issuers should also provide applicable reference numbers (e.g., ticket number, S/E number). Additional Issuer Support Requirements for Final Chargebacks after Compelling Evidence was provided by the Acquirer during Second Presentment: 1. The Issuer must provide one (1) of the following: a. Documentation that demonstrates the Issuer contacted the Cardmember with the Second Presentment Compelling Evidence and an Issuer Declaration refuting the Second Presentment Compelling Evidence, or b. if the Issuer did not attempt to contact or failed to contact the Cardmember, an Issuer Declaration refuting the Second Presentment Compelling Evidence and explaining why it was not presented to the Cardmember (e.g., the Issuer is unable to contact the Cardmember due to regulatory constraints).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4554 - Goods and Services Not Received (continued)

Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Goods or Services were received in their entirety by the Cardmember or the Cardmember's authorized representative. For Transactions to fund an SVDF, proof the funds were loaded. 2. Proof that the Goods or Services were delivered to the address specified by the Cardmember. 3. Proof refuting Cardmember's claim that Services were cancelled or that the Goods were returned to the S/E. 4. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 5. Proof that the Goods are held by Customs authorities and that the Cardmember has failed to claim them. 6. Proof that Goods were seized by Customs authorities in the destination country and the Cardmember is legally prohibited from claiming them. 7. In the case of funds dispensed from an ATM, provide Transaction Log showing proof funds were received by the Cardmember. 8. Proof that the First Chargeback was processed more than 120 days after the Cardmember becomes aware that the Goods and Services would not be provided. 9. Compelling Evidence as indicated in Table 7-15, "Compelling Evidence as a Second Presentment Responsibility," on page 301. 10. For Installment Payment Provider Transactions and Bill Payment Provider Transactions, proof that the Chargeback is not valid based on the Indirect Acceptor's terms and conditions agreed to by the Cardmember.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4750 - Car Rental Charge Non-Qualified or Unsubstantiated

Chargeback Type	Cardmember Dispute Chargeback
Chargeback Reason	Cardmember was incorrectly charged for car rental damage, theft, loss of use, or other extraordinary fees related to the damage, theft, or loss of use.
Description	The Issuer may charge back a Transaction using this ISO code under one (1) of the following circumstances: 1. The Cardmember was charged for car rental damage and one (1) of the following applies: a. The S/E failed to comply with the requirements of Section 4.2.19.3.1, "Capital Damages to Rental Vehicles - Charge Submission Requirements," on page 228 for the submitted Charge, or b. The Transaction amount charged to the Cardmember was more than 15% above the amount established in the specific estimate of the capital damages, or c. The Cardmember purchased the car rental S/E's collision, loss, or theft insurance. 2. The Cardmember was charged for theft or loss of use of the vehicle.
POS/ATM Eligibility	POS
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: • Charges for the original car rental as provided in the car rental agreement. • Transactions to fund a Stored Value Digital Facility (SVDF).
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment
Conditions	One (1) of the following conditions must exist for Chargebacks processed under this ISO Code: 1. The amount to be charged back is the full amount of the Transaction, or 2. The amount to be charged back is the amount that exceeded 15% over the specific estimate of the capital damages agreed to by the Cardmember.
Retrieval Required	No

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4750 - Car Rental Charge Non-Qualified or Unsubstantiated (continued)

Issuer Support	The Issuer must provide one (1) or more of the following to support a Chargeback processed under this ISO code: 1. If the Transaction amount exceeds the estimated amount by more than 15%, a copy of the specific estimate of the capital damages agreed to by the Cardmember, showing the amount agreed upon with the car rental S/E. 2. If the Cardmember purchased the S/E's collision, loss, or theft insurance - Documentation that proves the Cardmember purchased, and was charged for the car rental S/E's collision, loss, or theft insurance. 3. If the Cardmember was charged for theft or loss of use of the vehicle - Documentation that proves the Cardmember was charged for theft or loss of use of the vehicle. 4. If the Cardmember claims they did not agree to accept liability for the capital damages - Cardmember Documentation or an Issuer Declaration that states the Cardmember did not agree to accept liability for the capital damages.
Second Presentment Acquirer Responsibility	The Acquirer must provide one (1) of the following for Chargebacks processed under this ISO Code to support a Second Presentment. 1. In instances where the Cardmember claims the Transaction amount exceeded the estimated amount by more than 15% - Proof that the Charge submitted was within the specific estimate of the capital damages agreed to by the Cardmember, plus 15%. 2. In instances where the Cardmember claims they purchased the car rental S/E's collision, loss, or theft insurance - Proof refuting Cardmember's claim of S/E insurance (i.e., rental agreement evidencing Cardmember's waiver of insurance or Documentation that shows the Cardmember purchased insurance that was not sufficient to pay for the capital damages). 3. In instances where the Cardmember claims they were charged for theft or loss of use of the vehicle - Proof that the Charge was valid and not for theft or loss of use. 4. In instances where the Cardmember claims they did not agree to accept liability for the capital damages - Proof that the Cardmember agreed to accept liability for the capital damages. 5. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has been presented. 6. Proof that the Transaction falls into one (1) of the excluded Transaction types.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4752 - Credit/Debit Presentment Error

Chargeback Type	Processing Error Chargeback
Chargeback Reason	Credit Transaction sent as debit, or debit Transaction sent as Credit.
Description	A Credit Transaction appeared as a debit on the Cardmember's statement (or vice versa).
POS/ATM Eligibility	POS only
Excluded Transactions	None
Minimum Amount	$25
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.
Conditions	Chargeback amount is to be twice the original Transaction amount.
Retrieval Required	No
Issuer Support	Cardmember Documentation or Issuer Declaration that supports the Chargeback.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Transaction was correctly sent. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. If so, then the Second Presentment amount must equal Chargeback amount.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4754 - Local Regulatory/Legal Dispute

Chargeback Type	Cardmember Dispute Chargeback
Chargeback Reason	Disputes raised by Cardmember under rights provided by law and where no other Chargeback rights apply.
Description	Various laws provide rights to Cardmembers over and above those described in this edition of the *Business and Operational Policies* manual. Where such laws are in effect and the Cardmember claims the rights provided, the Issuer may charge back for this reason, but only where no other Chargeback rights apply, the Transaction meets the defined requirements, and both the Acquirer and Issuer have an obligation under the local regulation/law.
POS/ATM Eligibility	As prescribed by the applicable law
Excluded Transactions	As prescribed by the applicable law
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.
Conditions	To be used only when no other Chargeback type applies, the disputed Transaction meets the defined eligibility, and both the Acquirer and Issuer have an obligation under the local regulation/law.
Retrieval Required	As prescribed by the applicable law
Issuer Support	Cardmember Documentation and/or Issuer Declaration and Issuer Documentation citing the applicable law or regulation.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Supporting Documentation demonstrating that the alleged law/regulation does not exist (e.g., was repealed or expired), the Cardmember is not covered by it, it does not apply to the facts of the Cardmember's dispute, or it does not establish an obligation of the Acquirer. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4755 - No Valid Authorization

Chargeback Type	Fraud Chargeback
Chargeback Reason	The Cardmember denies participation in one (1) of the following: • A Transaction where Authorization was required but not obtained or an Authorization was declined or, • The S/E failed to obtain a single Authorization for the full amount of the Transaction, or • A Transaction which took place on a date falling outside the Valid Date Range of the Card. **Note:** S/Es that receive Authorizations for estimated Charge amounts may obtain additional Authorizations. Refer to Section 4.2.19, "Estimated Charge Amounts," on page 227 for more information.
Description	The Issuer may charge back a Transaction using this Chargeback ISO code under one (1) of the following circumstances: • The S/E submitted a Transaction for payment, which should have been, but was not Authorized, was declined or was not re-Authorized following an expired Authorization, or • The Transaction takes place on a date which falls outside the Valid Date Range of the Card, and the S/E failed to obtain an Authorization from the Issuer (regardless of any Network Floor Limit which may be in effect).
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from being processed under this ISO Code: 1. For Chargebacks processed under Chargeback Description one (1) or two (2) of this ISO Code: a. Chip Card Transactions where the Transaction Certificate provided in the First Presentment Chip Card Addendum (9240) indicates that Authorization was granted Offline by the Chip Card. 2. For Chargebacks processed under Chargeback Description one (1) of this ISO Code: a. Expresspay Transactions of less than or equal to the Cumulative Spend Protection Threshold listed in Table 4-1, "Expresspay at TAT - Operational Parameters," on page 219 or the Declined Authorization Protection amount listed Table 4-2, "Expresspay at TAT - Declined Authorizations," on page 220 completed at a TAT when the S/E has followed all requirements described in Section 4.2.9.1.2, "Authorization Requirements for Expresspay Transactions at TATs," on page 219. 3. Merchant-Presented Quick Response (MPQR) Transactions.
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4755 - No Valid Authorization (continued)

Conditions	The following Conditions exist for Chargebacks processed under this ISO Code: 1. For Chargebacks processed under Chargeback Description one (1) or two (2) of this ISO Code: a. The Issuer must manually enter the fraud Transaction into the WFIS or electronically transmit it into the AEGN Fraud Repository before filing this Chargeback. b. The Cardmember Account must be added to the Exception File before filing this Chargeback. 2. As applicable, the following conditions also exist for Chargebacks processed under: a. Chargeback Description one (1) of this ISO Code: i. If prior Authorization was provided for a lesser amount, the Chargeback amount is restricted to the difference of the Authorized amount and the Presentment Transaction amount. ii. For estimated Charge amounts, the Chargeback amount is restricted to the difference of the Authorized amount plus the allowable percentage and the Presentment Transaction amount. (Refer to Section 4.2.19, "Estimated Charge Amounts," on page 227 for more information.) 3. For Final Chargeback - This Chargeback is only applicable if the First Chargeback was either a fraud type or one of the following: a. 4512 - Multiple Processing b. 4516 - Request for Support Not Fulfilled c. 4517 - Request for Support Illegible/Incomplete d. 4754 - Local Regulations/Legal Dispute
Retrieval Required	No

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4755 - No Valid Authorization (continued)

Issuer Support	The Issuer must provide the following to support a Chargeback processed under this ISO code. For Chargebacks processed under: 1. Chargeback Description one (1) or two (2) of this ISO code: a. Cardmember Documentation or Issuer Declaration that supports the Chargeback. b. For airline Transactions, the Issuer must ensure that the Issuer Declaration or Cardmember Documentation contains both Cardmember name and Card Account number. If available, Issuers should also provide applicable reference numbers (e.g.,ticket number, passenger name(s), S/E number). 2. Chargeback Description two (2) of this ISO code: a. Provide the Valid Date Range of the Cardmember account Required for Final Chargeback Only: For Chip Card Transaction(s), the Issuer must provide a copy of the Cryptogram Information Data from the First Presentment Chip Card Addendum (9240) to prove that Authorization was declined or not given by the Chip Card.
Second Presentment Acquirer Responsibility	The Acquirer must provide one (1) of the following to support a Second Presentment: 1. For Chargebacks processed under Chargeback Description one (1) or two (2) of this ISO code: a. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed, or b. Proof that the Transaction falls into one (1) of the excluded Transaction types, or c. Proof the Acquirer received a valid Authorization. 2. For Chargebacks processed under Chargeback Description one (1) of this ISO Code: a. Proof the original Transaction was improperly described when sent; for example, the S/E type was improperly designated resulting in a lower Network Floor Limit being applicable 3. For Chargebacks processed under Chargeback Description two (2) of this ISO code: a. Proof the Transaction falls within the Valid Date Range printed on the Card

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4763 - Fraud Full Recourse

Chargeback Type	Fraud Chargeback
Chargeback Reason	The Card Account is closed or the Card is cancelled at the time of the Transaction or, the Cardmember denies participation in the Transaction and the S/E is listed on the High Risk S/E list. The Fraud Full Recourse Chargeback allows Issuers the right to transfer liability of all fraud types, including counterfeit Cards, to the Acquirer for any S/E subject to this Chargeback.
Description	Processing under this reason code requires that the S/E was listed on the High Risk S/E list at the time of the Chargeback under one (1) of the following categories: 1. A Fictitious and/or Collusive S/E who is listed on the High Risk S/E list with a risk indicator of "S", or 2. A prohibited or illegal industry S/E who is listed on the High Risk S/E list with a risk indicator of "I", or 3. A high Fraud to Gross (FTG) sale volume ratio S/E who is listed on the High Risk S/E list with a risk indicator of "F", or 4. An Internet Electronic Delivery S/E who is listed on the High Risk S/E list with a risk indicator of "T", or 5. S/E was cancelled for derogatory reasons and was listed on the High Risk S/E list with a risk indicator of "X".
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. AEIPS-compliant Chip Card Transactions where a Transaction Certificate is provided in the First Presentment or Transactions identified as Fallback in the First Presentment. 2. Expresspay Transactions of less than or equal to the Cumulative Spend Protection Threshold listed in Table 4-1, "Expresspay at TAT - Operational Parameters," on page 219 or the Declined Authorization Protection amount listed Table 4-2, "Expresspay at TAT - Declined Authorizations," on page 220 completed at a TAT. 3. Merchant-Presented Quick Response (MPQR) Transactions and the S/E has a risk indicator of "F." 4. High Risk S/Es listed under the following categories are not eligible for Excluded Transactions under this ISO code: a. Risk indicators of "I", "S", "X" b. Gambling MCCs 7801, 7802, 7995 Furthermore, AEGNS may, in its sole discretion, remove eligibility for Excluded Transactions for an industry or a specific S/E that represents elevated risk to the Network.
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment OR 365 days from the Network Processing Date of the Presentment for S/Es with risk indicators "S" or "I"

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4763 - Fraud Full Recourse (continued)

Conditions	The Issuer must meet all the following conditions: 1. May be used even if the Transaction was Authorized. 2. Amount to be charged back is the full Transaction amount. 3. The Cardmember Account must be added to the Exception File before filing this Chargeback. 4. Before filing this Chargeback, the Issuer must manually enter the fraud Transaction into the WFIS or electronically transmit it into the GNS Fraud Repository. 5. For Final Chargeback - This Chargeback is only applicable if the First Chargeback was either a fraud type or one of the following: a. 4512 - Multiple Processing b. 4516 - Request for Support Not Fulfilled c. 4517 - Request for Support Illegible/Incomplete d. 4754 - Local Regulations/Legal Dispute 6. For Fraudulent Application - This Chargeback fraud type is only applicable to recover one-half of losses when: a. At the time of the Chargeback, the S/E was included on the High Risk S/E list as a Fictitious and/or Collusive S/E with a risk indicator of "S," or a prohibited or illegal industry S/E with a risk indicator of "I." 7. SafeKey Transactions with the Network Indicator MPI04 must have occurred after the S/E was placed on the HRSE List with a “T” or “F” to be eligible for this type of Chargeback.
Retrieval Required	No
Issuer Support	Cardmember Documentation or Issuer Declaration that supports the Chargeback.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the S/E was not listed on the High Risk S/E list at the time of the Chargeback. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 3. Proof that the Transaction falls into one (1) of the excluded Transaction types.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4798 - Fraud Liability Shift - Counterfeit

Chargeback Type	Fraud Chargeback
Chargeback Reason	To transfer counterfeit fraud liability from the Issuer to the Acquirer for Transactions conducted with an AEIPS Chip Card at a POS device that is unable to process an AEIPS Chip Card Transaction.
Description	A Transaction has occurred for which: • The Cardmember denies participation, and • The Transaction is classified by the Issuer as counterfeit or skimmed fraud, and • The Transaction was processed on a Card Account that was issued with an AEIPS chip or AEIPS chip/PIN Card, and • The Transaction was performed using a lower level technology than the Card (i.e., Magnetic Stripe or key-entered).
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Mail/Telephone/Internet Transactions. 2. Transactions identified as Fallback in the First Presentment. 3. Transactions that occurred in which either the Issuer or Acquirer is not located in a designated AEIPS Counterfeit FLS country. 4. Digital Wallet Program Transactions. 5. Expresspay Transactions. 6. Eligible Transactions with an active Issuer Override Request status code in FraudNet. Refer to "Exhibit 15. Dynamic Fraud Management Network Services Terms and Conditions" on page 482 for more information on Eligible Transactions. 7. Merchant-Presented Quick Response (MPQR) Transactions. 8. Transactions to fund a Stored Value Digital Facility (SVDF). 9. Transactions occurring before October 14, 2022 where the Issuer or Acquirer is located in Bhutan, China, Laos, Lesotho, Nepal, Taiwan (Province of China), or Thailand.
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4798 - Fraud Liability Shift - Counterfeit (continued)

Conditions	The Issuer must meet all the following conditions: 1. The Transaction information must be submitted to the GNS Fraud Repository as skimmed or counterfeit fraud either by manually entering into the WFIS or electronically transmitting it to the GNS Fraud Repository prior to the Chargeback submission date. 2. The Cardmember Account must be added to the Exception File before filing this Chargeback. 3. The Issuer was certified by AEGNS to process Chip Card Transactions on or before the Transaction date. 4. The Card is identified by AEGNS as chip or chip/PIN capable. 5. The ICC Chip/PIN Indicator in the First Presentment indicates that a chip Transaction was not performed. 6. For Final Chargeback - This Chargeback is only applicable if the First Chargeback was either a fraud type or one of the following: a. 4512 - Multiple Processing b. 4516 - Request for Support Not Fulfilled c. 4517 - Request for Support Illegible/Incomplete d. 4754 - Local Regulations/Legal Dispute
Retrieval Required	No
Issuer Support	The Issuer must provide all of the following: 1. Issuer Declaration indicating the date the Account was listed on the Exception File. 2. Date that the Transaction information was submitted, and that confirmation was received from the GNS Fraud Repository with a fraud type code of skimmed or counterfeit.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Issuer Authorized the Transaction as a magnetic stripe-read when the Service Code was not a Chip Card-assigned Service Code. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 3. Proof that the Transaction falls into one (1) of the excluded Transaction types.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-Received

Chargeback Type	Fraud Chargeback
Chargeback Reason	To transfer lost/stolen/non-received fraud liability from the Issuer to the Acquirer for Transactions conducted with an AEIPS chip and PIN Card at a POS device that is unable to process an AEIPS chip and PIN Transaction. Only Transactions that take place in designated countries are eligible for Lost/Stolen/Non-received FLS.
Description	A Transaction has occurred for which: • The Cardmember denies participation, and • The Transaction is classified by the Issuer as lost, stolen or non-received fraud, and • The Issuer for the Transaction is located in an AEGNS-designated country for AEIPS Lost/Stolen/Non-received FLS, and • The Transaction occurred at an S/E located in an AEGNS-designated country for AEIPS Lost/Stolen/Non-received FLS, and • The Transaction was processed on a Card Account that was issued with an AEIPS chip/PIN Card, and • The Transaction was performed using a lower level technology than the Card, (Magnetic Stripe or key-entered), or the POS device was not able to accept PIN entry.
POS/ATM Eligibility	POS only
Excluded Transactions	The following Transactions are excluded from processing under this ISO Code: 1. Mail/Telephone/Internet Transactions. 2. Transactions identified as Fallback in the First Presentment. 3. Transactions that occurred in a country not designated by AEGNS for Lost/Stolen/Non-received FLS. 4. Transactions that occurred in which either the Issuer or Acquirer is not located in a designated AEIPS Lost/Stolen/Non-received FLS country. 5. Transactions that occurred at a PIN capable and enabled POS device located in Caribbean Countries, United States, or United States Territories. Refer to Section 7.10.8.1.2, "PIN Capable and Enabled POS Devices," on page 360 for additional information. 6. Digital Wallet Program Transactions. 7. Expresspay Transactions. 8. Transactions that qualify under the No Signature/No PIN Program where the POS device is PIN capable and enabled. Refer to Section 4.2.20.4, "No Signature/No PIN Program," on page 232 for additional information. 9. Eligible Transactions with an active Issuer Override Request status code in FraudNet. Refer to "Exhibit 15. Dynamic Fraud Management Network Services Terms and Conditions" on page 482 for more information on Eligible Transactions. 10. Merchant-Presented Quick Response (MPQR) Transactions. 11. Transactions to fund a Stored Value Digital Facility (SVDF).
Minimum Amount	$0
Chargeback Maximum Time to File	120 days from the Network Processing Date of the Presentment.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-Received (continued)

Conditions	The Issuer must meet all the following conditions: 1. The Transaction information must be submitted to the GNS Fraud Repository as fraud either by manually entering into the WFIS or electronically transmitting it to the GNS Fraud Repository prior to the Chargeback submission date. 2. The Cardmember Account must be added to the Exception File before filing this Chargeback. 3. The Issuer was certified by AEGNS to process AEIPS Chip/PIN Card Transactions on or before the Transaction date. 4. The Issuer for the Transaction is located in an AEGNS-designated country for AEIPS Lost/Stolen/ Non-received FLS. 5. The Transaction occurred at an S/E located in an AEGNS-designated country for AEIPS Lost/Stolen/Non-received FLS. 6. The Transaction occurred on or after the AEGNS-designated AEIPS Lost/Stolen/Non-received FLS effective date for both the Issuer and Acquirer countries. 7. The Card is identified as chip and PIN and one (1) of the following conditions are met: • The ICC chip/PIN indicator in the POS First Presentment (1240) message indicates that a chip Transaction was not performed, or • The ICC chip/PIN indicator in the POS First Presentment (1240) message indicates that a chip Transaction was performed but the PIN was not used due to the Terminal not being capable or the PIN pad was not working. 8. For Final Chargeback - This Chargeback is only applicable if the First Chargeback was either a fraud type or one of the following: a. 4512 - Multiple Processing b. 4516 - Request for Support Not Fulfilled c. 4517 - Request for Support Illegible/Incomplete d. 4754 - Local Regulations/Legal Dispute
Retrieval Required	No
Issuer Support	The Issuer must provide all of the following: 1. Issuer Declaration indicating the date the Account was listed on the Exception File. 2. Date that the Transaction information was submitted, and that confirmation was received from the GNS Fraud Repository with a fraud type code of lost, stolen, or non-received.
Second Presentment Acquirer Responsibility	One (1) or more of the following items must be provided: 1. Proof that the Issuer Authorized the Transaction as a magnetic stripe-read when the Service Code was not a Chip Card-assigned Service Code. 2. Proof that a correcting Transaction, which directly offsets the disputed Transaction, has already been processed. 3. Proof that the Transaction falls into one (1) of the excluded Transaction types.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10 Chargeback Policy Requiring Special Handling

This section details additional policy for Chargeback handling arising from unique programs or processing requirements that are not covered in the standard Chargeback policy.

7.10.1 AEGNS Network Disputes Manager-Processed Transactions

For Transactions processed via AEGNS Network Disputes Manager, supporting Documentation must be attached to the Transaction (Fulfillment Notification, First Chargeback, Second Presentment, Final Chargeback) at the time it is sent on AEGNS Network Disputes Manager.

Refer to Table 7-16, "Process Timeframes," on page 303 for additional information regarding submission of Documentation via AEGNS Network Disputes Manager. See the *Network Disputes Manager - User Guide*.

7.10.2 Chip Card Special Handling

Where a Transaction involves a Chip Card in a Chip-Enabled Device, and a validated Transaction Certificate exists for a Transaction, it is the responsibility of the Issuer to review the Transaction Certificate to ensure that the intended Chargeback Reason Code can be used for the Transaction.

Chip Card data restrictions are based upon the principles that:

- A validated Transaction Certificate is evidence that the Card was present at the time of the Transaction
- A Chip Card may Authorize a Transaction Offline, based on Issuer-defined parameters.

7.10.3 ATM Chargebacks

ATM Transactions are cash withdrawals by a Cardmember from an unattended, magnetic stripe-, or Chip Card-reading ATM. These Transactions have a restricted number of Chargeback opportunities.

The following table displays the Message Reason Codes that can be used for ATM Chargebacks (refer to the *Codes Reference Guide* for a list of all valid Message Reason Codes):

Table 7-18. Allowable Codes for ATM Dispute-Related Messages

Message Types/Codes	Valid Codes
Retrieval Request Notification Message Reason Codes	6304
Fulfillment Notification Message Reason Codes	• 6302 • 6303 • 6305
Chargeback Message Reason Codes	• 4516 • 4517 • 4530 • 4554 • 4754
Second Presentment Message Reason Codes	• 2000 • 2006 • 2011 • 2701
Itemized Document Codes	12

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.4 Cash Disbursement

Cash Disbursements are the manual disbursements of cash to Cardmembers by a Cash Disbursement Provider. Refer to the Network Specifications manuals for specific processing information about Cash Disbursement Transactions.

Issuers may request a copy of the ROC via the standard Retrieval Request process. When providing a copy of the ROC to a Cardmember, Issuers are only allowed to provide Cardmembers the details of the original ROC. Personalized government ID information must be removed from the ROC before the Issuer provides it to the Cardmember.

Note: Partial Chargebacks are not permitted on Cash Disbursement Transactions.

The following table indicates Message Reason Codes that can be used for Cash Disbursement Transactions (refer to the *Codes Reference Guide* for a list of all valid Message Reason Codes):

Table 7-19. Allowable Codes for Cash Disbursement Messages

Message Types/Codes	Valid Codes
Retrieval Request Notification Message Reason Codes	All codes are valid except 6304
Fulfillment Notification Message Reason Codes	All codes are valid except 6305
Chargeback Message Reason Codes	All codes are valid except: • 4540 • 4544 • 4553 • 4554 • 4750
Second Presentment Message Reason Codes	All codes are valid except: • 2007 • 2009 • 2701
Itemized Documentation Codes	All codes are valid except 12

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.5 Special Programs

Special programs with specific requirements exist to facilitate unique processing environments. Refer to Section 4.2.20, "Special Programs," on page 229 for more information.

7.10.5.1 No Signature/No PIN Program

The No Signature/No PIN Program allows a participating S/E to process a Transaction without obtaining the Cardmember's signature or PIN if all the requirements of the No Signature/No PIN Program are met, unless required by local law or regulation. Refer to Section 4.2.20.4, "No Signature/No PIN Program," on page 232.

The following table indicates Message Reason Codes that can be used for Transactions that qualify under the No Signature/No PIN Program (refer to the *Codes Reference Guide* for a list of all valid Message Reason Codes):

Table 7-20. Allowable Codes for No Signature/No PIN Program

Message Types/Code	Valid Codes
Retrieval Request Notification Message Reason Codes	All codes are valid except 6008
Fulfillment Notification Message Reason Codes	All codes are valid except 2700
Chargeback Message Reason Codes	All codes are valid except: • 4516 • 4517 • 4799[1]
Second Presentment Message Reason Codes	All codes are valid except 2700
Itemized Documentation Codes	All codes are valid except 01[2]

1. 4799 is invalid for Transactions that qualify under the No Signature/No PIN Program where the POS device is PIN-capable and enabled.
2. 01 is invalid only with Function Code 602 for Retrieval Request messages only.

7.10.5.2 ZIP Code Verification (ZCV) Program

The ZCV Program allows participating Merchants to submit the Cardmember's Billing address ZIP Code as part of the POS Authorization Request (1100) message for validation by the Issuer.

If a Transaction qualifies under the ZCV Program, certain dispute Message Reason Code restrictions apply. The following table indicates Message Reason Codes that can be used for ZCV Transactions (refer to the *Codes Reference Guide* for a list of all valid Message Reason Codes):

Table 7-21. Allowable Codes for ZCV Program

Message Types/Codes	Valid Codes
Retrieval Request Notification Message Reason Codes	All codes are valid except 6006
Fulfillment Notification Message Reason Codes	All codes are valid except 2700
Chargeback Message Reason Codes	All codes are valid
Second Presentment Message Reason Codes	All codes are valid except 2700
Itemized Documentation Codes	All codes are valid

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.6 Expresspay

An Expresspay Transaction is a Contactless Transaction initiated by the use of an Expresspay-enabled Card or Mobile Device at an Expresspay-enabled POS Device.

If a Transaction qualifies as an Expresspay Transaction, certain dispute Message Reason Code Restrictions apply. The following table indicates Message Reason Codes that can be used for Expresspay-enabled Card Transactions or Expresspay Transactions (refer to the *Codes Reference Guide* for a list of all valid Message Reason Codes):

Table 7-22. Allowable Codes for Expresspay Transactions

Message Types/Codes	Valid Codes
Retrieval Request Notification Message Reason Codes	All codes are valid.[1]
Fulfillment Notification Message Reason Codes	All codes are valid.
Chargeback Message Reason Codes	All codes are valid except: • 4516[2] • 4517[2] • 4527 • 4540 • 4544 • 4798 • 4799
Second Presentment Message Reason Codes	All codes are valid.
Itemized Document Codes	All codes are valid.

1. Refer to Table 7-3, "Retrieval Request Notification Reasons," on page 289 for additional information.
2. These codes are invalid for Expresspay Transactions where the Transaction amount is less than or equal to the country threshold for Expresspay Transactions as indicated in the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide* available on Knowledge Base.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.7 Digital Wallet Program

Digital Wallet Program Transactions are Transactions initiated by a Mobile Device. The five (5) types of Digital Wallet Program Transactions are:

- Digital Wallet Contactless-initiated Transactions
- Digital Wallet Application-initiated Transactions
- Digital Wallet MST Transactions
- Expresspay Mobile Transactions
- Consumer-Presented Quick Response (CPQR) Transactions

If a Transaction qualifies as a Digital Wallet Program Transaction, certain dispute Message Reason Code restrictions apply. The following table indicates Message Reason Codes that can be used for Digital Wallet Program Transactions:

Table 7-23. Allowable Codes for Digital Wallet Payments Transactions

Message Types/Codes	Valid Codes
Retrieval Request Notification Message Reason Codes	Some exclusions apply.[1]
Fulfillment Notification Message Reason Codes	All codes are valid.
Chargeback Message Reason Codes	All codes are valid except: • 4516[2] • 4517[2] • 4527 • 4544 • 4798 • 4799
Second Presentment Message Reason Codes	All codes are valid.
Itemized Document Codes	All codes are valid, except 01[3].

1. Refer to Table 7-3, "Retrieval Request Notification Reasons," on page 289 for additional information.
2. These codes are invalid for Expresspay Transactions where the Transaction amount is less than or equal to the country threshold for Expresspay Transactions as indicated in the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide* available on Knowledge Base.
3. 01 is invalid only with Function Code 602 for Retrieval Request Messages only.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.8 Fraud Liability Shift

A Fraud Liability Shift (FLS) occurs when a Participant fulfills certain policy requirements allowing Chargeback liability to shift to a different Participant.

7.10.8.1 AEIPS Fraud Liability Shift (FLS)

AEIPS FLS assigns fraud liability to the Issuer or Acquirer based on the party having the lowest chip capability at the Point of Sale (POS). Since the Issuer typically bears the liability for counterfeit and lost/stolen/non-received fraud, the liability is shifted to the Acquirer when the Acquirer's S/Es have not upgraded their POS devices to accept and process AEIPS Chip Cards. Global AEIPS FLS policy applies both intra-regionally (where the Issuer and S/E are in the same region) and inter-regionally (where the Issuer and S/E are in different regions). The following table describes the circumstances under which AEIPS Counterfeit and Lost/Stolen/Non-received FLS is assigned:

Table 7-24. AEGNS Assignment of Liability Detail

		Card Type	Tran Type	Liability	Valid FLS ISO Code(s)
Issuer and Acquirer are both in Designated AEIPS FLS Countries	**Issuer Certified**[1]	Chip and PIN	Chip and PIN	**Issuer** (All Fraud)	None[2]
			Chip/No PIN	**Acquirer** (Lost/Stolen/Non-received)[3] **Issuer** (All Other Fraud)	ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-received
			Magnetic Stripe	**Issuer**[4] (if Transaction identified as Fallback in First Presentment) **Acquirer** (All Other Fraud)[3]	ISO 4798 - Fraud Liability Shift - Counterfeit ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-received
		Chip Only	Chip/No PIN	**Issuer** (All Fraud)	None[2]
			Magnetic Stripe	**Issuer** (All fraud except counterfeit, and counterfeit if Transaction identified as Fallback in First Presentment) **Acquirer** (Counterfeit)[5]	ISO 4798 - Fraud Liability Shift - Counterfeit
		Magnetic Stripe	All	**Issuer** (All Fraud)	None[2]
	Issuer Not Certified	N/A	All	**Business As Usual** (Issuer All Fraud)	None[2]

1. Certified for AEIPS and by GNS to the 2.1 Release or greater.
2. "None" refers only to ISO Codes 4798/4799. Other ISO Codes may be valid for the Transaction.
3. Lost/Stolen/Non-received FLS applies when all conditions are met. Refer to Section 7.10.8.1.1, "Types of AEIPS FLS," on page 360 and "ISO 4799 - Fraud Liability Shift - Lost/Stolen/Non-Received" on page 352 for more information.
4. Or Issuer-authorized Card with altered service code data.
5. Counterfeit FLS applies only when all conditions are met. Refer to Section 8.9.1, "High Risk S/E List," on page 383, Section 7.10.8.1.1, "Types of AEIPS FLS," on page 360, or "ISO 4798 - Fraud Liability Shift - Counterfeit" on page 350 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.8.1.1 Types of AEIPS FLS

There are two (2) types of AEIPS FLS:

- Counterfeit FLS - The transfer of counterfeit fraud liability from the Issuer to the Acquirer (using Chargeback ISO Message Reason Code 4798 - Fraud Liability Shift - Counterfeit) for Transactions conducted with an AEIPS Chip Card at a POS device that is unable to process an AEIPS Chip Card Transaction.
- Lost/Stolen/Non-received FLS - The transfer of Lost/Stolen/Non-received liability from the Issuer to the Acquirer (using Chargeback Message Reason Code 4799 - Fraud Liability Shift - Lost/Stolen/Non-received) for Transactions conducted with an AEIPS chip and PIN Card at a POS device that is unable to process an AEIPS chip and PIN Transaction. To qualify, the Transaction must occur at an S/E located in an AEGNS-designated country for AEIPS Lost/Stolen/Non-received FLS. In addition, the Issuer for the Transaction must be located in an AEGNS-designated country for AEIPS Lost/Stolen/Non-received FLS. The following table lists the countries by region, as designated by AEGNS, where AEIPS Lost/Stolen/Non-received FLS is in effect:

Table 7-25. AEIPS Lost/Stolen/Non-Received FLS Participation

Region	Global AEIPS Lost/Stolen/Non-Received FLS Policy Applies in the Following Markets
EMEA	Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Gibraltar, Greece, Greenland, Hungary, Iceland, Ireland, Israel, Italy, Kazakhstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Macedonia (Formerly Yugoslav Republic of), Malta, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, Ukraine
APAC	Marshall Islands, Malaysia
Americas	Brazil, Canada, Caribbean Countries, Mexico, United Status, United States Territories

7.10.8.1.2 PIN Capable and Enabled POS Devices

AEIPS Lost/Stolen/Non-received FLS policy does not apply to Transactions at PIN capable and enabled POS devices that originated from an S/E in Caribbean Countries, United States, or United States Territories. For purposes of this policy, a Transaction at a PIN capable and enabled POS device is defined as a Transaction where both the Point of Service Data Code Position 1 with a value of "5" and Position 2 with a value of "1" were present in the POS First Presentment (1240) message. In addition, the Card Acceptor Country Code will determine whether the Transaction originated from an S/E in Caribbean Countries, United States, or United States Territories.

7.10.8.2 Fallback

Issuers will be liable for Issuer authorized Fallback Transactions if the Transaction was completed at an identified AEIPS Chip-Enabled Device and the Card was AEIPS-compliant but could not be read. For dispute logic purposes, AEGNS will identify Fallback through use of Point of Service Data Codes in the First Presentment record. If the Point of Service Data Code is not sent, AEGNS will assume the Transaction is not Fallback and liability will be assigned to the Acquirer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.8.3 American Express SafeKey Fraud Liability Shift

The SafeKey FLS shifts liability for fraud away from Acquirers and their S/Es for SafeKey Transactions if all of the following requirements are met:

- The Acquirer is certified for SafeKey.
- The Acquirer and S/E are in compliance with the AEGNS SafeKey Acquirer Requirements. Refer to Section 2.9.18, "American Express SafeKey Acquirer Requirements," on page 107.
- The Transaction Authentication was Attempted or Fully Authenticated as provided by the SafeKey service during the Transaction Authentication. This is identified by the Electronic Commerce Indicator (ECI) containing a value of either 06 or 05, respectively, on the POS First Presentment (1240) message or, for Acquirers located in Japan, the Authorization Request (1100) message.
- The S/E is in compliance with the AEGNS S/E fraud monitoring policies. Refer to:
  - Section 8.9.1, "High Risk S/E List," on page 383
  - Section 8.9.3, "S/E Risk Management," on page 388
  - Section 8.9.6, "S/E Monitoring for Fraud Liability Shift Eligibility," on page 391

If all of these requirements are met, the AEGN will provide the Issuer with a Program Indicator on the POS First Presentment (1240) message. The Program Indicator with the SafeKey value indicates that the Transaction qualifies for the SafeKey Fraud Liability Shift. Refer to the *Network Specifications - Financial/Non-Financial* manual for details on the POS First Presentment (1240) message.

AEGNS reserves the right to invalidate SafeKey FLS eligibility from Transactions if either of the following occur:

- The S/E or Cardmember modifies data used for SafeKey Transaction Authentication after the Transaction has been Attempted or Fully Authenticated.
- The S/E uses the American Express Verification Value (AEVV) for an invalid purpose.
- The ECI indicator in the POS Authorization Request (1100) did not contain a value of either 06 or 05.

Issuers may be liable for fraud losses regardless of participation in SafeKey by the Issuer or their Cardmember.

Note: SafeKey Global FLS is not applicable for the following Card products:

- All anonymous Card Products (see Section 2.10.13, "American Express SafeKey Issuer Requirements," on page 119)
- United States-issued Prepaid Cards

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The following table indicates Message Reason Codes that can be used for Transactions that qualify for SafeKey:

Table 7-26. Allowable Codes for SafeKey

Message Type/Code	Valid Codes
Retrieval Request Notification Reason Codes	All codes are valid except: • 6003[1] • 6008
Chargeback Message Reason Codes	All codes are valid except: • 4516 • 4517 • 4540[2]
Itemized Document Codes	All codes are valid except 01[3]

1. 6003 is invalid only with Chargeback ISO Codes 4540 and 4763.
2. 4540 is invalid only if the Transaction qualifies for SafeKey FLS.
3. 01 is invalid only with Function Code 602 for Retrieval Request messages only.

7.10.9 Promotional Program Transactions

The following applies to Chargebacks processed on Promotional Program Transactions:

- Cardmember's Transaction for the purchase - The Issuer must process the dispute Transaction using the Chargeback ISO Code that matches the dispute reason (e.g., ISO Code 4540 - Card Not Present, ISO Code 4554 - Goods and Services Not Received, etc).
- Promotional Program Debit and Credit Transactions - Issuers and Acquirers must process dispute Transactions through the AEGNS Network Disputes Manager Good Faith process. Section 7.11, "Good Faith," on page 364 for additional information.

Note: AEGNS will reject all Retrieval Request and Chargeback Transactions that are submitted on the Debit and Credit Promotional Program Transactions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.10.10 Merchant-Presented Quick Response

Merchant-Presented Quick Response (MPQR) is an Issuer Originated Payment (IOP) Transaction that allows Cardmembers to initiate Transactions using an Issuer application on a Mobile Device to capture a Merchant-Presented QR Code.

MPQR Transactions are identified in the POS First Presentment (1240) message and the Authorization Request (1100) message with value "8" in Position 6 and value "7" in Position 3 of the Point of Service Data Code field.

Note: If AEGNS is the Token Service Provider (TSP), AEGNS will provide a PAN to Token translation service on behalf of the Issuer.

The following table indicates the Message Reason Codes that can be used for MPQR Transactions:

Table 7-27. Allowable Codes for Merchant-Presented Quick Response

Message Type/Code	Valid Codes
Retrieval Request Notification Reason Codes	All codes are invalid.
Chargeback Message Reason Codes	All codes are valid except: • 4516 • 4517 • 4521 • 4523 • 4527 • 4534 • 4540 • 4544 • 4755 • 4763[1] • 4798 • 4799
Second Presentment Message Reason Codes	All codes are valid.
Itemized Document Codes	All codes are valid.

1. 4763 is invalid only with an HRSE Indicator of “F.”

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.11 Good Faith

The Good Faith process allows Acquirers and Issuers to resolve issues outside of the Chargeback process.

For Good Faith Transactions, the transfer of financial liability will only occur following agreement by both Acquirer and Issuer.

This section covers the policy for Participants submitting Good Faith Transactions.

7.11.1 Good Faith Request

An Acquirer or Issuer may submit a Good Faith request to the other Participant where the filing Participant identifies a Transaction that could be resolved outside of the Chargeback process. Examples may include, but are not limited to:

- An Issuer processed a Chargeback then subsequently received a credit for the Transaction.
- A Participant did not process a dispute Transaction within the necessary timeframes.
- A Participant receives additional pertinent information after submission of a dispute Transaction.

All POS and ATM Transactions are eligible for Good Faith processing.

Note: All pre-Arbitration and pre-Compliance requests are processed through the Good Faith Request process.

7.11.2 Good Faith Filing Procedures

When a Participant identifies a Transaction that could be resolved through a Good Faith request, that Participant contacts the other Participant involved in the Transaction to request approval to process a Good Faith request. Good Faith requests can be submitted by a Participant through the automated or manual Good Faith submission process. Refer to Section 7.11.2.1, "Automated Good Faith Submission," and Section 7.11.2.2, "Manual Good Faith Submission," on page 365 for additional information. The sending Participant must provide all information and supporting Documentation to the receiving Participant to facilitate analysis and resolution of the Good Faith request.

Receiving Participants are not obliged to accept all Good Faith requests. Receiving Participants are required to review and consider each request in light of its individual merits and must respond to the sending Participant. Participants that do not respond are subject to a non-response fee.

Participants must deliver a Good Faith response using the same submission process as the Good Faith request. For example, if the Good Faith request was received via the AEGNS Network Disputes Manager automated Good Faith submission process, then the Good Faith response must be submitted using the AEGNS Network Disputes Manager automated Good Faith submission process. If the Good Faith request was received via the manual Good Faith submission process, then the Good Faith response must be submitted using the manual Good Faith submission process.

AEGNS will process financial adjustments for the amount approved by the receiving Participant and Good Faith fees. These financial adjustments will be reflected in the Participant's Daily Activity Report and/or Daily Settlement Advisement.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.11.2.1 Automated Good Faith Submission

Participants should refer to the *Network Disputes Manager - User Guide* for additional information on the functions and features of the AEGNS Network Disputes Manager automated Good Faith submission process.

Participants must submit automated Good Faith submission requests for POS and ATM Transactions within 720 days from the Network Processing Date of the First Presentment.

Requesting Participants should not submit more than one (1) automated Good Faith submission request on the same Transaction at any one (1) time. Subsequent Good Faith requests are allowed only after previous Good Faith requests have been accepted, cancelled, or declined.

7.11.2.2 Manual Good Faith Submission

Participants must utilize the manual Good Faith submission process only for Good Faith requests for POS and ATM Transactions greater than 720 days from the Network Processing Date of the First Presentment, or for pre-Compliance not relating to a Transaction. AEGNS will not process manual Good Faith requests for POS and ATM Transactions received less than 720 days from the Network Processing Date of the First Presentment.

Upon receipt of a written acceptance response, a filing Participant should submit a properly completed AEGNS Good Faith Form together with the receiving Participant's written acceptance and a copy of supporting Documentation, if appropriate, to AEGNS Good Faith. This can be sent via email with return receipt request to GNSgoodfaiths@aexp.com or via the postal service. Refer to Section 7.11.5, "Good Faith Submission Address," on page 366 for more information.

Refer to "Exhibit 18. AEGNS Good Faith Form" on page 486 for a copy of the AEGNS Good Faith Form.

If a Participant submits a Good Faith Form without the receiving Participant's proper written approval or the Good Faith Form is incomplete, AEGNS will reject the Good Faith request and inform both Participants.

7.11.3 Good Faith Processing Timeframes

AEGNS will provide the Participant's Good Faith contact, as listed in the Participant Directory, a detailed listing of the prior month's approved Good Faith Transaction amounts and applicable fees no later than the 15th of the month. These financial adjustments will be reflected in the Participant's Daily Activity Report and/or Daily Settlement Advisement.

7.11.4 Good Faith Fees

All approved Good Faith requests processed by AEGNS are subject to a processing fee. This processing fee will be charged to both Participants for each approved Good Faith request. Participants that do not respond to a Good Faith Request are subject to a non-response fee. Refer to Section 10.2.4, "Good Faith Fees," on page 402 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.11.5 Good Faith Submission Address

Participants utilizing the manual Good Faith submission process must submit the completed Good Faith Form, a copy of the written approval from the other Participant, and all required supporting Documentation to the following address for processing:

AEGNS Arbitration Committee
American Express (India) Private Limited
Network Policy Compliance Team
14th Floor, Tower-C
Building No. 5
DLF Cyber City, Phase - III
Gurgaon - 122002 (Haryana)
India

7.11.6 Good Faith Corrections and Reversals

Participants who approve a Good Faith request and subsequently wish to reverse the Transaction will be required to initiate a new Good Faith request back to the original filing Participant.

Note: There may be situations in which an Arbitration Filing is submitted by the Acquirer and is subsequently withdrawn prior to the filing review. After the withdrawal, if funds are still required to be exchanged, Participants should not submit a Good Faith request to initiate the movement of funds. Participant reporting and funds movement (to include disputed amount and filing fee) will be executed as part of the Arbitration withdrawal process.

7.11.7 Good Faith Arbitration Withdrawal Procedure

If the receiving Participant accepts or approves the Good Faith request, the accepting Participant must withdraw the Arbitration case (if any) in the AEGNS Network Disputes Manager (NDM), for appropriate financial adjustment, within thirty (30) days from the date the Arbitration filing was accepted by the AEGNS Arbitration Committee. Failure to do so will result in a case review process as described in Section 7.12.3.1, "Review Process for Accepted Filings," on page 373. The AEGNS Arbitration and Compliance Committee may assess a penalty fee against Participants who fails to withdraw an Arbitration case after accepting or approving a Good Faith request. Refer to Table 10-2, "Arbitration Fees," on page 402.

7.12 Arbitration and Compliance

The Arbitration and Compliance processes allow Acquirers and Issuers to resolve issues outside of the Chargeback process. All decisions of the AEGNS Arbitration Committee are final, and all Acquirers and Issuers are required to comply with these decisions and accept the financial liability as determined by the AEGNS Arbitration Committee.

This section covers the processes for Participants submitting an Arbitration Filing or Compliance Filing to the AEGNS Arbitration Committee.

7.12.1 Arbitration

If an Acquirer determines, based on a review of the Final Chargeback and any further supporting Documentation provided by the Issuer and the relevant Network rules, that there is sufficient justification to dispute the Final Chargeback, an Arbitration Filing may be submitted through AEGNS Network Disputes Manager to the AEGNS Arbitration Committee. Acquirers are strongly encouraged, but not required, to pursue a pre-Arbitration attempt (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information) prior to submitting an Arbitration Filing.

An Acquirer must submit separate Arbitration Filings for each disputed Transaction.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.12.1.1 Arbitration Filing Procedures

The Arbitration Filing consists of:

- A submission through AEGNS Network Disputes Manager and attachments containing:
  - A narrative description of the problem
  - The sequence of events in chronological order

  Refer to the *Network Disputes Manager - User Guide* on Knowledge Base for additional information.
- Legible copies of all the documents provided as support of the Retrieval Request/Fulfillment (if required), First Chargeback, Second Presentment, and Final Chargeback. Submitted documents must have been exchanged between Participants during the Disputes Process Transaction Life Cycle and, if applicable, pre-Arbitration (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information). Acquirers must clearly mark each document to indicate which stage in the Disputes Process Transaction Life Cycle it was exchanged.
- If Arbitration Filing with Documentation exceeds the maximum number of attachments allowed through AEGNS Network Disputes Manager, the Acquirer must submit the additional Documentation in writing, in a manner which provides signed proof of delivery, to:

  AEGNS Arbitration Committee
  American Express (India) Private Limited
  Network Policy Compliance Team
  14th Floor, Tower-C
  Building No. 5
  DLF Cyber City, Phase - III
  Gurgaon - 122002 (Haryana)
  India

  If applicable, documentation must be translated and provided in English.

  A copy of all materials sent to the AEGNS Arbitration Committee address must also be sent, in a manner which provides signed proof of delivery, to the Arbitration/Compliance contact listed in the Participant Directory for the receiving Network Issuer. The Acquirer is required to provide proof that the additional Arbitration Filing Documentation was sent to the Issuer. Refer to Section 7.3.2.14, "Documentation Delivery," on page 285 for additional information.

Failure to adhere to Arbitration Filing procedures will result in:

- Rejection (provisional or final) of a filing by the AEGNS Arbitration Committee based on Section 7.12.3, "AEGNS Arbitration and Compliance Filing Review Process," on page 372.
- Forfeiture of the filing fee by the Acquirer
- Possible assessment of penalty fees against the Acquirer based on Section 7.12.1.3, "Arbitration Fees," on page 368.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.12.1.2 Arbitration Submission Timeframe

An Arbitration Filing must be submitted through AEGNS Network Disputes Manager with all related Documentation within forty-five (45) days of the Network Processing Date of the Final Chargeback.

Any documents sent to AEGNS shall be deemed received on the day that a filing number has been created by AEGNS Network Disputes Manager. Refer to the *Network Disputes Manager - User Guide* on Knowledge Base for additional information on the functions and feature of the AEGNS Arbitration Submission process.

Any additional Documentation sent in writing must be received by the AEGNS Arbitration Committee within forty-five (45) days of the Network Processing Date of the Final Chargeback.

When calculating the forty-five (45) days, Participants must take into account that delivery will only be accepted by AEGNS on Monday through Friday during normal business hours. Where the 45th day is a holiday in India, delivery will be accepted on the next Business Day. It is the filing party's responsibility to ensure that its Arbitration Filing has been received and acknowledged by the AEGNS Arbitration Committee within the appropriate timeframe.

7.12.1.3 Arbitration Fees

All Arbitration Filings submitted through AEGNS Network Disputes Manager to the AEGNS Arbitration Committee are subject to a filing fee, penalty fee, and Arbitration review fee as described in Section 10.2.3, "Arbitration Fees," on page 402 and Table 10-2, "Arbitration Fees," on page 402. The AEGNS Arbitration Committee may assess a penalty fee(s) against either party involved in the dispute, whether or not the ruling is in their favor, should it determine that the party violated Network policy. AEGNS will process a debit financial adjustment for the appropriate fee(s) upon resolution of a filing. These financial adjustments will be reflected in the Participant's Daily Activity Report and/or Daily Settlement Advisement.

- **Filing fee:** This fee will be assessed on all submitted filings, including filings re-submitted by Acquirers following a provisional reject by the AEGNS Arbitration Committee. Filings re-submitted by Acquirers following provisional rejection by the AEGNS Arbitration Committee will be subject to a new filing fee. Acquirers will remain liable for filing fees on rejected filings. The filing fee on accepted filings will be collected from the responsible Participant(s) upon resolution of the filing.
- **Penalty fee:** This fee may be assessed against Participants who violated Network policy. The AEGNS Arbitration Committee may assess multiple penalty fees against either or both Participants if it determines that the Participant violated Network policy during the processing of the Transaction. Penalty fees may be assessed against either Participant regardless of whether or not the ruling is in their favor.
- **Arbitration review fee:** This fee will be assessed thirty (30) days from the date the AEGNS Arbitration Committee accepts the filing and will be collected from the responsible Participant(s) upon resolution of the filing. Filings withdrawn by either party within thirty (30) days from the date the filing was accepted by the AEGNS Arbitration Committee will not be reviewed by the AEGNS Arbitration Committee and are not subject to the Arbitration review fee.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.12.1.4 Arbitration Withdrawal Procedures

If the receiving Issuer agrees to accept the financial liability for an Arbitration Filing, the Issuer may submit a withdrawal request through AEGNS Network Disputes Manager within thirty (30) days from the date the filing was accepted by the AEGNS Arbitration Committee, stating the reason for the withdrawal. AEGNS will collect the filing fee from the accepting Issuer and move financial liability for the Transaction from the Acquirer to the Issuer within forty-five (45) days of the date of acceptance as part of the Arbitration withdrawal process. These financial adjustments will be reflected in the Participant's Daily Activity Report and/or Daily Settlement Advisement.

In the event the Acquirer determines a filing was submitted and should be withdrawn, the Acquirer may submit a withdrawal request through AEGNS Network Disputes Manager within thirty (30) days from the date the filing was accepted by the AEGNS Arbitration Committee, stating the reason for the withdrawal. Notification by the Acquirer to the AEGNS Arbitration Committee of its desire to stop further action on the filing will result in the forfeiture of the filing fee.

Note: There may be situations in which an Arbitration Filing is submitted by the Acquirer and is subsequently withdrawn prior to the filing review. After the withdrawal, if funds are still required to be exchanged, Participants should not submit a pre-Arbitration Request (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information) to initiate the movement of funds. Participant reporting and funds movement (to include disputed amount and filing fee) will be executed as part of the Arbitration withdrawal process.

7.12.2 Compliance

An Acquirer or Issuer may submit a Compliance Filing through AEGNS Network Disputes Manager to the AEGNS Arbitration Committee when they can provide valid Documentation of a violation of the policies in the *Business and Operational Policies* manual at the time of the Transaction or violation by another Participant. The Compliance Filing must meet the following criteria:

- A right of First Chargeback, Second Presentment and/or Final Chargeback is not and was not available during the Disputes Process Transaction Life Cycle, and
- The filing Participant is able to provide evidence that they have or will suffer a financial loss due to the violation. The Participant may not use the violation itself as the sole reason for considering a Compliance Filing, and
- The filing Participant has attempted pre-Compliance (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information) to resolve the dispute and that effort has not been successful.

All pre-Compliance correspondence and Documentation regarding the Compliance Filing must be sent to the receiving Participant at least thirty (30) days before the initiating Participant files a Compliance Filing.

Participant(s) may submit one (1) Compliance Filing for multiple linked Transactions, where the violation circumstances are identical. Refer to the *Network Disputes Manager - User Guide* for additional information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.12.2.1 Compliance Filing Procedures

The Compliance Filing consists of:

- A submission through AEGNS Network Disputes Manager and attachments containing:
  - A narrative description of the violation
  - The specific policy that was violated
  - The sequence of events in chronological order

  Refer to the *Network Disputes Manager - User Guide* for additional information regarding Compliance forms and attachments.
- Legible copies of all the documents provided in support of the pre-Compliance request (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information).
- If applicable, legible copies of all documents supplied in support of Retrieval Request/Fulfillment, First Chargeback and Second Presentment
- A description and supporting Documentation to validate the financial loss incurred or to be incurred
- If Compliance Filing Documentation (refer to Section 7.3.2.14, "Documentation Delivery," on page 285) exceeds the maximum number of attachments allowed through AEGNS Network Disputes Manager, the sending Participant must submit the additional Documentation in writing in a manner which provides signed proof of delivery, to the AEGNS Arbitration Committee at:

  AEGNS Arbitration Committee
  American Express (India) Private Limited
  Network Policy Compliance Team
  14th Floor, Tower-C
  Building No. 5
  DLF Cyber City, Phase - III
  Gurgaon - 122002 (Haryana)
  India

  A copy of all materials sent to the AEGNS Arbitration Committee address must also be sent, in a manner which provides signed proof of delivery, to the Arbitration/Compliance contact listed in the Participant Directory for the receiving Participant. The filing Participant is required to provide proof that the additional Compliance Filing Documentation was sent to the receiving Participant. Refer to Section 7.3.2.14, "Documentation Delivery," on page 285 for additional information.

Failure to adhere to Compliance Filing procedures will result in:

- Rejection (provisional or final) of a filing by the AEGNS Arbitration Committee as described in Section 7.12.3, "AEGNS Arbitration and Compliance Filing Review Process," on page 372
- Forfeiture of the filing Participant's filing fee
- Possible assessment of penalty fees as described in Section 7.12.2.3, "Compliance Fees," on page 371

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.12.2.2 Compliance Submission Timeframe

Compliance Filings must be submitted through AEGNS Network Disputes Manager with all related Documentation within the timeframes listed below:

- For violations involving a Transaction, the Compliance Filing must be submitted through AEGNS Network Disputes Manager within 180 days from the Network Processing Date of the Presentment.
- For any violations not involving a Transaction, the Compliance Filing must be submitted through AEGNS Network Disputes Manager within 180 days from the date the violation occurred.

Any documents sent to AEGNS shall be deemed received on the day that a filing number has been created by AEGNS Network Disputes Manager. Refer to the *Network Disputes Manager - User Guide* for additional information.

Any additional Documentation sent in writing must be received by AEGNS Arbitration Committee within the timeframes outlined in this section. When calculating the 180 days, Participants must take into account that delivery will only be accepted by AEGNS on Monday through Friday during normal business hours. Where the 180th day is a holiday in India, delivery will be accepted on the next Business Day. It is the filing party's responsibility to ensure that its Compliance Filing has been received and acknowledged by the AEGNS Arbitration Committee within the appropriate timeframe.

7.12.2.3 Compliance Fees

All Compliance Filing submitted through AEGNS Network Disputes Manager to the AEGNS Arbitration Committee are subject to a filing fee, penalty fee, and compliance review fee as prescribed in Section 10.2.5, "Compliance Fees," on page 402 and Table 10-3, "Compliance Fees," on page 402.

The AEGNS Arbitration Committee may assess a penalty fee(s) against either party involved in the dispute, whether or not the ruling is in their favor, should it determine that the party violated Network policy. AEGNS will process a debit financial adjustment for the appropriate fee(s) upon resolution of a filing. These financial adjustments will be reflected in the Participants' Daily Activity Report and/or Daily Settlement Advisement. See Section 10.2.5, "Compliance Fees," on page 402.

- **Filing fee:** This fee will be assessed on all submitted filings, including filings re-submitted by Participants following a provisional reject by the AEGNS Arbitration Committee. Filings re-submitted following provisional rejection by the AEGNS Arbitration Committee will be subject to a new filing fee. Filing Participants will remain liable for filing fees on rejected filings. The filing fee on accepted filings will be collected from the responsible Participant(s) upon resolution of the filing.
- **Penalty fee:** This fee may be assessed to Participants who violate Network policy in the dispute. The AEGNS Arbitration Committee may assess multiple penalty fees against either or both Participants if it determines that the Participant violated Network policy during the dispute. Penalty fees may be assessed against either Participant regardless of whether or not the ruling is in their favor.
- **Compliance review fee:** This fee will be assessed thirty (30) days from the date the AEGNS Arbitration Committee accepts the filing and will be collected from the responsible Participant(s) upon resolution of the filing. Filings withdrawn by either party prior to
thirty (30) days from the date the filing was accepted by the AEGNS Arbitration Committee will not be reviewed and are not subject to the Compliance review fee.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

7.12.2.4 Compliance Withdrawal Procedures

If the receiving Participant agrees to accept the financial liability for a Compliance Filing the receiving Participant must submit a withdrawal request through AEGNS Network Disputes Manager, within thirty (30) days from the date the filing was accepted by the AEGNS Arbitration Committee, stating the reason for the withdrawal. AEGNS will collect the filing fee from the accepting Participant and move financial liability from the filing Participant to the receiving Participant within forty-five (45) days of the date of acceptance as part of the Compliance Filing withdrawal process. These financial adjustments will be reflected in the Participant's Daily Activity Report and/or Daily Settlement Advisement.

In the event the filing Participant determines a filing was submitted and should be withdrawn, the filing Participant may submit a withdrawal request through AEGNS Network Disputes Managers, within thirty (30) days from the date the filing was accepted by the AEGNS Arbitration Committee stating the reason for the withdrawal. Notification by the filing Participant to the AEGNS Arbitration Committee of its desire to stop further action on the filing will result in the forfeiture of the filing fee.

Note: There may be situations in which a Compliance Filing is submitted by the Participant and is subsequently withdrawn prior to the filing review. After the withdrawal, if funds are still required to be exchanged, Participants should not submit a pre-Compliance Request to initiate the movement of funds. Participant reporting and funds movement (to include disputed amount and filing fee) will be executed as part of the Compliance Filing withdrawal process.

7.12.3 AEGNS Arbitration and Compliance Filing Review Process

Upon receipt of an Arbitration or Compliance Filing by the AEGNS Arbitration Committee, the filing will be reviewed to determine if it meets the AEGNS procedural filing requirements.

The AEGNS Arbitration Committee may refuse to accept a filing for any of the following reasons:

1. Insufficient Documentation of the criteria described in Section 7.12.1, "Arbitration," on page 366 or Section 7.12.2, "Compliance," on page 369 as applicable;
2. For a Compliance Filing, the pre-Compliance requirements were not fulfilled properly, not fulfilled at all, or not fulfilled within the required timeframe, as required by Section 7.12, "Arbitration and Compliance," on page 366. Acquirers are required to pursue a pre-Compliance attempt (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information).
3. For an Arbitration Filing, the necessary steps in the Chargeback process were not completed; or
4. The filing was submitted past the timeframe (i.e., for an Arbitration Filing, the timeframe specified in Section 7.12.1.2, "Arbitration Submission Timeframe," on page 368, and, for a Compliance Filing, the timeframe specified in Section 7.12.2.2, "Compliance Submission Timeframe," on page 371.)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

If the AEGNS Arbitration Committee determines that a filing falls into one (1) of the above categories, it may:

- Make a provisional rejection of the filing.

  If a filing is not accepted by the AEGNS Arbitration Committee for reasons one (1) or two (2) above, the items to fix the reject may be resubmitted through AEGNS Network Disputes Manager, provided it complies with all of the following requirements:
  - The Participant making the second filing cured all the procedural defect(s) or violation(s) for which the filing was originally not accepted and the second filing, as submitted, cannot be rejected by the Committee for one (1) or more of the other procedural violations or defects outlined in items one (1) to four (4) above.
  - The Participant submitted the second filing within the original required timeframe allowed under the *Business and Operational Policies* manual for the original filing.
  - The filing fee for the second filing may be forfeited if the filing criteria are not met.
- Make a final rejection of the filing.

If a filing is not accepted by the AEGNS Arbitration Committee because of reasons three (3) or four (4) above, such disposition shall be deemed a final decision, the Participant shall have no further recourse (i.e., be precluded from having the AEGNS Arbitration Committee rule on the substantive merits of the filing), and the filing fee will be forfeited.

7.12.3.1 Review Process for Accepted Filings

If the AEGNS Arbitration Committee accepts the filing, it will conduct the review process under the following guidelines:

1. For all filings that comply with the filing requirements, the AEGNS Arbitration Committee will review the facts and supporting Documentation presented by the Participants, and may conduct further investigation as it deems appropriate. The Committee shall base any decision on the Purpose and intent of the Chargeback rules and any other relevant section(s) of the *Business and Operational Policies* manual. Unless otherwise stated in the Chargeback rule, the Committee shall refer to and base its decision on the *Business and Operational Policies* manual in effect and subsequent *Network Participant Updates* as of the Transaction Date of the particular Transaction that is at issue in the filing.
2. Participants in the dispute must fully cooperate in the review process and must make available any relevant records or other Documentation as required by the AEGNS Arbitration Committee.
3. Where a Compliance Filing has been accepted, the AEGNS Arbitration Committee will allow the receiving Participant an opportunity to submit any Documentation it deems appropriate in the form of a rebuttal response to the filing through AEGNS Network Disputes Manager. Receiving Participants are actively encouraged to take this opportunity to provide additional clarification on the filing.
4. Where an Arbitration Filing has been accepted, the AEGNS Arbitration Committee will not accept any Documentation other than that which was previously exchanged by the Acquirer and Issuer during the standard Chargeback processing cycle. When the Arbitration filing is received in the Issuer AEGNS Network Disputes Manager inbox, such Issuer should immediately verify the accuracy of the attached Documentation and is actively encouraged to take this opportunity to report any discrepancies and provide additional clarification on the filing in the form of an Issuer rebuttal through AEGNS Network Disputes Manager.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5. Numbers three (3) and four (4) above establish the review and rebuttal process for Participants against whom the filing is submitted. Participants should provide a rebuttal to an Arbitration or Compliance filing through AEGNS Network Disputes Manager within thirty (30) days from the date the AEGNS Arbitration Committee accepts the filing. Failure to file a rebuttal within thirty (30) days will constitute agreement that the submitted Documentation is accurate. The date the AEGNS Arbitration Committee accepts the filing will be shown in the Participants' AEGNS Network Disputes Manager inbox and AEGNS Network Disputes Manager reports.
6. If a Good Faith request is accepted or approved, the Arbitration case must be withdrawn in AEGNS Network Disputes Manager (NDM) as described in Section 7.11.7, "Good Faith Arbitration Withdrawal Procedure," on page 366.
7. At the conclusion of the review process, the AEGNS Arbitration Committee will issue a ruling that will constitute a final decision regarding the complaint. AEGNS will process a financial adjustment for reimbursement to a Participant that receives a ruling in its favor and collect from the other Participant for the amount in question plus the appropriate fee within forty-five (45) days of the date of the ruling letter. If the filing Participant is found responsible for the disputed amount, they will automatically forfeit the filing fees and have no further recourse for the disputed amount.

The Arbitration Committee decision may result in either:

- One (1) Participant assigned full liability or
- Participants sharing financial liability

The Arbitration and Compliance processes described in this section are the sole Network remedies for Participants with respect to Chargeback disputes and policy violations.

7.12.3.1.1 Filing Review Process Timeframe

The AEGNS Arbitration Committee will use reasonable efforts to complete the filing review process and communicate its decision to both the filing and receiving Participants involved in the filing within seventy-five (75) days from the date of acceptance of the filing by the AEGNS Arbitration Committee. The Arbitration Committee allows thirty (30) days for rebuttal or withdrawal from the accepted date and forty-five (45) days for review and decision. The date the AEGNS Arbitration Committee accepted the filing will be shown in the Participants' AEGNS Network Disputes Manager inbox and AEGNS Network Disputes Manager reports.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8 Security and Fraud

8.1 Introduction

This chapter provides Participants with information that will enable them to maintain a high level of security across the Network. The chapter provides details of security requirements regarding the production and delivery of Cards, security management, fraud reporting, risk monitoring, and risk management.

8.2 Card Production

Card Production includes all processes related to the security of manufacturing and personalization of Cards. Issuers and Card Production Vendors involved in Card Production must comply with all requirements set forth in the following sections. In addition to complying with the AEGNS DSP, all entities involved in Card Production must comply with the relevant *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

Participants that do not comply with any requirements detailed in this policy are subject to non-compliance fees as described in Section 10.7.1, "General Non-Compliance Fees," on page 411.

8.2.1 Certification Requirements for Card Production

All entities, including Mobile Entities, involved in the manufacturing and personalization of Cards and Expresspay Mobile for Issuers must be certified by AEGNS in order to produce and personalize Cards and Expresspay Mobile for Issuers for use on the Network.

Certification by the Network does not constitute a guarantee nor does it release the Issuer from their contractual responsibility to any third party. Lists of certified Card manufacturers and Card personalization vendors are available on Knowledge Base.

All Card Production entities must meet the requirements of the AEGNS Network Cards chapter in the *Network Specifications - Instructions* manual, the Card Production-related content under the Marketing section on Knowledge Base, and other applicable AEGNS Guidelines including, but not limited to, the AEIPS Chip Card Specifications, Expresspay Card Specifications, Expresspay Mobile Specifications, *Issuer Expresspay Mobile Implementation Guide, Expresspay Mobile Device Certification Process Guide, Expresspay Mobile HCE Issuer Implementation Guide, Expresspay Mobile HCE Security Requirements Guide,* and *Expresspay Mobile Secure Element Certification Process Guide*.

All certified Card Production Vendors must have executed an agreement with the Issuer, containing the detailed requirements related to all Card manufacturing and Card personalization services those entities provide. In addition, all certified Card Production Vendors must use a Card Production Security Assessor (CPSA) Company in compliance with the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

AEGNS may suspend or revoke its approval for a certified Card Production Vendor to produce Cards for use on the Network should a certified Card Production Vendor violate the terms and conditions of the agreement between it and the Issuer or fail to comply with the requirements of the Card Production policy.

AEGNS will provide Issuers with written notification ninety (90) days prior to the revocation of the Certification of a Card Production Vendor. AEGNS reserves the right to suspend a Card Production Vendor with less than ninety (90) days' notice in the event of a material violation of the terms of the AEGNS Certification.

The Issuer and its Card Production Vendors bear all liability and responsibility for Cards and Mobile Devices.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Unless otherwise provided for in an Issuer's written agreement with the certified Card Production Vendor, the certified Card Production Vendor's responsibility and liability for Cards ceases and becomes the responsibility of the Issuer or its Mobile Entities, including Service Providers, as applicable, upon shipment or pickup from the certified Card Production Vendor's facility.

AEGNS and American Express Entities have no liability for any losses, costs, expenses, or liability incurred by the Issuer or for damages (including without limitation, special, indirect, consequential, exemplary, speculative, punitive damages), lost profits, expenses, or costs incurred by the Issuer as a result of acts or omissions of the certified Card Production Vendor or of suspension or revocation of the certified Card Production Vendor's Certification to produce Cards.

8.2.2 Sensitive Materials

All materials used in Card Production are to be considered sensitive, and the manufacturing or personalization entity's security must be considered compromised should loss or theft occur.

Sensitive materials include, but are not limited to the following:

- Partial or completed printed Card stock
- Personalized Cards
- Magnetic stripe materials
- Signature panel materials
- Holographic devices
- Encryption and validation software and hardware
- Cardmember Account numbers or other Cardmember Information
- Card design, specifications, and any high-resolution artwork
- EMV Integrated Circuit Card (ICC) chips

Issuers and Card Production Vendors must also comply with the requirements on handling and securing sensitive materials during Card Production as detailed in the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

All sensitive materials must be secured under procedures requiring the supervision of two (2) employees. Each step in the Card Production process should include blind count reconciliation. Packaging and transportation guidelines described in Section 8.3, "Shipments from Card Manufacturer to Card Personalization Site," on page 378 and Section 8.4, "Delivery of Personalized Cards to Cardmembers," on page 378 must be followed when shipping sensitive materials.

8.2.3 Access Control

All Card Production Vendor and Issuers must comply with the access control requirements detailed in the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.2.4 Notification in Case of Loss or Theft During Card Production

All entities involved in Card Production must comply with the notification requirements detailed in the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

The Card Production Vendor or Issuer must notify AEGNS within twenty-four (24) hours following the discovery of loss or theft or suspected loss or theft of Cards and/or Card materials, including Account Data, via email at gnsfraud@aexp.com. Subsequent to the initial report, any additional information relating to the loss or theft must be reported to AEGNS via email at gnsfraud@aexp.com within twenty-four (24) hours of its discovery.

Issuers that do not comply with the notification requirements as stated in this policy, including the obligation of Card Production Vendors to immediately notify Issuers of loss or suspected loss or theft of Cards and/or Card materials, including Account Data, may be subject to non-compliance fees as described in Section 10.6.2, "Notification of Data Compromise Non-Compliance Fees," on page 411.

8.2.5 Reporting in Case of Loss or Theft During Card Production

Following notification in case of the suspected, confirmed, or attempted loss or theft of Cards and/or Card Production materials, including Account Data, Issuers, and Card Production Vendors must report to AEGNS all known information regarding the loss or theft in accordance with the requirements stated in this section. Issuers and Card Production Vendors must also comply with the reporting requirements in case of loss or theft during Card Production as detailed in the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

All Issuers and Card Production Vendors involved in Card Production must include the following additional information when reporting the suspected, confirmed or attempted theft or loss of Cards and/or Card Production materials, including Account Data:

- Description and quantity of all Card Production materials, Cards and information suspected, or confirmed of being misappropriated, lost, or stolen including, but not limited to:
  - Cardmember Account numbers,
  - Cardmember Information,
  - Other information serving to identify the Cards or Cardmembers,
  - Type of Card(s) missing,
  - Number of Card(s) missing,
  - Batch number(s) involved,
  - Effective and Expiration Date(s) of the Card(s).
- Issuer(s) affected,
- Potential for compromise, i.e., percentage of order completed,
- Date, time, and location (including address) that the suspected, confirmed or attempted loss or theft occurred and the identity of any suspects,
- Name, telephone number and address of any law enforcement or other third party notified or involved.
- Pertinent details regarding the loss and the ensuing investigation,

Issuers that do not comply with the reporting requirements as stated in this policy, including the reporting obligation of Card Production Vendors to Issuers in case of loss or suspected loss of Cards and/or Card materials, including Account Data, may be subject to non-compliance fees as described in Section 10.6.1, "Data Security Policy (DSP) Non-Compliance Fees," on page 411.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.2.6 Card Production Audit Controls

Card Production Vendors and Issuers must maintain audit control logs throughout the manufacturing and personalization phases of Card Production to ensure the security of both physical and logical components of the process. For details on Card Production audit controls, refer to the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

AEGNS reserves the right to inspect the premises of Issuers or their vendors/Service Providers at any time to ensure full compliance with the operating rules described in this policy. AEGNS also reserves the right to request, at its own discretion, any Documentation validating the correct execution and monitoring of all policies and processes related to Card Production.

Issuers may be liable for costs associated with inspections conducted by AEGNS.

8.3 Shipments from Card Manufacturer to Card Personalization Site

AEGNS requires Issuers to ensure that their Card manufacturers comply with all requirements regarding preparation, packaging, shipment, and storage as detailed in the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

All Cards must be inventoried by the Issuer or Card personalization vendor immediately upon receipt and periodically thereafter to ensure complete Card accountability.

If a discrepancy is discovered and cannot be accounted for and resolved, AEGNS must be notified at gnsfraud@aexp.com no later than twenty-four (24) hours after the discrepancy is found.

8.4 Delivery of Personalized Cards to Cardmembers

This chapter summarizes requirements related to the delivery of personalized Cards to Cardmembers.

8.4.1 Preparation for Delivery

Prior to delivery, every possible precaution must be taken to ensure that the address of the Cardmember is correct. The address must contain a postal code, where used by the postal system.

AEGNS recommends that the mailing be prepared by the Issuer's own employees in-house and not by a mailing house or temporary employees. However, if the Issuer expects to use a third party, the Issuer must notify AEGNS in writing at gnsfraud@aexp.com thirty (30) days prior to using such third party. The third party must be certified by AEGNS and follow all security standards established for the AEGN.

8.4.2 Precautions Against Mail Theft

Issuers must make sure that PIN mailers and Cards are mailed separately in accordance with the Card delivery-related requirements detailed in the *PCI Card Production and Provisioning Logical Security Requirements and PCI Card Production and Provisioning Physical Security Requirements*, which are available at www.pcisecuritystandards.org.

Issuers must pay particular attention to postal codes and other destination areas where mail thefts are known to occur. In these areas special mailing or delivery procedures must be considered including, but not limited to, registered mail, certified mail, Cardmember pickup with identification, and personal or carrier delivery.

Return addresses on envelopes containing Cards must not bear the Issuer's identification, but only a special post office box serviced by the Issuer's authorized personnel.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Whenever possible, the envelopes containing the Cards should be combined with as much regular mail as possible to disguise the contents of the envelopes and distribute the risk of bulk losses. Issuers should reschedule the delivery of outgoing Cards to their carrier whenever the originally scheduled delivery would subject the Cards to storage in unsecured areas.

The Issuer must maintain a record of the method, date, and time of delivery or collection, and the postal mailing location for each Card. In cases involving losses in the mail, the Issuer should report to the postal authorities within twenty-four (24) hours of the determination that a loss has occurred. The Issuer must also report the loss to AEGNS at gnsfraud@aexp.com.

8.4.3 Return of Undeliverable Cards

Mail containing Cards that could not be delivered and are returned by the post office or other delivery service must be returned to a secured location and placed into dual custody by the entity responsible for receiving the returned Cards. Issuers and Card Personalization Vendors must implement controls to ensure complete accountability of returned Cards including their storage and destruction.

8.4.4 Card Activation

Card activation is a process whereby the Issuer or its agent causes a block against Card usage to be placed on the Issuer's Authorization system before the Card is delivered to the Cardmember. Upon receipt of the Card, a notice on the Card advises the Cardmember to contact their Issuer to activate their Card. Upon authenticating the identity of the Cardmember, the Issuer will remove the block, thereby allowing usage of the Card. AEGNS strongly recommends that Issuers use this process for all Cards. The Card Activation Process is mandatory for Prepaid Cards.

8.5 Participant Security Management

8.5.1 Security Office

Participants must have an infrastructure designed to ensure the compliance with Network rules and guidelines for Card security and fraud reduction. Card security for Participants should include, but not be limited to, the following functions:

1. Preventing, detecting, analyzing, and reviewing all fraudulent uses of Cards,
2. Planning and supervising the physical protection of the Participant's building,
3. Conducting employee background checks.

Additionally, Issuers must plan and supervise the manufacturing, personalization, and delivery of Cards.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.5.1.1 Security Contact Information

Each Participant must provide AEGNS with the current contact information of the executives who lead the Card security, fraud, and credit risk departments within the Participant's organization. Contact information must include the following:

- Full name and position/title
- Name of Participant/Bank
- Direct office and alternate (if available) telephone number(s)
- Business fax number(s), if available
- Emergency contact information for use outside of business hours
- Business email address, if available

Contact information must be sent to AEGNS Fraud and Security at gnsfraud@aexp.com. Any changes must be communicated within 30 days. Acceptable formats include spreadsheets, word processing documents, or plain text files.

8.5.2 Investigations

Participants must contact AEGNS Fraud and Security to report any suspected or confirmed security breach and must, to the best of their ability, provide requested investigative assistance to AEGNS, other Participants, and to the appropriate law enforcement agencies, in accordance with any laws applicable to AEGNS and any other Participant.

8.5.2.1 Investigative Responsibilities

Provided that such assistance is in compliance with applicable law, the assistance to be provided pursuant to Section 8.5.2, "Investigations," should include, but not necessarily be limited to:

1. Conducting interviews with S/Es, Cardmembers, suspects, witnesses, and law enforcement personnel.
2. Obtaining handwriting specimens, photographs, fingerprints, and any other similar physical evidence.
3. Recovering lost, stolen, counterfeit, or other fraudulently obtained or used Cards and other materials.
4. Arranging for arrests of persons when requested.
5. Conducting inspections of facilities of Card manufacturers.
6. Performing any other reasonable investigative assistance involving fraudulent Card activity directly with the other Participant(s).

8.5.2.2 Fraud Recoveries

Fraud recoveries involving two (2) or more Participants must be routed through AEGNS Fraud and Security to facilitate appropriate disbursement.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.5.3 AEGNS Fraud and Security Investigation Services

Participants may request guidance, advice or investigative assistance with fraud or security issues from American Express Global Security. American Express Global Security contacts are identified in the Participant Directory on Knowledge Base. When contacting American Express Global Security for assistance, Participants should also notify AEGNS Fraud and Security at gnsfraud@aexp.com.

Acquirers, Issuers, or AEGNS may call upon American Express Global Security personnel to conduct fraud investigations for their benefit. American Express Global Security, which is headquartered in New York, maintains security offices worldwide. These offices are primarily staffed with former law enforcement personnel from the region in which they are situated, who enjoy excellent relationships with their former and other law enforcement agencies. Their experience and expertise routinely contribute to the achievement of successful investigative results and the prevention and suppression of fraud losses. Such investigations conducted on behalf of Issuers, Acquirers or AEGNS will be performed with professionalism and sensitivity, and due regard for the confidential information of Participants.

American Express Global Security provides a variety of investigative and security-related services that are performed inside or outside of a Participant's core market. Investigators can provide risk analysis, financial crimes expertise, litigation support, investigator training, rapid response, and perform suspect employee investigations.

In addition, American Express Global Security may provide:

- Security system design and specifications
- Transportation expertise
- Facilities protection programs (access control, close circuit TV, employee and visitor badge access services, and software Encryption)
- Assistance with establishing employee background verification and crisis management programs
- Expert cyber investigative and forensic services and consulting

Participants that request investigative services from AEGNS and/or American Express Global Security may be charged fees. See Section 10.3.4, "Security and Fraud Investigation Service Fees," on page 405.

8.6 FraudNet

GNS FraudNet is a Web-based application that provides real-time fraud data and fraud management functions which assist Participants in mitigating fraud occurrences and losses. Some of the benefits offered by GNS FraudNet are as follows:

- Timely access to fraud data
- Enhanced Acquirer fraud actioning
- Better insight into fraud Chargeback opportunities
- Improved batch processing
- Overall reduction in fraud losses due to fraud-related information exchange between the AEGN and Participants

GNS FraudNet also provides an environment for future fraud-mitigating functionality.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.6.1 FraudNet Registration

To fully leverage FraudNet, all Participants must register for and utilize FraudNet. The minimum FraudNet registration requirements are detailed below:

- Issuers are required to have at least one (1) FraudNet user registered for Urgent Investigation Request (UIR) and the Participant Communication Platform (PCP).
- Acquirers are required to have at least one (1) FraudNet user registered for Urgent Investigation Request (UIR), S/E Actioning System (SEAS), and the Participant Communication Platform (PCP).

Participants must ensure that FraudNet registration is kept current. To request FraudNet access, please visit Knowledge Base homepage (www.amexglobalnetwork.com/knowledgebase). To delete any user(s) who should no longer have access to FraudNet, please email gns.user.services@aexp.com.

Participants who fail to meet the minimum FraudNet registration requirements will be subject to penalty fees as outlined in Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

AEGNS in its sole discretion reserves the right to refuse a UIR request and/or revoke a Participant's access to the UIR function in FraudNet.

8.6.2 FraudNet Training

For more information regarding navigation and use of FraudNet features, review the *GNS FraudNet User Guide* located on Knowledge Base (www.amexglobalnetwork.com/knowledgebase).

Participants may contact their AEGNS representative to coordinate FraudNet training.

8.7 Issuer Fraud Reporting

Issuers must report all of their Confirmed Fraud activity to AEGNS. Such fraud activity reporting must occur by the next Business Day after the verification of the fraud activity regardless of any past, or possibility for future, recoveries. See the *Codes Reference Guide* for the Fraud Type Codes used to classify fraud activity.

If after the initial fraud activity type is identified and reported, further investigation determines that the Transaction or occurrence is erroneous or of a different fraud activity type, the previously reported activity must be resubmitted using the revised fraud activity type code or record. The GNS Fraud Repository will accept revisions of previously reported fraud transactions under new codes.

If a Participant has not submitted any fraud reporting for a given month, the Participant must submit an empty data file by the third Business Day of the following month to indicate that no fraud has occurred.

To avoid Fraud Reporting non-compliance penalty fees, Issuers are advised to:

1. Validate the Fraud Repository Response (9334) message to determine that all Fraud Repository Files (9324) submitted to AEGNS have been successfully processed.
2. Reconcile Fraud Reports (Issuer Gross Fraud Update or Issuer Fraud Summary) to ensure that the fraud reported is being accepted by the AEGN. All rejected records must be corrected and resubmitted within the current reporting month.
3. Submit a Fraud Repository File (9324) with an empty data set by the third Business Day of the following month.

The Fraud Non-Compliance Fee Schedule A will be used to determine the fees associated with non-compliance. See Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.7.1 Issuer Fraud Data Entry

The Fraud Repository will be updated with information from Issuers to allow fraud to be monitored within the AEGN. Issuers will have access to update the system via a batch update facility. Issuers will be responsible for entering all Transactions, including On-Us Transactions, into the system when there is Confirmed Fraud. The Issuers will categorize the fraud into types using the fraud type codes identified. Each fraudulent Transaction will be entered into the Fraud Repository with a fraud type and other required data. Issuers may be requested to complete reconciliation against the Fraud Repository files to validate accuracy of the data provided. Issuers are required to use best efforts to ensure accuracy and are responsible for any consequential action or loss as a result of any errors.

8.8 AEGNS Fraud Reports

Fraud data reported by Issuers and S/E data reported by Acquirers is combined to produce fraud reports that are available to both Issuers and Acquirers by the 10th of each month on GNS FraudNet. Refer to the *Network Specifications - Instructions* manual for details regarding the fraud reports. For report access information, please see the *GNS FraudNet User Guide.*

8.9 AEGNS Acquirer and S/E Risk Management

AEGNS reviews Acquirers and S/Es by monitoring reported fraud data, S/E data, Authorizations and Presentments for risk patterns. Acquirers will be notified of S/Es identified as potential High Risk S/Es via the S/E Actioning System (SEAS) on GNS FraudNet. When AEGNS notifies an Acquirer of a potential High Risk S/E, such notification will include one (1) or more required actions to address the fraud risk concerns. These actions may include, but are not limited to, the following:

1. Cancellation of the S/E
2. S/E notification of a probationary period during which time the S/E is subject to Fraud Full Recourse Chargebacks
3. Fraud prevention training onsite with the S/E
4. Installation of a POS device that reads and transmits entire magnetic stripe data
5. Perform site visitation of the S/E
6. Reduction of the S/E floor limit to zero (0)
7. Permanent addition of the S/E to the High Risk S/E list
8. Mandate the S/E capture and send the PCSC for all Card Not Present Transactions

8.9.1 High Risk S/E List

An Acquirer is required to place an S/E that qualifies for any of the High Risk criteria detailed in Section 8.9.2, "High Risk S/E Criteria," on page 385 on the AEGNS High Risk S/E list unless prohibited under the Participant's local law. The High Risk S/E list is available to all Participants on FraudNet.

If AEGNS determines that an S/E meets the conditions for one (1) or more of the High Risk S/E Criteria, AEGNS will notify the Acquirer with a High Risk listing recommendation via the S/E Actioning System (SEAS) on GNS FraudNet. AEGNS reserves the right to immediately list on the High Risk S/E list any S/E that meets any of the High Risk S/E list criteria detailed in Section 8.9.2, "High Risk S/E Criteria," on page 385. AEGNS will notify an Acquirer when an S/E has been listed.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

If an Acquirer determines an S/E meets the conditions for one (1) or more of the High Risk S/E Criteria, the Acquirer must add the S/E to the High Risk S/E list. Acquirers may add an S/E to, or heighten the status of, an S/E on the High Risk S/E list, through GNS FraudNet or by submitting the S/E Demographics Detail Data (9640) message to the GNS Fraud Repository (refer to the *Network Specifications - Financial/Non-Financial* manual). Acquirers must be registered to utilize the High Risk S/E update functionality in GNS FraudNet. Refer to the *GNS FraudNet User Guide* for details on High Risk S/E procedures.

If an Issuer suspects that an S/E meets one (1) or more of the High Risk S/E Criteria, and the S/E is not on the High Risk S/E list, the Issuer may request the addition of the S/E to the High Risk S/E list. When an Issuer chooses to make a High Risk S/E listing request, it must use the High Risk S/E list request functionality on GNS FraudNet. A detailed explanation and sufficient Documentation to support the High Risk S/E request must be provided (i.e., dispute/Chargeback transaction support, Cardmember declarations, law enforcement/security reports). AEGNS will determine, based on the evidence provided by the Issuer and existing S/E Fraud data, which Issuer recommended High Risk S/E listing requests will be communicated to Acquirers via an S/E Actioning System (SEAS) recommendation on GNS FraudNet. If the evidence provided by the Issuer is found to be insufficient and/or the existing S/E Fraud data does not support a High Risk listing or S/E Actioning System (SEAS) recommendation, AEGNS will reject the High Risk S/E listing Request from the Issuer.

While the S/E is on the High Risk S/E list, the Acquirer accepts full Chargeback liability for all fraud incurred as described under Chargeback Reason "ISO 4763 - Fraud Full Recourse" on page 348.

Refer to the *Codes Reference Guide* for a complete list of valid Card Acceptor High Risk Indicators.

8.9.1.1 Removing an S/E from the High Risk S/E List

AEGNS will periodically review S/Es on the High Risk S/E list. When an S/E no longer meets the criteria for which it was added to the High Risk S/E list, the S/E will be removed from the list.

An S/E that is considered high risk as a result of Fraud to Gross (FTG) performance will be removed from the High Risk S/E list if either of the following occurs for that S/E:

- Below 0.9% FTG performance per month for three (3) consecutive months, or
- Below $25,000 gross fraud per month for three (3) consecutive months.

To ensure AEGNS is using the most current information to assess the high risk status of an S/E, the Acquirer should submit any modified S/E characteristics to the GNS Fraud Repository via the S/E Demographics Detail Data (9640) message. AEGNS will reassess the S/E's high risk status based on the updated information provided by the Acquirer and the criteria described in Section 8.9.2, "High Risk S/E Criteria," on page 385 to determine if the S/E should be removed from the High Risk S/E list. Refer to the *Network Specifications - Financial/Non-Financial* manual for more information regarding the S/E Demographics Detail Data (9640) message.

If an Acquirer is not certified to submit the S/E Demographics Detail Data (9640) message, the Acquirer may make an appeal to the AEGNS Fraud and Security department for removal of the S/E from the High Risk S/E list. The appeal request must show sufficient support to justify why the S/E should be removed from the High Risk S/E list. In the event that the AEGNS Fraud and Security department finds that the S/E still qualifies for the High Risk S/E list, the request for removal will be denied. The S/E will remain on the High Risk S/E list for an additional three (3) month period. After the three (3) months have expired, the Acquirer may initiate another appeal.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.9.2 High Risk S/E Criteria

AEGNS considers an S/E a High Risk S/E when it meets at least one (1) of the following criteria (listed in hierarchical order, most severe to least severe):

1. An S/E has been cancelled for being a Fictitious and/or Collusive S/E. See Section 8.9.2.1, "Fictitious and/or Collusive S/E," on page 385.
2. An S/E has been cancelled for being an illegal business, or is in a prohibited industry. See Section 8.9.2.2, "Illegal or Prohibited Industry," on page 385.
3. An S/E's performance threshold falls into either a Low Tier or High Tier FTG calculation.
4. An S/E is identified as conducting business in a high risk industry, as described in Section 8.9.2.4, "High Risk S/E Industries," on page 386.
5. An S/E has been cancelled for derogatory reasons. See Section 8.9.2.5, "Cancelled S/Es (Derogatory)," on page 387.

8.9.2.1 Fictitious and/or Collusive S/E

Once an Acquirer identifies that an S/E is fictitious, it must immediately do the following:

- List that S/E on the High Risk S/E list with a risk indicator of "S" and
- Cancel the S/E.

If AEGNS identifies a Fictitious and/or Collusive S/E, AEGNS will place the S/E on the High Risk S/E list and notify the Acquirer when the S/E has been listed. The Acquirer must cancel the S/E account immediately upon notification from AEGNS.

An Acquirer that allows Transactions to process from a Fictitious and/or Collusive S/E, subsequent to placement on the High Risk S/E list, may be subject to penalty fees detailed in Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

8.9.2.2 Illegal or Prohibited Industry

Once an Acquirer identifies that an S/E is in an illegal or prohibited industry, it must immediately do the following:

- List that S/E on the High Risk S/E list with a risk indicator of "I" and
- Cancel the S/E.

See Section 2.9.4.1, "Prohibited Industries," on page 94.

If AEGNS identifies an illegal or prohibited industry, AEGNS will place the S/E on the High Risk S/E list and notify the Acquirer when the S/E has been listed. The Acquirer must cancel the S/E account immediately upon notification from AEGNS.

An Acquirer that allows Transactions to process from an Illegal or Prohibited Industry S/E, subsequent to placement on the High Risk S/E list, may be subject to non-compliance fees detailed in Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.9.2.3 Fraud to Gross Sales Volume Ratio

An S/E's performance threshold falls into either a Low Tier or High Tier FTG calculation. This FTG calculation excludes Fraudulent Applications and SafeKey Transaction Attempts.

The following table describes the two (2) Tiers within FTG Performance criteria:

Table 8-1. Fraud to Gross Performance Criteria

Tier	Performance	Actions Taken
Low Tier	• S/E fraud level equals or exceeds 0.9% FTG **and** • S/E has a minimum fraud total amount of $25,000 (USD) gross fraud in a one (1) month period	• Acquirer will be notified that S/E has exceeded the thresholds of both 0.9% FTG and $25,000 (USD) gross fraud. • S/E has a three (3) month timeframe to remain below the FTG Low Tier criteria. • If S/E does not remain below the FTG criteria for three (3) consecutive months, they will be subject to Fraud Full Recourse (FFR) Chargebacks and will no longer qualify for SafeKey FLS. Refer to "American Express SafeKey Fraud Liability Shift" on page 361 for more information. • S/E will have a risk indicator of "F."
High Tier	• S/E fraud level equals or exceeds 1.8% FTG **and** • S/E has a minimum fraud total amount of $50,000 (USD) gross fraud in a one (1) month period	• Acquirer will be notified that S/E has exceeded the thresholds of both 1.8% FTG and $50,000 (USD) gross fraud. • S/E will be subject to Fraud Full Recourse (FFR) Chargebacks and will no longer qualify for SafeKey FLS. Refer to "American Express SafeKey Fraud Liability Shift" on page 361 for more information. • S/E will have a risk indicator of "F."

S/Es must remain on the High Risk S/E list until their FTG ratio falls below the requirements. Refer to "Removing an S/E from the High Risk S/E List" on page 384 for more information.

Other performance criteria may be evaluated prior to the removal of the S/E. In the event the AEGNS Fraud and Security department finds the S/E still a high risk, the request for removal will be denied for an additional three (3) months, after which time another appeal may be made, starting the process over again.

8.9.2.4 High Risk S/E Industries

S/Es conducting business in high risk industries must be added to the High Risk S/E list with a risk indicator of "T" upon new S/E signing. If the Acquirer, subsequent to signing an S/E, identifies, or is notified by AEGNS that the S/E is conducting business in a high risk industry, the Acquirer must add the S/E to the High Risk S/E list within thirty (30) days of such identification or notification.

S/Es conducting Gambling and Lottery Transactions (identified with MCCs 7800, 7801, 7802, or 7995) must be added to the High Risk S/E list with a risk indicator of "T."

Active S/Es with a risk indicator of "T" must remain on the High Risk S/E list until the S/E is either cancelled by the Acquirer or no longer conducts business in a high risk industry.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.9.2.5 Cancelled S/Es (Derogatory)

An Acquirer may choose to cancel their agreement with an S/E for many reasons (see the Cancellation Status Codes section in the *Codes Reference Guide*). An S/E whose Card acceptance agreement is cancelled by the Acquirer for derogatory reasons, as listed in Table 8-1, "Derogatory Status Reason Codes (Cancellation)," on page 387 must be added to the High Risk S/E list with the associated risk indicator of "I" (prohibited or illegal industry S/E), "S" (fictitious), or "X" (cancelled for derogatory reasons—other than "I" or "S"). Each cancelled S/E must remain on the High Risk S/E list for a period of six (6) months.

Derogatory reasons may include high levels of fraud, a fictitious and/or Collusive S/E, or any of the risky behaviors identified as follows:

- High Chargeback Volumes.
- Unsubstantiated S/E Credit Volumes.
- Instances of Multiple ROC disputes. Refer to "ISO 4534 - Multiple ROCs" on page 328.
- High ratio of mismatch between the PCSC provided by the S/E and the PCSC printed on the Card.
- Potential Point of Compromise (POC).
- Keyed transaction volumes.
- Volume of Transactions below floor limit.

An Acquirer that allows Transactions to process from an S/E that should have been cancelled for derogatory reasons, as listed in Table 8-1 subsequent to placement on the High Risk S/E list, may be subject to penalty fees detailed in Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

Table 8-1. Derogatory Status Reason Codes (Cancellation)

Cancellation Code Description	Card Acceptor High Risk Indicator
01 Cancelled - Out of Business	X
02 Cancelled - Bankruptcy	X
07 Cancelled - Merchant In Receivership	X
15 Cancelled - Fraud/Credit Risk	X
20 Cancelled - Factoring	X
25 Cancelled - Fraud Merchant	S
26 Cancelled - High Cardmember Fraud	X
27 Cancelled - Illegal Business	I
30 Cancelled - In Liquidation	X
33 Cancelled - Sold - No Resign	X

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.9.3 S/E Risk Management

Acquirers are required to implement a procedure to monitor or cause to be monitored S/E Transactions for activity indicative of fraud. This procedure should include thresholds set by the Acquirer that accommodate the differences among individual S/Es. Events such as legitimate seasonal fluctuations and system outages should also be considered in the monitoring process. The following activities must be monitored:

- Increased percentage of keyed versus swiped Transactions
- Increased percentage of Transactions below the S/E Floor Limit
- Out of pattern Authorizations and Presentments
- Out of pattern daily volume
- Excessive Retrieval Request Notifications or Chargebacks
- Change in Presentment method
- Change in sales method
- Credit ROCs without corresponding Charges
- Other appropriate fraud detection mechanisms

If an Acquirer observes S/E(s) engaging in any of the above activities, and the volume of those activities exceeds that Acquirer's thresholds, then that Acquirer must immediately do **all** of the following:

- Take appropriate action to limit financial losses
- Identify Participants that could incur financial losses by the above activities
- Alert impacted Participants with an Urgent Investigation Request (UIR) via FraudNet

The Acquirer may also choose to notify the other impacted Participants in order to expedite resolution of the incident. The *Participant Directory* on Knowledge Base contains Participant contact information.

8.9.3.1 Acquirer UIR

Participants can communicate urgent fraud-related transaction information to each other via the GNS FraudNet UIR system. An Issuer (Filing Network Participant - FNP) may contact the Acquirer (Receiving Network Participant - RNP), via GNS FraudNet with a UIR to either:

- Request verification of the legitimacy of a Transaction and/or an S/E, or
- Notify an Acquirer that the Issuer observed high risk behavior by that Issuer's Cardmember when transacting at the Acquirer's S/E. Refer to Section 8.10.3, "Cardmember Risk Management," on page 392 for additional information.

Likewise, an Acquirer (FNP) may contact the Issuer (RNP), via GNS FraudNet with a UIR to either:

- Request validation of the Charge with the Cardmember, or
- Notify an Issuer that the Acquirer observed high risk behavior by that Acquirer's S/E when transacting with the Issuer's Cardmember(s). Refer to Section 8.9.3, "S/E Risk Management," on page 388 for additional information.

In cases where an Issuer validates a Charge in response to a UIR, an S/E must continue to follow all Card acceptance procedures in connection with the Charge. Refer to Section 4.2, "S/E Card Acceptance Procedures," on page 214 for complete acceptance procedures.

When an Acquirer is the RNP on a UIR, it must take appropriate action based on the content of the UIR and respond to the Issuer (FNP) within seventy-two (72) hours of the receipt of the UIR. Response via the UIR system is always required.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

An Acquirer who fails to respond to any UIR initiated by an Issuer within a seventy-two (72) hour period, will be considered non-compliant with the AEGN UIR process. An Acquirer must check the FraudNet UIR queue on a daily basis to ensure a timely response. For information on the Online UIR system, refer to the *GNS FraudNet User Guide.*

UIR compliance will be monitored monthly by AEGNS. When an Acquirer's UIR compliance rate falls below 95% in a single month, regardless of whether UIR-related transactions prove fraudulent, the Acquirer will be subject to penalty fees as detailed in Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

8.9.3.2 Acquirer Participant Communication Platform (PCP)

Participants will receive notification of major fraud events from AEGNS via the FraudNet Participant Communication Platform. Due to the urgency of these communications, Participants are required to read all items within seventy-two (72) hours of the communication being sent.

PCP compliance will be monitored monthly by AEGNS. For information on the FraudNet PCP system refer to the *GNS FraudNet User Guide.*

8.9.4 S/E Actioning System (SEAS)

When AEGNS identifies an S/E that meets any of the criteria outlined in Section 8.9.2, "High Risk S/E Criteria," on page 385, or meets any other criteria deemed by AEGNS to indicate high risk behavior on the part of the S/E, AEGNS will send a recommendation to the Acquirer via GNS FraudNet's S/E Actioning System (SEAS recommendation). There are two (2) types of SEAS recommendations:

- Add the S/E to the High Risk S/E list (High Risk Listing recommendation).
- Take one (1) or more actions described in the *GNS FraudNet User Guide* Chapter "Service Establishment Actioning System (SEAS) Operational Procedures" (Manual Review recommendations).

An Acquirer must take appropriate action in accordance with the SEAS recommendation within thirty (30) calendar days of receiving it. For additional information regarding SEAS, refer to the *GNS FraudNet User Guide* Chapter "Service Establishment Actioning System (SEAS) Operational Procedures."

If an Acquirer takes an action other than what is recommended in the SEAS recommendation, the Acquirer must provide sufficient supporting evidence to AEGNS to justify its actions by using one (1) of the following two (2) methods:

- The Acquirer must submit an updated S/E Demographics Detail Data (9640) message.
- The Acquirer must contact the AEGNS Fraud and Security department through the Knowledge Base Support Center.

8.9.4.1 High Risk Listing Recommendations

AEGNS will make a High Risk Listing Recommendation when an evaluation of the S/E indicates that it meets the High Risk S/E listing criteria.

If the SEAS recommendation includes a High Risk Listing Recommendation and the Acquirer:

- Fails to respond within the required thirty (30) calendar day timeframe, or
- Fails to add the S/E to the High Risk S/E list in accordance with the SEAS recommendations and does not provide sufficient support to AEGNS to justify not following the SEAS recommendation,

then AEGNS reserves the right to immediately add the S/E to the High Risk S/E list without further notification to the Acquirer.

When an S/E is added to the High Risk S/E list by AEGNS due to a SEAS recommendation, the date reflected on the High Risk S/E list for adding the S/E may be populated with the creation date of the SEAS recommendation.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.9.4.2 Manual Review Recommendations

Manual Review recommendations are made by AEGNS when an S/E:

1. Exceeds 2% FTG,
2. Exceeds $30,000 (USD) in fraud, or
3. Continues to submit Transactions after cancellation

In the case of (1) and (2) above, the Manual Review recommendation will include a requirement for the Acquirer to implement PCSC capture for their Card Not Present Merchants and provide an adequate fraud reduction plan to AEGNS.

In addition, the Manual Review recommendation may include other recommended actions as described in the *GNS FraudNet User Guide* Chapter "Service Establishment Actioning System (SEAS) Operational Procedures."

If the SEAS recommendation includes a Manual Review recommendation and the Acquirer:

1. Fails to respond within the required thirty (30) calendar day timeframe or
2. Fails to follow the Manual Review recommendation and does not provide sufficient support to AEGNS to justify not following the SEAS recommendation,

then AEGNS may assess a non-compliance fee on the Acquirer. Refer to Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403 for more information.

8.9.4.3 SEAS Compliance Monitoring

AEGNS will compile the percentage of instances each month in which an Acquirer:

- Responded late to a SEAS recommendation,
- Took an action other than the SEAS recommendation without AEGNS' approval, and/or
- Failed to respond to a SEAS recommendation.

This percentage will be the "Overall SEAS Compliance Rate" of the Acquirer. An Acquirer who falls below a 98% "Overall SEAS Compliance Rate" each month will be subject to non-compliance fees as described in Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

8.9.5 AEGNS Investigation of S/Es

AEGNS may investigate any S/E at any time. Acquirers are obligated to fully cooperate with any such investigation. AEGNS' decisions shall be final. Investigations may include, but not be limited to an examination of the S/E's or Acquirer's:

- Solicitation method/region
- Application and supporting Documentation
- Agreement terms and conditions
- POS devices and processing program
- Authorizations and Presentment data
- Monitoring reports

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.9.6 S/E Monitoring for Fraud Liability Shift Eligibility

AEGNS monitors fraud performance monthly for S/Es participating in select Fraud Liability Shift (FLS) policies. If the S/E's Fraud to Gross Sales Volume Ratio (FTG) exceeds the designated threshold for Transactions that qualify for the policy, the FLS may be suspended until the S/E becomes compliant with the fraud monitoring threshold associated with that policy.

Note: AEGNS reserves the right to immediately suspend an S/E's participation in any FLS policy due to FTG performance or other high risk behavior.

Acquirers will be notified via the S/E Actioning System (SEAS) on GNS FraudNet when one (1) or more of their S/Es exceeds the designated threshold. If the Acquirer disagrees with the FTG ratio provided by AEGNS, the Acquirer will be given thirty (30) days to provide sufficient support to AEGNS to justify the S/E's continued participation in the FLS. Supporting Documentation should be attached to the Acquirer's response to the original SEAS notification. Should sufficient support not be provided, the S/E's participation in an FLS will be suspended after the thirty (30) day period.

From the time an S/E's participation in an FLS is suspended, it will remain suspended until either the S/E's FTG performance or Total Fraud Volume (if applicable) remains below the threshold for three (3) consecutive months.

An S/E that is subject to repeated suspensions from one (1) or more FLS policies may be permanently excluded from participation in all FLS policies.

8.9.6.1 American Express SafeKey Fraud Liability Shift Qualification S/E Fraud Thresholds

S/Es may not qualify for SafeKey FLS when both of the following conditions exist:

- The S/E's monthly Fraud to Gross Sales Volume Ratio (FTG)[1] is greater than or equal to 0.9%, and
- The S/E's monthly total Fraud Value[1] is greater than or equal to $25,000 (USD).

Refer to Section 7.10.8.3, "American Express SafeKey Fraud Liability Shift," on page 361 for additional information.

8.10 AEGNS Issuer and Cardmember Risk Management

8.10.1 Card Security

An Issuer is responsible for the security of Cards and Cardmember Information as referenced in Section 8.2.1, "Certification Requirements for Card Production," on page 375 and Section 2.10.4, "Use of Cardmember Information," on page 113, respectively. Issuers shall cooperate with AEGNS, including implementing procedures and making all expenditures which are commercially reasonable, in order to promote fraud control for issued Cards. Issuers are liable for all fraud losses from counterfeit and application fraud on Cards that appear to be, and were accepted as, legitimate Cards, provided that all other Card acceptance procedures were followed by the S/E.

Acquirers may be liable for counterfeit fraud losses if the S/E has not been upgraded with a Chip-Enabled Device. See Section 7.10.8.1, "AEIPS Fraud Liability Shift (FLS)," on page 359 for additional information.

1. Excludes Transactions classified as SafeKey Attempted (as indicated by the Electronic Commerce Indicator within the POS First Presentment (1240).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.10.2 5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program

5CSC and iCSC are fraud tools supported by AEGNS and are primary components of Card security policy. Use of 5CSC on the magnetic stripe, or iCSC on the magnetic stripe equivalent on the Card's chip, allows Issuers to more effectively evaluate fraud risk when making an approve/decline decision on an Authorization Request. 5CSC and iCSC program requirements are detailed below:

- Issuers are required to encode 5CSC on the magnetic stripe for every Card in their portfolio. If issuers opt to utilize iCSC, they must encode the iCSC on the magnetic stripe equivalent of AEIPS Chip Cards.

  Note: The 5CSC is not encoded within the magnetic stripe equivalent data on an Expresspay Card that is used during an Expresspay Transaction in magnetic stripe mode.

- Issuers are required to validate 5CSC (or iCSC, if used) during the Authorization process. Validation of 5CSC and iCSC requires that when an Issuer receives the 5CSC or iCSC value in the magnetic stripe data field of the POS Authorization Request (1100) message, the Issuer must validate that the 5CSC or iCSC value received matches the 5CSC or iCSC value re-created by the Issuer using an algorithm of Cardmember Account information.
- Issuers are required to factor the result of 5CSC or iCSC validation into their risk criteria for decisioning the Authorization Request.
- Issuers using iCSC for their contact chip must also use iCSC for their Contactless chip.

Note: Acquirers are required to transmit magnetic stripe data for all Transactions that are magnetic stripe-read and magnetic stripe equivalent chip data for all Transactions that are chip-read.

5CSC and iCSC validation are supported by the Network when utilizing Host Stand-In. 5CSC and iCSC validation is not, however, supported by the Network when utilizing Remote Stand-In.

Issuers that do not comply with 5CSC and iCSC encoding requirements are subject to non-compliance fees. See Section 10.3.3, "5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program Non-Compliance Fees," on page 405 for more information.

8.10.3 Cardmember Risk Management

Issuers must implement a procedure to monitor or cause to be monitored all Cardmember Transactions for indications of fraud or Cardmember risky behavior. This procedure
should include thresholds set by the Issuer that accommodate the differences among individual Cardmembers.

Transaction monitoring should include:

- Percentage of Authorizations versus Presentments
- Out of pattern volume
- Excessive disputes
- Excessive loss of Card or claims of fraud
- Credit ROCs without corresponding Charges
- Anti-Money Laundering monitoring and reporting as required according to local laws and regulations, and according to AEGNS requirements
- Other appropriate fraud detection mechanisms

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Additional monitoring for Prepaid Cards should include:

- Out of pattern Load/Reload/spend
- Out of pattern refund requests
- Reload payment rejects
- Overspend
- Order and Reload accept/decline rates
- Fraud/debit balance exposure
- Loading done by third parties
- Loading of Prepaid Cards just under local regulatory reporting thresholds conducted multiple times on the same Card
- Third party funding followed by a transfer of funds to an unrelated account
- Loading followed by ATM withdrawals
- Use of Prepaid Cards to make multiple withdrawals from different ATMs
- Use of Prepaid Cards exclusively for cash withdrawals

Issuers should also monitor non-reloadable Prepaid Card Transactions for unusual activity which may indicate illicit use of such Cards. Monitoring should include:

- High volume or out of pattern increase in the volume of Card purchases from a distributor
- Unusually frequent exchanges for cash
- High volumes of gift card Transactions occurring at a single Merchant
- Patterned or even amount Transactions

If an Issuer observes Cardmember(s) engaging in any of the above activities, and the volume of those activities exceeds that Issuer's thresholds, then that Issuer must immediately do **all** the following:

- Take appropriate action to limit financial losses
- Identify Participants that could incur financial losses by the above activities
- Alert impacted Participants with an Urgent Investigation Request (UIR) via FraudNet

The Issuer may also choose to notify the other impacted Participants in order to expedite resolution of the incident. The *Participant Directory* on Knowledge Base contains Participant contact information.

8.10.3.1 Dynamic Fraud Management

To maintain a high level of security and prevent fraud on the Network, AEGNS reserves the right to assess the fraud risk and decision Authorization Requests for all Transactions. If AEGNS declines an Authorization Request (1100) message, the Issuer will receive a POS Authorization Advice (1120) message indicating the decline.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.10.3.1.1 Issuer Override Request and Fraud Liability

Issuer Override Request (IOR) allows an Issuer to submit a request to suspend Dynamic Fraud Management decline Authorization Responses for specific Card Account Numbers during a period defined by the Issuer. This allows the Issuer to decision all Transactions, including Transactions that would have been declined by AEGNS. The IOR feature is available to Issuers through FraudNet. An IOR can be created before or after a Transaction has been declined by AEGNS. Issuers are advised that an IOR will apply to all Eligible Transactions conducted on the relevant Card Account Number for the duration of the IOR. For additional information and how to create IORs, refer to the *GNS FraudNet User Guide*.

Issuers may not submit Chargebacks under the following Fraud Chargeback ISO codes for all Eligible Transactions with an active IOR status code in FraudNet:

- 4527 Missing Imprint
- 4534 Multiple ROCs
- 4540 Card Not Present
- 4798 Fraud Liability Shift - Counterfeit
- 4799 Fraud Liability Shift - Lost/Stolen/Non-Received

8.10.3.1.2 Dynamic Fraud Management Network Services

AEGNS requires Issuers to have robust fraud prevention controls to manage fraud risk. To enhance Issuers' fraud controls, AEGNS provides Dynamic Fraud Management Network Services (DFMNS), a set of fraud Authorization tools that provide real-time fraud assessment and management. DFMNS assesses the risk of each Eligible Transaction on the Network and provides Issuers with a Fraud Probability Score and Recommendation Code.

Some of the benefits offered by DFMNS include:

- Real-time evaluation of potential fraud risk on individual Eligible Transactions, taking into account available Network information
- Easy access to Eligible Transaction Authorization decision results
- Real-time alerts for rapid Cardmember verification in conjunction with other controls the Issuer may have
- Enhanced fraud investigation and Issuer fraud risk decisions

8.10.3.1.3 Dynamic Fraud Management Network Services Use

Each Issuer will receive DFMNS and can use this service in two (2) ways:

- Alerts through WINTER (WINdow To Early Referrals), a FraudNet application available to all Issuers, which provides the results of the Authorization decision, along with the Fraud Probability Score and a Recommendation Code.
- Issuers may elect to certify to receive both the Fraud Probability Score and the Recommendation Code, real-time in their respective Authorization Request (1100), POS Authorization Advice (1120), Payment Token Provisioning Request (1100), Payment Token Post Provisioning Notification (1120), and ATM Financial Transaction Request (1200) messages. By receiving the information in this manner, Issuers can incorporate the DFMNS into their own Authorization decisioning processes.

Fees for DFMNS will be specified in the Participant Agreement. Contact your AEGNS representative for more information.

Additional information about DFMNS terms and conditions can be found in "Exhibit 15. Dynamic Fraud Management Network Services Terms and Conditions" on page 482.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.10.3.2 Issuer UIR

Participants can communicate urgent fraud-related transaction information to each other via the GNS FraudNet UIR system. An Acquirer (FNP) may contact the Issuer (RNP), via GNS FraudNet with a UIR to either:

- Request validation of the Charge with the Cardmember, or
- Notify an Issuer that the Acquirer observed high risk behavior by that Acquirer's S/E when transacting with the Issuer's Cardmember(s). Refer to Section 8.9.3, "S/E Risk Management," on page 388 for additional information.

In cases where an Issuer validates a Charge in response to a UIR, an S/E must continue to follow all Card acceptance procedures in connection with the Charge. Refer to Section 4.2, "S/E Card Acceptance Procedures," on page 214 for complete acceptance procedures.

Likewise, an Issuer (FNP) may contact the Acquirer (RNP), via GNS FraudNet with a UIR to either:

- Request verification of the legitimacy of a Transaction and/or an S/E, or
- Notify an Acquirer that the Issuer observed high risk behavior by that Issuer's Cardmember when transacting at the Acquirer's S/E. Refer to Section 8.10.3, "Cardmember Risk Management," on page 392 for additional information

When an Issuer is the RNP on a UIR, it must take appropriate action based on the content of the UIR and respond to the Acquirer (FNP) within seventy-two (72) hours of the receipt of the UIR. Response via the UIR system is always required.

An Issuer who fails to respond to a UIR initiated by an Acquirer within a seventy-two (72) hour period will be considered non-compliant with the AEGN UIR process. For information on the Online UIR system, refer to the *GNS FraudNet User Guide.*

UIR compliance will be monitored monthly by AEGNS. When an Issuer's UIR compliance rate falls below 95% in a single month, regardless of whether UIR-related transactions prove fraudulent, the Issuer will be subject to non-compliance fees as detailed in Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

8.10.3.3 Recurrent Cardmember Fraud

An Issuer must hold the Cardmember responsible for safeguarding the Card, Mobile Device, and Card Account number by requiring the Cardmember to do the following:

- Sign the Card immediately upon receipt.
- Make certain the Card is returned to the Cardmember after each purchase.
- Do not loan or give the Card or Mobile Device to anyone.
- Notify the Issuer immediately if the Card or Mobile Device is lost or stolen.
- Secure or destroy documents that display the Card number; such as charge receipts, carbons, travel itineraries, and statements.
- Do not give the Card number to anyone over the telephone unless the Cardmember initiated the call.

An Issuer must monitor Accounts for recurrent fraud. When Cardmembers have had three (3) or more lost, stolen, or returned Cards in a three (3) year period, the Issuer must review for cancellation. If cancellation is possible for any other reason, the Card should be cancelled and such reason should be used. The Cardmember must be notified of cancellation and the Account number listed on the Exception File.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.10.3.4 Issuer Participant Communication Platform (PCP)

Participants will receive notification of major fraud events from AEGNS via the FraudNet Participant Communication Platform. Due to the urgency of these communications, Participants are required to read all items within seventy-two (72) hours of the communication being sent.

PCP compliance will be monitored monthly by AEGNS. For information on the FraudNet PCP system, refer to the *GNS FraudNet User Guide*.

8.10.4 Issuer Fraud Rate

Issuers are required to manage their portfolio so as to minimize fraud on their Cards. Fraud rate monitoring is intended to improve overall performance, strengthen the value proposition of AEGNS as a premium Network and improve the end-user experience on the Network.

AEGNS will monitor each Issuer's Gross Fraud Rate on a quarterly basis and compare the Issuer's gross fraud rate to the Regional Gross Fraud Rate. Regions are defined as:

- United States/Canada
- Latin American/Caribbean
- Asia Pacific
- Europe/Middle East/Africa

AEGNS will use the following methodology to calculate the Issuer's Gross Fraud Rate and the Regional Gross Fraud Rate:

1. Determine each Issuer's Gross Fraud Rate by dividing the Issuer's gross fraud in a particular quarter, by the Issuer's billed business in that quarter.
   Gross fraud Transactions and billed business include On-Us Transactions.
2. Determine the average Regional Gross Fraud Rate by dividing the region's gross fraud in a particular quarter by the total billed business in that quarter.
3. Calculate the difference between each Issuer's Gross Fraud Rate and the average Regional Gross Fraud Rate. If the Issuer's Gross Fraud Rate is higher than the Regional Gross Fraud Rate, AEGNS will determine whether the difference is outside the expected statistical norm for that quarter.
4. Issuers whose Gross Fraud Rate is higher than the expected statistical norm for two (2) consecutive calendar quarters will be considered out of compliance with this policy.

AEGNS will notify Issuers of their non-compliant status. Non-compliant Issuers must take appropriate steps to reduce their fraud rate, including providing an adequate fraud reduction plan to AEGNS. Issuers that do not comply may be subject to non-compliance fees. Refer to Section 10.3.1, "Fraud Non-Compliance Fee Schedule A," on page 403.

8.10.5 Fraud Risk Services

To improve the POS Authorization process and detection of fraudulent charges, AEGNS offers the following fraud mitigating tools to Network Participants:

- American Express SafeKey On-Behalf-Of Services
- AEIPS and Expresspay On-Behalf-Of Services

Refer to the Network Specifications manuals for more information. Participants interested in these tools should contact AEGNS through the Knowledge Base Support Center.

Note: Fees may be associated with using these fraud mitigation tools.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

8.10.5.1 SafeKey On-Behalf-Of Services

SafeKey On-Behalf-Of Services are an alternative to an Issuer's in-source developed or hosted SafeKey capability. The SafeKey On-Behalf-Of Services provide:

- SafeKey Authentication in the Internet environment
- SafeKey validation in the POS Authorization Response (1110) message

Refer to the American Express SafeKey Issuer Implementation Guides for additional information.

8.10.5.2 AEIPS and Expresspay On-Behalf-Of Services

American Express Cryptogram Validation Service validates the cryptogram for both AEIPS and Expresspay product types (including magstripe Contactless).

The Network will validate AEIPS and Expresspay (including magstripe Contactless) cryptograms on behalf of an Issuer and send an indicator to the Issuer with the validation results.

In addition, for Issuers unable to process EMV data, AEGNS offers an EMV to magstripe processing service. EMV data contained in the original Authorization Request sent by the Acquirer to AEGNS is not sent to the Issuer. AEGNS validates key EMV data and records the validation results. The Network will send the same message format and data fields as a magstripe Transaction, together with the EMV validation results and the EMV to magstripe processing indicator, to the certified Issuer in the POS Authorization Request (1100) message and the ATM Financial Transaction Request (1200) message. The POS First Presentment (1240) and the ATM First Presentment (1240) messages sent to the Issuer will contain the Chip Card Addendum (9240).

The cryptogram validation and the EMV to magstripe services are available during Stand-In for POS Transactions only.

Refer to the Network Specifications manuals for additional information.

8.11 Fraud Mitigation Practices

The following table lists both required and optional fraud mitigation practices for both Issuers and Acquirers that are used to help prevent the fraudulent use of Cards:

Table 8-2 Fraud Mitigation Practices

Fraud Practice/Tool	Description	Mandatory (M)/ Recommended (R)	Issuer-Focused	Acquirer-Focused	AEGNS-Supplied
Validation of Bit 53 (Card Security Code)	Issuers must validate the 3- or 4-digit PCSC (or OTP if used instead of the PCSC) for all Transactions on which the PCSC is present (see the "Business Policies and Rules" chapter beginning on page 11).	M (Issuers) R (Acquirers)	•	•	
5CSC Validation	Issuers must encode the 5CSC on the magnetic stripe and on the magnetic stripe equivalent of AEIPS Chip Cards and validate the 5CSC during Authorization (see "Security and Fraud" chapter beginning on page 375).	M	•		

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 8-2 Fraud Mitigation Practices (continued)

Fraud Practice/Tool	Description	Mandatory (M)/ Recommended (R)	Issuer-Focused	Acquirer-Focused	AEGNS-Supplied
iCSC Validation	Issuers that choose to use iCSC on their Chip Cards must encode the iCSC instead of the 5CSC on the magnetic stripe equivalent of AEIPS Chip Cards and validate the iCSC during Authorization of Chip Cards (see "Security and Fraud" chapter beginning on page 375)	M	•		
Dynamic Card Security Code (DCSC)	In instances where Transactions require DCSC in the POS Authorization Request (1100) Message, the AEGN will provide the DCSC value. When received from the AEGN, S/Es must submit the DCSC value in the PCSC field of the POS Authorization Request (1100) Message. The AEGN validates the DCSC value on behalf of the Issuer.	M (Acquirers, transmission of DCSC in applicable Transactions)		•	•
Automated Address Verification (AAV)	U.S. and Canadian Issuers must match a Cardmember's address information against the address provided on the Authorization Request (see Section 5.10.1, "Address Verification," on page 261). Acquirers and S/Es in American Express SafeKey markets must ensure this practice is enabled if available for that market.	M (U.S./Canadian Issuers and certain Acquirers) R (All other Acquirers and Issuers)	•	•	
Cardmember Identification Standards	In order to help prevent Account takeovers, Issuers should always verify their Cardmember's identity over the telephone or on the Internet by asking questions only the Cardmember can answer.	R	•		
Fraud Authorization Modeling	The combination of various pieces of information to evaluate the fraud risk associated with each Transaction during the Authorization process.	R	•		
Fraud Authorization Rules	Rules that are employed during the Authorization process to assist the Issuer in making the Authorization decision.	R	•		

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 8-2 Fraud Mitigation Practices (continued)

Fraud Practice/Tool	Description	Mandatory (M)/ Recommended (R)	Issuer-Focused	Acquirer-Focused	AEGNS-Supplied
Negative File	Non-issued and closed Account numbers should be checked during the Authorization process.	R	•		
Expiration Date Validation	Acquirers must provide an Expiration Date for all keyed Transactions (excluding recurring billing Transactions) and Issuers should validate the Expiration Date during the Authorization process. This helps prevent losses associated with mass-generation of fraudulent Account numbers.	M (Acquirers) R (Issuers)	•	•	
Capturing the PCSC at the POS	S/Es should capture the 3CSC or 4CSC at the Point of Sale to potentially reduce counterfeit Card fraud. Acquirers and S/Es in American Express SafeKey markets must ensure this practice is enabled if available for that market.	M (Acquirers in SafeKey markets) R (all other Acquirers)		•	
S/E Identification Standards	Acquirers should employ identification standards for S/Es who contact Acquirers by telephone or over the Internet, especially for critical Account changes (e.g., Settlement banking information).	R		•	
Merchant Risk Assessments	Acquirers must identify High Risk S/E behavior and take appropriate mitigating action. See Section 8.9, "AEGNS Acquirer and S/E Risk Management," on page 383.	M		•	
Dynamic Fraud Management Network Services (DFMNS)	DFMNS are a set of fraud Authorization tools that provide real-time fraud assessment and management for Eligible Transactions to enhance Participants' fraud controls.	R	•		•

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

9 AEGNS Service Performance Program

9.1 Internal Service Metrics

AEGNS, upon request, may require Participants to provide Internal Servicing Metrics. Examples of Internal Servicing Metrics may include, but are not limited to, customer surveys, onsite reviews of Participant servicing operations, and other standard customer servicing key performance indicators. Participants are required to track and monitor their own Internal Servicing Metrics in order to ensure delivery of high-quality service to customers that is consistent with the American Express Brand.

Participants that fail to provide Internal Servicing Metrics upon request within the established timeframes set forth by AEGNS will be subject to non-compliance fees. Refer to Section 10.7.1, "General Non-Compliance Fees," on page 411 for more information.

If a review of the Internal Servicing Metrics indicates the Participant's customer servicing is, at AEGNS' discretion, deficient or inconsistent with the American Express Brand, AEGNS may place the Participant on an Action Plan to address these deficiencies.

9.2 AEGNS Servicing Action Plan

AEGNS has the right to place a Participant on an Action Plan if a review of the Participant's Internal Service Metrics indicates the Participant's customer servicing, at AEGNS' discretion, is deficient or inconsistent with American Express standards.

AEGNS will provide written notification to Participants placed on an Action Plan, detailing their customer servicing deficiency. Participants are required to work with AEGNS to remediate any deficiencies specified in the Action Plan. Participants failing to adhere to the Action Plan may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10 Network Fees

10.1 Introduction

The purpose of this chapter is to inform Participants of certain fees AEGNS assesses. Additional fees are set out in each Participant Agreement. Fees are assessed in valid settlement currencies. The default settlement currency is U.S. Dollars. Acquirers and Issuers wishing to settle in a currency other than U.S. Dollars must contact their AEGNS representative. AEGNS reserves the right to change the amounts of the fees listed in this chapter and to impose additional fees for additional services made available by AEGNS. Contact your AEGNS representative for more information.

AEGNS shall calculate the amount of the fees payable by Participants in respect of the prior calendar month. Fees are detailed on the Participant's monthly settlement advisement and/or appear on the Fee Detail Section of the Daily Activity Report. Refer to Section 6.4.1, "Settlement Process," on page 272 for additional information.

Fees described in this chapter are identified by use of Valid Billing Unit Codes. Refer to the *Codes Reference Guide* for more information.

10.2 Disputes Fees

The following sections detail fees associated with dispute processing. Refer to the "Chargeback Policies" chapter beginning on page 280 for additional information.

10.2.1 Network Disputes Manager License Fees

Participants must be licensed by AEGNS to use Network Disputes Manager (NDM). A fee of $100 will be assessed monthly to each Participant. The following table outlines the fee schedule:

Table 10-1. Network Disputes Manager Fees

Fee Type	Fee Amount (USD)	Frequency
NDM License Fee	$100	Monthly

Note: Participants can use the NDM Disputes Online functionality at no extra cost. For more information on NDM Disputes Online refer to the *Network Disputes Manager - User Guide* on Knowledge Base.

Note: Participants that operate in multiple countries and/or have multiple Organization Identifiers will be assessed this fee once each month.

10.2.2 Pre-Arbitration and Pre-Compliance Processing Fees

A $10 (USD) administrative fee will be assessed to each Participant (Acquirer *and* Issuer) involved in the pre-Arbitration or pre-Compliance (refer to Section 7.11.1, "Good Faith Request," on page 364 for more information) transaction. These fees will be deducted from each Participant's Settlement. Refer to Section 7.3.2.10, "Pre-Arbitration," on page 285 and Section 7.3.2.12, "Pre-Compliance Requirement," on page 285 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.2.3 Arbitration Fees

All Arbitration Filings submitted to the AEGNS Arbitration Committee are subject to a filing fee and an Arbitration review fee. Penalty fees may be assessed against Participants if Network policy and/or submission requirements are not followed. Penalty fees may be assessed against either Participant regardless of whether the ruling is in their favor. Refer to Section 7.12.1, "Arbitration," on page 366 for more information.

Table 10-2. Arbitration Fees

All Fees are in U.S. Dollars	Filing Fee	Arbitration Review Fee	Penalty Fee (Per Violation)
Arbitration	$150	$250	$100

10.2.4 Good Faith Fees

All approved Good Faith requests submitted to AEGNS Good Faiths are subject to a $10 (USD) processing fee. This processing fee will be charged to both Participants for each Good Faith request processed. Participants that do not respond to a Good Faith Request are subject to a $100 (USD) non-response fee.

10.2.5 Compliance Fees

All Compliance Filings submitted to the AEGNS Arbitration Committee are subject to a filing fee and a compliance review fee. Penalty fees may be assessed to Participants if Network policy and/or submission requirements are not followed. Penalty fees may be assessed against either Participant regardless of whether the ruling is in their favor. Refer to Section 7.12.2, "Compliance," on page 369 for more information.

Table 10-3. Compliance Fees

All Fees are in U.S. Dollars	Filing Fee	Compliance Review Fee	Penalty Fee (Per Violation)
Compliance	$150	$250	$100

10.2.6 Dispute Transaction Fees

These fees are assessed to the sending Participant when a dispute message is processed through the Network as described in Section 7.3.2.7, "Dispute Transaction Fees," on page 284.

Table 10-4 Dispute Transaction Fees

Dispute Message (ISO Message Number)	Participant Responsible	Fee Amount Per Transaction (USD)
Retrieval Request (1642)	Issuer	$2.00
Fulfillment (1640)	Acquirer	$0.00
First Chargeback (1442)	Issuer	$3.00
Second Presentment (1240)	Acquirer	$3.00
Final Chargeback (1442)	Issuer	$0.00

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.2.7 Dispute Message Reject Fee

These fees are assessed to the sending Participant for any dispute Transaction message that is rejected as described in Section 7.3.2.8, "Dispute Message Reject Fee," on page 285.

Table 10-5 Dispute Message Reject Fee

Participant Responsible	Fee Amount per Transaction (USD)
Issuer	$5.00
Acquirer	$5.00

10.3 Fraud Fees

The following sections detail the fees associated with security and fraud.

10.3.1 Fraud Non-Compliance Fee Schedule A

Table 10-6, "Fraud Non-Compliance Fee Schedule A," on page 403 is a general fee table that is referenced for a variety of fraud policy, product registration and data reporting violations detailed in Section 10.3.2, "Violations Subject to Fraud Non-Compliance Fee Schedule A," on page 404. Violations must be of the same fraud compliance requirement and within the timeframes defined in Table 10-7, "Violations Subject to Fraud Non-Compliance Fee Schedule A," on page 404 to be considered a multiple violation subject to escalating fees.

Table 10-6. Fraud Non-Compliance Fee Schedule A

Non-Compliance	Fee Assessed (USD)
1st Violation	$1,000[1]
2nd Violation	$5,000
3rd Violation	$10,000
4th Violation	$25,000
5th Violation	The fee will be at the discretion of AEGNS.
6th Violation or more	Additional fees will be equal to all penalty fees levied for a 12 month period. The 12 month period begins upon the 1st violation.

1. For UIR, SEAS, or Issuer fraud reporting, in lieu of assessing $1,000 (USD), a non-compliance warning notification will be sent to the Participant, and thereafter subsequent violations will be based on a 12-month rolling assessment.

Note: In addition to the non-compliance fees outlined above, AEGNS reserves the right to collect additional fees associated with the monetary loss sustained to AEGNS or any injured Participants on the AEGNS Network due to any violations subject to this fee table.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.3.2 Violations Subject to Fraud Non-Compliance Fee Schedule A

Table 10-7, "Violations Subject to Fraud Non-Compliance Fee Schedule A," on page 404 summarizes the various fraud related violations and explains what defines a "unique violation" when determining violation levels in Table 10-6, "Fraud Non-Compliance Fee Schedule A," on page 403.

Table 10-7 Violations Subject to Fraud Non-Compliance Fee Schedule A

Fraud Compliance Requirement	Assessment Frequency	Violation Description
FraudNet Registration (Section 8.6, "FraudNet," on page 381)	Monthly	The first month an insufficient registration violation occurs will be considered a first violation Each consecutive month in which a Participant incurs an insufficient registration violation for FraudNet will result in an escalated violation level.
Fraud Reporting (Section 8.7, "Issuer Fraud Reporting," on page 382)	Monthly	The first month of unreported fraud as described in Section 8.7, "Issuer Fraud Reporting," on page 382 will be considered a first violation. Each month thereafter subsequent violations will be based on a 12-month rolling assessment.
Transactions processed after an S/E was to be cancelled. • Section 8.9.2.1, "Fictitious and/or Collusive S/E," on page 385 • Section 8.9.2.5, "Cancelled S/Es (Derogatory)," on page 387 • Section 8.9.2.2, "Illegal or Prohibited Industry," on page 385	When Identified	Any instance in which transactions are processed after an S/E has been placed on the High Risk S/E list, with any of the high risk indicators below, will be considered a unique violation of policy. • "S" Fictitious and/or Collusive S/E, or • "X" Cancelled for derogatory reasons, or • "I" Illegal or Prohibited Industry Each unique violation will be subject to escalating fines. Violations will be tracked for a 12 month period from January 1 through December 31.
Urgent Investigation Request (UIR) Compliance • Section 8.9.3.1, "Acquirer UIR," on page 388 • Section 8.10.3.2, "Issuer UIR," on page 395	Monthly	The first month in which a Participant's UIR compliance rate is below 95% will be considered a first violation. Each month thereafter subsequent violations will be based on a 12-month rolling assessment. (The UIR compliance rate consists of the percentage of non-responses and late responses to all Urgent Investigation Requests in a given month.)
S/E Actioning System (SEAS) • Section 8.9.4, "S/E Actioning System (SEAS)," on page 389	Monthly	The first month in which a Participant's "Overall SEAS Compliance Rate" is below 98% will be considered a 1st violation. Each month thereafter subsequent violations will be based on a 12-month rolling assessment. (The "Overall SEAS Compliance Rate" includes SEAS recommendations which are non-actioned, actioned late or under-actioned by the Acquirer in a given month.)
Issuer Fraud Rate • Section 8.10.4, "Issuer Fraud Rate," on page 396	Quarterly	The 1st quarter and each subsequent quarter in which a Participant does not take appropriate steps to reduce their fraud rate, including providing an adequate fraud reduction plan to AEGNS, will be considered a unique violation of policy. Each unique violation will be subject to escalating fees.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.3.3 5-Digit Card Security Code (5CSC) and Integrated Circuit Card Security Code (iCSC) Program Non-Compliance Fees

AEGNS will assess a non-compliance fee to Participants that fail to comply with 5CSC (or iCSC, if used) encoding requirements. For the first violation in a 12-month rolling period, AEGNS will send a non-compliance warning notification to the Participant. For subsequent violations within the same 12-month rolling period, the fee is detailed in the following table:

Table 10-8. 5CSC and iCSC Program Non-Compliance Fees

Monthly Non-Compliance Fee	$10,000

Note: In addition to the non-compliance fees outlined above, AEGNS reserves the right to collect additional fees associated with the monetary loss sustained to AEGNS or any injured Participants on the AEGN by the failure of the offending Participant to encode 5CSC in accordance with AEGNS policy.

10.3.4 Security and Fraud Investigation Service Fees

A fee may be charged to Participants using American Express Global Security resources. This fee is structured into three (3) plan options depending on the complexity of the investigation or services requested.

Plan 1 - This fee plan is established at AEGNS Deal Implementation and the fee structure is based upon the Participant's security needs and other services purchased at the time of signing.

Plan 2 - This fee plan allows Participants with a large, unexpected security or investigative requirement to establish a one (1) year servicing agreement for a flat fee of $25,000 (USD) and a pre-arranged work support agreement.

Plan 3 - This fee plan is structured for Participants needing consultation and security services on a case by case basis. The plan allows for invoicing and payment at a rate of $170 (USD) per hour for services used.

For more information, contact your AEGNS representative.

10.3.5 FraudNet License Fees

Participants must be licensed by AEGNS to use FraudNet. The following table outlines the fee schedule:

Table 10-9. FraudNet Reporting Fees

Fee Type	Fee Amount (USD)	Frequency
FraudNet License Fee	$540	Monthly

AEGNS requires at least one (1) FraudNet user per Participant. AEGNS encourages Participants to have enough users to ensure coverage outside regular working hours, including weekends and national holidays. Refer to the *GNS FraudNet User Guide* on Knowledge Base and the "Security and Fraud" chapter beginning on page 375 in the *Business and Operational Policies* manual for more information.

Note: Participants that operate in multiple countries and/or have multiple Organization Identifiers will be assessed this fee once each month.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.3.6 Urgent Investigation Request (UIR) Fees

Participants who originate (file) UIRs (Filing Network Participants) will be assessed a fee of $5 (USD) per originated UIR. This fee will be assessed once per quarter for all UIRs originated in the prior quarter.

AEGNS requires that at least one (1) FraudNet User be registered for UIRs per Participant. AEGNS encourages Participants to have enough users to ensure their ability to meet UIR timeframe requirements, including coverage outside regular working hours, including weekends and national holidays.

Refer to the *GNS FraudNet User Guide* on Knowledge Base and the "Security and Fraud" chapter beginning on page 375 in the *Business and Operational Policies* manual for more information.

The following table outlines the fee schedule:

Table 10-10. FraudNet Reporting Fees

Fee Type	Fee Amount (USD)	Frequency
Urgent Investigation Request (UIR) Fee	$5.00	Quarterly

10.4 Network Connectivity Fees

The following sections specify fees associated with Network connectivity. Participants must link to the Network using one (1) of the approved connection methods agreed by the Participant and AEGNS. For additional information, see the "AEGNS Systems Access and Interface Requirements" chapter beginning on page 415.

10.4.1 GLOBE Fees

The fees related to the GLOBE, as defined in the "AEGNS Systems Access and Interface Requirements" chapter beginning on page 415, including insurance fees, are specified in the Lease/License Agreement (if applicable) or the Participant Agreement.

10.4.2 GLOBE Relocation Fees

GLOBE Participants will pay a fee to AEGNS to cover AEGNS' costs of relocating a GLOBE Package. These fees include the total actual GLOBE relocation costs, and any emergency connectivity and/or configuration recovery expense associated with re-establishing GLOBE connectivity in the event service connection is lost due to Participant mishandling. The fees will be billed directly to the GLOBE Participant.

See the "AEGNS Systems Access and Interface Requirements" chapter beginning on page 415.

10.4.3 Internet Virtual Private Network Fees

The fees related to Internet Virtual Private Network (IVPN) are specified in the Participant Agreement. Participant shall be independently responsible for fees related to Internet access and connectivity. For additional information, see the "AEGNS Systems Access and Interface Requirements" chapter beginning on page 415.

10.5 Service Fees

The following sections detail the fees associated with services. For additional information, please contact your AEGNS representative.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.5.1 Remittance Fees

When a Cardmember initiates a remittance through an American Express Entity or when a Cardmember misdirects an online payment to American Express, a $50 (USD) fee will be charged to the Issuer.

10.5.2 Product Enhancement Service Fees

AEGNS will arrange with certified vendors to provide the Product Enhancements offered. AEGNS will bill the Participant based on the negotiated price with the vendor. The billing for Product Enhancements will appear on the Participant's Daily Settlement Advisement.

10.5.3 Fees for Additional Cardmember Benefits and Services

Contact your AEGNS representative for additional information.

10.5.4 ATM Service Fees

The network fees for ATM transactions are specified in the Participant Agreement or ATM agreement.

10.5.5 Active BIN Rental Fee

AEGNS will assess a fee to Issuers for each active BIN assigned to them.

Table 10-11. Active BIN Rental Fees

Amount	Assessment Basis	Assessment Frequency
$175 USD	Per active BIN	Monthly

10.5.6 Network Test Simulator Fees

The Network Test Simulator Fees shall be paid according to Table 10-12. Refer to Section 11.7, "Network Test Simulator," on page 424 to for information about how to access the Network Test Simulator.

Table 10-12. Network Test Simulator Fees

Fee Type	Payment Due	Fee Amount (USD)
Certification Network Test Simulator	Payable upon initial launch of the Network Test Simulator and then yearly following each anniversary of the initial launch.	$2550 (includes 3 users)
Additional Users	Payable upon implementation of additional user. May be prorated to the anniversary date of the Network Test Simulator being deployed and then annually thereafter.	$250
Developer's Functionality	Payable upon initial launch of the Network Test Simulator and then yearly following each anniversary of the initial launch. Payable upon implementation of developer functionality. May be prorated to the anniversary date of the Network Test Simulator being deployed and then annually thereafter.	$500

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.5.7 Manual Funds Exchange Processing Fee

All Participants processing settlements manually will be assessed a monthly service fee to offset the expense to AEGNS of maintaining the costly manual process. See Section 6.4.2.2, "Manual Funds Exchange," on page 274 for more information.

Table 10-13. Manual Funds Exchange Processing Fees

Fee Type	Amount	Frequency
Manual Funds Exchange Processing Fee	$500	Monthly

10.5.8 Settlement Advisement Fee

All Participants will be assessed a monthly fee for the provision of a Settlement Advisement at the request of the Participant and/or to support the Participant's Settlement process when the Net Settlement needs to be calculated outside of the standard daily Settlement and Funds Exchange service.

Table 10-14. Settlement Advisement Fee

Payer	Amount	Assessment Basis	Assessment Frequency
Participant	$200	Per Organization Identifier and currency combination	Monthly

See Section 6.4.1.2, "Settlement Advisement," on page 273 for more information.

10.5.9 Late Settlement Fee

All Participants will be assessed a fee for each delayed Settlement as a result of Participant failure to process a Funds Exchange within the timeframes established by AEGNS.

Table 10-15. Late Settlement Fee

Payer	Amount	Assessment Basis	Assessment Frequency
Participant	$500	Per late Settlement	Per incident

See Section 6.2, "Overview," on page 269 for more information related to the Settlement process.

10.5.10 Funds Exchange Reissue Fee

All Participants will be assessed for each reissued Funds Exchange due to a Funds Exchange failure attributable to the Participant.

Table 10-16. Funds Exchange Reissue Fee

Payer	Amount	Assessment Basis	Assessment Frequency
Participant	$500	Per Funds Exchange reissued	Per incident

See Section 6.4.3.2, "Participant Failure to Settle on a Timely Basis," on page 275 for more information.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.5.11 Premium Product Platform (PPP) Fees

Issuers (including their contracted American Express-approved vendors) must be licensed by AEGNS to use the Premium Product Platform (PPP). Platform fees are based on the Card product(s) (American Express Enterprise Line Centurion, American Express Enterprise Line Platinum, or Blue Box Line Super Premium) issued, the modules selected by the Issuer, and the number of users each Issuer and/or their respective vendors requested.

Table 10-17. Premium Product Platform (PPP) Fees

Type of Product	Core Modules[1]	Case Management	Fee Frequency	Notes
First product (e.g., American Express Enterprise Line, Platinum)	$833	$417	Monthly	Per Issuer
Second product (e.g., American Express Enterprise Line Platinum and Blue Box Line Super Premium)	$1,250	$417	Monthly	Per Issuer
Licenses	$18	N/A	Monthly	Per Issuer per user First five (5) user licenses per Issuer are complimentary

1. Core Modules are as follows: Person Account, Benefit Content, Recommendations, Elite Tier Registrations, Metrics, and Customer Preferences.

10.5.12 Issuer Personalization Certification Testing

Issuers of Advanced Payment Products are required to successfully complete the end-to-end Issuer personalization Certification process for all such products. Fees associated with Certification testing are described in this section.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.5.12.1Online Personalization Validation Tool Fees

Online Personalization Validation (OPV) is an online Certification tool allowing Issuers to self-test and validate that their payment products are configured according to AEGNS requirements. Refer to the *Issuer Personalization Certification Guide* for further information.

Issuers must adopt the Online Personalization Validation (OPV) tool for Issuer Personalization Certification testing purposes.

The fees defined below are charged on a per Certification basis. If multiple Certification types are required to be certified concurrently, the highest listed fee will apply and cover all Certifications.

Table 10-18. Online Personalization Validation Tool Fees

Certification Type	Fees
New Profile: • New Issuer/new to EMV • Existing Issuers with new profile • New chip • Change to a personalization bureau	$6,000
Changes to Existing Profile: • Change to CVM • Profile changes	$3,500
Issuer Public Key Extension or Renewal	$1,500

Note: Contact your AEGNS representative if exceptional circumstances prevent use of the OPV tool.

Note: Only in exceptional circumstances, and with prior approval from the AEGNS Certification team, will Cards be submitted to AEGNS for lab testing. Refer to Table 10-19, "AEGNS-Led Issuer Personalization Certification Testing Fees," on page 410.

10.5.12.2AEGNS-Led Issuer Personalization Certification Testing Fees

The fees described in the table below are applicable only in exceptional circumstances and only with prior approval from the AEGNS Certification team.

Table 10-19. AEGNS-Led Issuer Personalization Certification Testing Fees

Fee Type	Fees
Per Certification Fee	$15,000
User Acceptance Testing Fee	$3,000 (per round)
Chip Beta Testing Fee	$1,500 (per round)

User acceptance testing is conducted at a Chip Card product level and typically per BIN or EMV profile (prompted by the use of different keys per BIN issued and the different EMV profiles, when applicable).

A Chip Beta Test is then conducted at a Card type level. Typically, each plastic type or Card product is assigned to a Chip product or BIN that has completed user acceptance testing.

The user acceptance testing and Chip Beta testing fees quoted above are per round of testing. The fees ultimately billed may differ from the original estimate, depending on the number of rounds of testing required to successfully complete Issuer personalization Certification.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.6 Data Security Fees

The following sections detail the fees associated with Data Security Policy. Refer to Section 2.4, "Participant Data Security Policy," on page 38 for additional information.

10.6.1 Data Security Policy (DSP) Non-Compliance Fees

All Participants must comply with the AEGNS Data Security Policy. Participants that fail to comply with DSP may be subject to fees, as described below.

Table 10-20. Data Security Policy (DSP) Non-Compliance Fees

Standard	Fee
First non-compliance incident in a rolling 12-month period	Up to $50,000 (USD)
Each subsequent non-compliance incident in a rolling 12-month period	Up to $100,000 (USD)

10.6.2 Notification of Data Compromise Non-Compliance Fees

Failure to notify AEGNS of a suspected or confirmed Data Compromise can result in increased costs and liability to all parties. Any Participant who does not comply with the notification provisions of the AEGNS Data Security Policy will be subject to a non-compliance fee of up to $100,000 (USD) per incident. Refer to Section 2.4.9, "Requirements for Notification of Data Compromise," on page 47 for details.

10.7 Miscellaneous

The following sections detail fees and assessments not classified in a unique section. For additional information, please contact your AEGNS representative.

10.7.1 General Non-Compliance Fees

AEGNS may assess fees to Participants for violations of GNS policy documented in the *Business and Operational Policies* manual. These fees may be assessed when there are no pre-defined compliance fees for the policy violation or when pre-defined compliance fees have been assessed, but the Participant has not taken action to correct the policy violation. The General Non-Compliance Fees will be assessed as follows:

Table 10-21. General Non-Compliance Fees

Compliance Violation	Fees
First violation of policy regulation	Up to $5,000 (USD)
Second violation of the same policy regulation within a 12-month period after notification of the 1st violation from AEGNS	Up to $5,000 (USD)
Third violation of the same policy regulation within a 12-month period after notification of the 1st violation from AEGNS	Up to $10,000 (USD)
Fourth violation of the same policy regulation within a 12-month period after notification of the 1st violation from AEGNS	Up to $25,000 (USD)
Fifth violation of the same policy regulation within a 12-month period after notification of the 1st violation from AEGNS and assessed each month the violation remains uncorrected	Up to $50,000 (USD)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.7.2 Brand Protection Fees

10.7.2.1 Brand Protection Assessment Fees

AEGNS will assess a processing fee, which covers the following:

- Evaluation of the questionnaire (for which AEGNS may procure the services of a third party).
- A report on findings which will be sent to the Acquirer.
- Subsequent work required to track remediation efforts and the issuance of a letter from AEGNS confirming the Brand Protection Assessment has been completed to the satisfaction of AEGNS.

If applicable, the letter will also state that the Acquirer is approved, subject to all other requirements of the *Business and Operational Policies* manual, to acquire S/Es in industries or participating in activities listed in Section 2.9.4.2, "Restricted Industries," on page 95.

Table 10-22. Brand Protection Assessment Fees

Assessment Level	Processing Fees
Initial	$20,000 (USD)
Supplemental	$10,000 (USD)

10.7.2.2 Brand Protection Non-Compliance Fees

Acquirers are subject to Brand Protection non-compliance fees as described in Table 10-23, "Brand Protection Non-Compliance Fees," on page 412 for violations of the Brand Protection policies. Brand Protection non-compliance fees for violations related to Illegal or Brand Damaging Activity will be waived if the Acquirer reports the violations to AEGNS in writing before AEGNS notifies the Acquirer of the violations, so long as the violations are then corrected according to policy stated in Section 2.9.5.4, "Correcting Violations," on page 99.

Table 10-23. Brand Protection Non-Compliance Fees

Violation	Non-Compliance Fees
Illegal or Brand Damaging Activity	1st violation within a 12 month period: Up to $20,000 (USD). 2nd violation within a 12 month period subsequent to the first violation: Up to $50,000 (USD). 3rd and all subsequent violations within a 12 month period subsequent to the first violation: Up to $100,000 (USD).
Failure to complete an investigation and respond in writing to AEGNS with all requested information when notified of a violation of Brand Protection policies, within the timeframes stated in Table 2-12, "Investigation Time Periods," on page 99.	1st violation within a 12 month period: Up to $10,000 (USD). 2nd violation within a 12 month period subsequent to the first violation: Up to $50,000 (USD). 3rd and all subsequent violations within a 12 month period subsequent to the first violation: Up to $100,000 (USD).
Failure to correct violations within timeframes stated in Section 2.9.5.4, "Correcting Violations," on page 99	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 10-23. Brand Protection Non-Compliance Fees (continued)

Incorrect MCC assigned to S/E in industry listed in Table 2-11, "Restricted Industries Requirements," on page 95	1st violation within a 12 month period: Up to $10,000 (USD) per S/E or Sponsored Merchant. 2nd violation within a 12 month period subsequent to the first violation: Up to $50,000 (USD) per S/E or Sponsored Merchant. 3rd and all subsequent violations within a 12 month period subsequent to the first violation: Up to $100,000 (USD) per S/E or Sponsored Merchant.
Non-conforming Point of Service Data Code[1] on transactions from S/E in an industry listed in Table 2-11, "Restricted Industries Requirements," on page 95	
Failure to complete a Brand Protection Assessment when required by AEGNS	1st violation within a twelve (12) month period: Up to $10,000 (USD). 2nd violation within a twelve (12) month period subsequent to the first violation: Up to $50,000 (USD). 3rd and all subsequent violations within a twelve (12) month period subsequent to the first violation: Up to $100,000 (USD).
Failure to correct any deficiencies (as determined by AEGNS) that may be identified during a Brand Protection Assessment	
Failure to register an S/E or Payment Facilitator that meets the criteria listed in Section 2.9.4.2, "Restricted Industries," on page 95 prior to the S/E transacting on the Network	Up to $10,000 (USD) per S/E or Payment Facilitator

1. See the *Codes Reference Guide* for more information.

10.7.3 Reporting Fees

The ability to utilize reporting to analyze, plan, and improve business is essential to successfully operate on the American Express Global Network. Reports are available in Reporting Center.

10.7.3.1 Portfolio Reporting Fee

This mandatory fee is assessed to all Participants. The initial Portfolio Reporting available will be the Enhanced Dispute Reports (EDR) to support the Global Disputes Monitoring Program (GDMP) Compliance Program. EDR report types include high level summary reports, transaction summary reports, and detailed transaction information. The data in the reports includes disputes volume and dispute rates separated into Chargeback types. Participants can view the dispute rates for their region and for the American Express Global Network.

Table 10-24. Portfolio Reporting Fees

Fee Type	Fee Amount (USD)	Frequency
Portfolio Reporting Fee	$250	Monthly

Note: Participants that operate in multiple countries and/or have multiple Organization Identifiers will be assessed this fee once each month.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

10.7.4 Network Assessment Program Reports and Fees

The following tables detail the availability of reports and fees associated with the Network Assessment Program. See Section 2.2.17.1, "Network Assessment Program," on page 27 for more information.

Table 10-25. Report Availability and Fees

Report	Annual Report Availability	Fees
SOC 1	December 15	$0
SOC 2	August 15	$0
Ethical Hacking (per application)	September 30	$0

Table 10-26. Operational Support Fee Schedule

Report	Fees
Assessment fee - per assessment	$135,000
Additional Ethical Hacking – per additional application	Fee established upon request from the Participant



This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11 AEGNS Systems Access and Interface Requirements

11.1 Introduction

The purpose of this chapter is to supply the American Express Global Network (AEGN) Acquirers and Issuers with the information necessary to access AEGNS systems and interface Participant systems with AEGN systems and equipment. This chapter includes policies regarding AEGNS Systems User Access and the use of American Express owned hardware and software, including licensing requirements.

American Express Global Network Services (AEGNS) has established a highly reliable and efficient global network. The highest quality industry providers and products are utilized where available. The overall Network is monitored twenty-four (24) hours per day, 365 days per year. If a Global Online Business Exchange (GLOBE) or IVPN Participant experiences any issues in performance or reliability, they should immediately notify the AEGN Help Desk.

11.2 AEGNS Systems User Access Policy

As business needs dictate, Participants (which include their Authorized Processors and vendors) may require access to certain AEGNS systems including Knowledge Base, Network Disputes Manager, and other distributed or mainframe systems.

AEGNS has established policies, standards, and procedures which work together to express expectations, requirements, and actions required to ensure appropriate access control over AEGNS systems.

For questions regarding the AEGNS Systems User Access policy, send an email to GNS User Services at gns.user.services@aexp.com.

11.2.1 Requesting Access to AEGNS Systems

Only individuals within Participant organizations who have a specific business-driven need to access AEGNS' systems should request this access. Access to AEGNS' systems must be requested through an approved American Express user access form or online enrollment process.

All access requests must be supported with a valid business justification and manager approval. User access forms must be fully completed by the individual who is requesting access to AEGNS' system and the requestor must agree to the specific terms and conditions for the requested system access.

For further information regarding approved American Express user access forms or about requesting access to AEGNS' systems, contact your AEGNS Operations Manager. To request access to Knowledge Base Services, go to www.amexglobalnetwork.com/knowledgebase.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.2.2 Access Control Policy

Personnel must be positively authenticated and authorized prior to being granted access to American Express information resources. Access must be based on an employee's role, and is limited to the minimum necessary to perform their job function. The following access control policy governs user access to AEGNS systems:

- Access will be strictly limited to appropriate individuals on a need-to-know and least privileged basis, where "least privilege" means that an individual shall be able to access only such information and resources that are necessary to perform their legitimate job function.
- All users must be uniquely identified prior to obtaining access to American Express systems.
- Connections to AEGNS' systems must use Authentication, which is defined as a "user ID" and "password."
- All user accounts for third-party access to American Express networks or systems must only be enabled upon approval of American Express management and must be disabled upon completion of the services being provided.
- The immediate manager of the user or the User Certification Contact is responsible for ensuring that user access privileges are changed in accordance with new job functions or assignments.

11.2.3 User Level Policy

The following policies apply to individual users who have been granted access to AEGNS systems:

1. In connection with the use of AEGNS systems, users must not access:
   a. Their own Cardmember Account for any reason
   b. Another employee's Cardmember Account if they have personal knowledge that the Account holder is an employee
   c. Any Cardmember Account that they are not required to access as part of the performance of their job
2. Users of American Express' information resources are accountable for all actions performed under their User ID and are responsible for protecting and managing the confidentiality of their passwords.
3. Each user must have a unique identifier (User ID) which is never shared.
4. Each user will protect their User ID with a password that must never be shared. The user's password identifies them to the system. The computer system tracks all entries that are made by the Person who makes them. If a user's password is used by anyone in a manner that results in errors or fraud, they shall be held accountable for such errors or fraud.
5. Users shall not use another Person's password or User ID.
6. Passwords must not be saved or embedded in function keys, scripts, macros or other similar ways.
7. Passwords must be changed at least every 30 days for each AEGNS system.
8. User IDs and passwords must not be recorded where they can be seen or found.
9. User IDs may be suspended or revoked from use if they have not been used for 35 consecutive days.
10. User accounts not used for 90 days may be deleted from the AEGNS system.
11. Users must sign off or log out of their user account when they leave their workstation including, but not limited to, time away from their workstation for breaks, lunch, meetings, etc.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.2.4 Information Security Awareness Training

All users (including Participant's employees, contractors, temporary workers, and vendors) with access to AEGNS systems and data are required to complete the security awareness training annually. AEGNS data includes highly sensitive information such as S/E and transactional information, Cardmember details (i.e., Personally Identifiable Information (PII)), and any other data considered highly sensitive.

At a minimum, information security awareness training must incorporate:

- Creating strong passwords
- Phishing techniques/identification and malware
- Protecting American Express information
- Importance of encrypting and storing sensitive data
- Reporting and managing data security incidents

AEGNS provides two (2) options for meeting this requirement:

- Participants deliver their own internal information security awareness training that meets the minimum listed requirements above.
- Participants request written information security awareness training materials from AEGNS and Participant delivers training internally.

Participants must provide AEGNS with an attestation of compliance confirming adherence to information security awareness training requirements. The attestation submission period for a given Participant will be determined by AEGNS and communicated to the Participant together with instructions for completing the attestation. Participants that fail to comply with information security awareness training requirements in accordance with this section or that do not submit the attestation of compliance may be subject to non-compliance fees as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

AEGNS reserves the right to conduct an audit of the Participant's compliance to the information security awareness training requirements in accordance with Section 2.2.17, "Audit Rights," on page 26.

AEGNS may revoke user access for any individual(s) failing to adhere to these requirements.
For more details about information security awareness training, contact your AEGNS representative.

11.2.5 Timely Notification of Changes in User Access

Participants are responsible for immediately notifying AEGNS of any changes to a user's employment status within their organization, or at an Authorized Processor or Vendor, that would affect the user's need to access AEGNS systems. Changes in a user's employment status that could affect user access include changes in the user's job function or assignment and user resignations, terminations or transfers.

Participants are responsible for designating an authorized User Certification Contact within their organization who will be responsible for notifying AEGNS of any users who no longer require access to AEGNS systems. This notification must be processed via the GNS User Certification service available through Knowledge Base immediately after the change in the user's employment status.

For more information about this requirement or the GNS User Certification service, send an email to GNS User Services at gns.user.services@aexp.com.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.2.6 User Re-Certification

AEGNS reserves the right to audit user access to AEGNS' systems at any time. Periodically, AEGNS will notify Participants that they must verify the users from their organization who have access to specific AEGNS systems. Participants are responsible for designating a User Certification Contact within their organization who will be responsible for responding to these requests via the GNS User Certification service available through Knowledge Base. Failure to respond to user re-Certification requests shall result in users' access to AEGNS systems being revoked. For further information regarding the AEGNS user re-Certification process or the GNS User Certification service, send an email to GNS User Services at gns.user.services@aexp.com.

11.2.7 Confidentiality

In connection with work performed for their job, users of AEGNS systems may have access to confidential AEGNS information. Examples of confidential information include, but are not limited to, any information relating to AEGNS' or any of its Participants' customer lists, customer Account information, marketing philosophy and objectives, competitive advantages and disadvantages, financial results, product features, product development, advertising and sales programs and other information which would give AEGNS or its Participants an opportunity to obtain an advantage over its competitors or which AEGNS or its Participants is ethically or legally obligated to protect from unauthorized sources.

AEGNS desires to protect its confidential information and requires that users of AEGNS systems safeguard all confidential information and not reveal confidential information to any third party (including, without limitation, at conferences, seminars, meetings of professional organizations, by publication in journals or the granting of interviews to journalists or other members of the news media) or use confidential information for their own benefit or the benefit of any third party, except to the extent necessarily required for performance of their jobs.

Users of AEGNS systems must help safeguard AEGNS customers' expectations of privacy by exercising diligence and care in the handling of confidential information relating to such customers.

11.2.8 Security Policy Violations

Participants are responsible for notifying AEGNS of any known violation to the AEGNS Systems User Access policy. Additionally, Participants are required to take appropriate disciplinary action with respect to any individual within their organization who willfully disregard these policies, up to and including discharge from their employment. Any violation of the User Access policy should be reported to GNS Information Security by email to GNS User Services at gns.user.services@aexp.com.

11.3 AEGNS Email Policy

Participants and their Service Providers are required to ensure that all sensitive or confidential data, including information sent to AEGNS personnel via email, is encrypted.

Data transmitted between Participants or their Service Providers and AEGNS via connections such as the GLOBE or IVPN, or systems such as AEGNS Network Disputes Manager and FraudNet are already secure. If Participants or their Service Providers need to exchange sensitive or confidential data, including Cardmember Information or Personally Identifiable Information (PII), via email, the email must be encrypted by the sender. Any email responses back to the sender containing any such sensitive or confidential information must also be encrypted. Participants who do not comply with this policy may be subject to non-compliance fees as described in Section 10.7.1, "General Non-Compliance Fees," on page 411.

AEGNS reserves the right to request from Participants, at its own discretion, Documentation confirming the use of secure email communication as stated in this section.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.3.1 Transport Layer Security Configuration Implementation

The AEGNS standard for secure encrypted email is Transport Layer Security (TLS). Participants and their Service Providers that communicate directly with AEGNS (i.e., "@aexp.com" email domain) must configure their email servers to require TLS to create a secure and encrypted email channel for emails. Email communications between a Participant and its Service Providers (including cloud services) that contain any American Express data must also utilize TLS or another more secure Encryption method to secure the communication.

Participants and their Service Providers must coordinate with AEGNS to test and implement secure email technology. Please note that the implementation of secure email technology will be limited to email exchange between Participants and/or their Service Providers and AEGNS.

For more information on the implementation and testing of a secure email technology, please contact your AEGNS representative.

11.3.2 Domain Name System Requirements

Participants and their Service Providers who do not utilize Domain Name System (DNS) may experience a loss of communications into and/or from AEGNS due to Internet Protocol (IP) address changes within the Network. DNS is a method to associate the name of a domain (for example @aexp.com) to an IP address and facilitates the delivery of emails. DNS must be used for email domain name resolution for email gateway connections rather than static IP addresses on the Network.

11.4 Security

Information, and the technology used to support that information, has significant value to AEGNS and Participants. Both are subject to various threats that, if realized, could result in direct financial loss to AEGNS and Participants.

11.4.1 Connectivity Security

All connections between the Network and Participants must have sufficient access control and monitoring in place to limit Network communication to approved applications and Participants only.

11.4.2 Information Security

Where applicable, confidentiality and integrity of data exchanged between the Participant and AEGNS must be secure and access must be restricted to appropriate personnel. This will ensure that only authorized personnel have access to sensitive data. Connections and equipment utilized for Network connectivity shall be used only in accordance with the Network Manuals or as specifically agreed, in written form, with the Network. Participants must implement reasonable measures to ensure that no other party has access to equipment or facilities used to maintain Participants connectivity to the Network.

11.5 Participant Connectivity to the Network

Participants are required to maintain a persistent connection between Participant host systems and the Network in order to enable the exchange of data files and online real-time transaction messages. The manner in which a Participant connects to the Network will be jointly determined by the Participant and AEGNS following consideration of available capabilities, relevant market regulations and other applicable factors. Generally, Participants will connect to the network via one (1) or a combination of the following methods:

- GLOBE
- Internet Virtual Private Network (IVPN) across the Internet

The following sections specify the above methods in more detail.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.5.1 The GLOBE

The Global Online Business Exchange (GLOBE) is a method of connectivity between a Participant and the Network. The GLOBE is a proprietary hardware platform designed to route communications messages traveling into and out of a Participant's network. A GLOBE is generally located at a pre-approved Participant location, typically in the same data center or suite as the Participant's host processing platforms. This close proximity is important because the GLOBE provides sophisticated real-time monitoring that may alert our teams to problems even before they impact our customers. Such close monitoring is only provided with a GLOBE solution.

The GLOBE is a platform that serves as a gateway between a Participant's host systems and the Network. The GLOBE consists of networking equipment and security equipment that enable Participants to establish Network and application connectivity between their host systems and the Network, connecting the Participant's processing center with the Network. It supports the online transmittal of Authorization traffic and the electronic transfer of data and report files.

AEGNS designs, provides, and maintains the GLOBE at the Participant's agreed processing site. AEGNS is the sole owner of the GLOBE residing on the processing site. As applicable, AEGNS rents the GLOBE to Participants or Authorized Processors in accordance with the provisions of this manual, the *Network Connectivity* manual, or any other applicable AEGNS manual.

11.5.1.1 Additional Requirements

The following sections apply to Participants connecting to the Network via a GLOBE.

11.5.1.1.1 Terms and Conditions

1. Title to the GLOBE is and at all times shall remain in AEGNS, and the Participant shall not cause or suffer any substitution, exchange, or addition of or to a GLOBE.
2. The GLOBE is and shall remain property of AEGNS and shall not be attached to or become part of any realty.
3. AEGNS will deliver the GLOBE to the Participant or its Authorized Processor at the location and time agreed by AEGNS and the Participant, but shall not be required to deliver the GLOBE until all relevant import and export approvals, permissions, permits, and licenses have been obtained. AEGNS shall have no liability to the Participant for any delay in obtaining export approvals, permissions, permits, or licenses. The GLOBE shall be installed and used at the address of the Participant or such other location as agreed by AEGNS, and the Participant shall not relocate a GLOBE or any component without the prior written consent of AEGNS. Written consent, if granted, will be provided to the Participant within ten (10) days of the Participant’s notification to AEGNS of the intent to move the GLOBE. In the event such prior written consent is granted by AEGNS, the Participant shall strictly adhere to any and all guidelines and procedures regarding GLOBE relocation, as prescribed by the AEGNS manuals, by written agreement, or any written communication by AEGNS or its designee.
4. The Participant will not sell, mortgage, assign, transfer, lease, sublet, loan, part with possession of or encumber the GLOBE or any component or permit any liens or charges to become effective thereon or permit or attempt to do any of the acts aforesaid.
5. The Participant shall, at the Participant's own expense, take such action as may be necessary:
    a. To remove any encumbrance, lien or charge.
    b. To prevent any third party from acquiring any other interest in the GLOBE (including, without limitation, by reason of the GLOBE being deemed to be a fixture or part of any realty). Prior to the relocation of the GLOBE or any component, the Participant shall promptly execute and deliver such agreements and documents as may be reasonably requested by AEGNS in connection with such relocation, including (without limitation) any financing statements or other documents required to protect AEGNS' interest under applicable law.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6. EXCEPT AS EXPRESSLY PROVIDED IN THIS CHAPTER OR IN THE PARTICIPANT AGREEMENT, AEGNS PROVIDES THE GLOBE OR ANY OTHER METHOD OF NETWORK CONNECTIVITY TO PARTICIPANT "AS IS" AND MAKES NO AND EXPRESSLY DISCLAIMS ALL OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OR OF NON-INFRINGEMENT. PARTICIPANT IS SOLELY RESPONSIBLE FOR ADEQUATE SAFEGUARDS AND PROTECTIONS OF THE MANNER IN WHICH IT CONNECTS TO THE NETWORK, INCLUDING ANY INFORMATION AND DATA OR ANY OTHER MATERIALS AND/OR INFORMATION THAT MAY BE INCLUDED IN OR AFFECTED BY SUCH CONNECTIVITY. PARTICIPANT'S SOLE REMEDY, AND AEGNS' SOLE RESPONSIBILITY, IN THE EVENT OF ANY FAILURE OR MALFUNCTION OF SUCH CONNECTIVITY SHALL BE TO REPAIR OR REPLACE THE CONNECTION, UNLESS EXPLICITLY SET OUT IN THE MANUALS OR THE PARTICIPANT AGREEMENT.
7. Upon the request of AEGNS, the Participant will permit AEGNS or a designee of AEGNS to have access to the GLOBE at all reasonable times for the purpose of inspection and examination. The Participant shall neither make nor cause to be made any alterations in the GLOBE without the prior written consent of AEGNS.

11.5.1.1.2 Risk of Loss

For the period from the date on which the GLOBE is delivered to the Participant or the Participant's agent until the date of its redelivery to AEGNS:

1. The GLOBE shall be held at all times at the sole risk of the Participant for injury, damage (including, without limitation, damage to third parties and their property), loss, destruction, theft, expropriation or requisition (as to either title or use).
2. In case before return to AEGNS a GLOBE is destroyed, lost, stolen, or otherwise appropriated, the Participant agrees promptly to notify AEGNS and to pay, or cause to be paid, at AEGNS' option, on demand, as reimbursement to AEGNS for such loss, an amount equal to the fair market value of the GLOBE at the time of the loss as reasonably determined by AEGNS, or another amount agreed between the Participant and the Network, in either case, payment of which shall relieve the Participant from liability for any further rent with respect to such GLOBE. Such amount may be offset by any amount received by AEGNS under an insurance policy for which premiums have been wholly paid for by the Participant.

11.5.1.1.3 Insurance

In exchange for the fees paid by the Participant as set out in the "Network Fees" chapter beginning on page 401 for the period from the date on which the GLOBE is delivered to the Participant or the Participant's agent until the date of its redelivery to AEGNS, AEGNS will obtain insurance on behalf of the Participant, naming American Express or AEGNS as "loss payee" against the loss, theft or destruction of or damage to the GLOBE, including loss by fire and all risks of physical loss. The deductible, payment of which shall be the responsibility of the Participant in the event of any loss, will not exceed $10,000 (USD). In the event the deductible is increased, AEGNS must notify the Participant in advance of any claim.

In addition, the Participant shall obtain public liability insurance, naming American Express as an "additional insured," covering both personal injury and property damage arising out of or in connection with the use or operation of the GLOBE. All such insurance shall be with companies rated by a public rating agency and shall carry a rating of "very good" or better, or "investment grade" or better, in an amount no less than $1,000,000 (USD) combined single limit personal injury and property damage. Certificates evidencing said coverage should indicate that American Express is included as "additional insured" under the Participant's general liability insurance. The Participant hereby appoints AEGNS as the Participant's attorney-in-fact to make claim for, receive payment of, execute and endorse all documents, checks or drafts for loss or damage under any such insurance policy. In the event the amount of insurance proceeds with respect to any total loss is less than the amount due to AEGNS under Section 11.5.1.1.2, "Risk of Loss," on page 421, the Participant agrees to promptly pay to AEGNS the difference in such amounts.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.5.1.1.4 GLOBE Relocation

Participants must notify AEGNS of their intent to relocate a GLOBE, adhering to the timeframes shown in Table 11-1, "GLOBE Relocation Requirements," on page 422. AEGNS will provide approval for the relocation within ten (10) Business Days of the required notification date. Depending on the complexity of the intended move, an IP address, Telecom, and GLOBE configuration may be needed.

Level 3 moves must be coordinated by AEGNS.

Participants that fail to meet the notification requirements may be subject to a non-compliance fee as stated in Section 10.7.1, "General Non-Compliance Fees," on page 411.

Table 11-1. GLOBE Relocation Requirements

Move Type	Move Description	Required Move Notice Time	General Comments
Level 1	Moving within same floor of same building	30 days	No change is required in telecommunications, IP address, or port. Minimal AEGNS or Help Desk support is required.
Level 2	Moving to a different floor of same building	60 days	Possible change in telecommunications, IP address, or port. Limited AEGNS or Help Desk support is required.
Level 3	Moving to a different building	120 days Circuit order lead time will vary by country and a minimum of 120 days is required and may take longer in some countries. AEGNS will notify the Participant of the lead time for relocating the circuit within 45 days of receipt of GLOBE Relocation Request.	Required change in telecommunications. Possible change in IP address and port. Full AEGNS or Help Desk support is required. Level of support determined by the complexity of move requested.

11.5.1.1.5 GLOBE Returns

Within ten (10) days following the expiration or termination of the Participant Agreement, the Participant shall arrange for the return of the GLOBE in accordance with AEGNS' reasonable instructions.

In such event, or in the event a GLOBE is required to be returned to AEGNS for any other reason, the Participant shall be responsible for covering all expenses associated with the proper packaging and shipment of the GLOBE. Due to the proprietary nature of the GLOBE, and the confidential data housed on the equipment, the packaging and shipping of the GLOBE must be performed by a vendor certified by AEGNS to perform such activity. For information on vendors certified for this purpose, contact your AEGNS representative.

11.5.1.2 General

The Participant shall pay, or cause to be paid, to AEGNS the replacement cost and/or the repair and refurbishing cost, including cleaning, for an amount designated by AEGNS, if any GLOBE is returned damaged or incomplete, or shows signs of excessive wear and tear, within ten (10) days of AEGNS' request.

In the event the GLOBE, in the form provided to the Participant, is decommissioned, redesigned, or becomes otherwise non-compliant with applicable law or the policies contained in the Manuals, AEGNS shall work with the Participant to implement an alternative method enabling Participant connectivity with the Network and the parties shall execute any agreements or other documents necessary to effectuate such change.

If the Participant becomes aware of any actual, alleged, or threatened claim or action arising from any claim that the GLOBE, in whole or in part, or the Participant's use thereof, infringes the rights of any third party, the

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Participant shall immediately notify AEGNS and provide copies of any papers or documents related to such claim which are in the Participant's possession.

The Participant shall pay all taxes (including personal property, sales, and VAT) and import duties imposed on:

- The GLOBE,
- Its importation into the country where the delivery address is located, and
- Any GLOBE-related fees, exclusive, however, of taxes based on AEGNS' income, which taxes shall be paid by AEGNS.

If any tax for which the Participant is responsible hereunder is paid by AEGNS, the Participant will reimburse American Express upon AEGNS' submission of proof of payment.

11.5.2 Internet Virtual Private Network Connections

Internet Virtual Private Network (IVPN) is a low cost, encrypted Network connectivity solution that provides high availability and security via Internet Protocol Security (IPSec). High availability consists of redundant regional AMEX hubs, routers, and Internet Service Providers (ISPs) providing diverse connectivity paths and infrastructure. The AEGN routes processed Transactions and files through the Participant's IVPN to the Participant's host. The connection supports online transmittal of Authorization traffic, the transfer or Clearing and Settlement files, and electronic transfer of network-generated reports from the Network to Participants. AEGNS monitoring of an IVPN connection is limited to the portion of the connection that is hosted within the AEGN environment.

AEGNS recommends IVPN connections be utilized in the following situations:

- When faster speed-to-market is a priority
- To support testing and Certification
- In parallel during installation of the GLOBE
- As an additional option for back-up connectivity
- When investment to install and maintain the GLOBE is not feasible

IVPN connections cannot be used where local regulation does not allow IVPN connectivity or contractual Service Level Agreements (SLAs) exist.

11.5.2.1 Additional Requirements

When IVPN is used as a permanent solution to connect to the Network, two (2) IVPN connections via different Internet Service Providers (ISPs) must be configured to diverse AEGNS data centers to provide resilience.

The Participant will be solely responsible for the negotiation and management of the service arrangement for IVPN connectivity with the Internet Service Provider (ISP) of their choice, and associated costs.

During an IVPN outage, the Participant will provide technical support twenty-four (24) hours per day, seven (7) days per week to troubleshoot the outage in collaboration with AEGNS until the connection to the AEGN is restored.

11.6 Terminal Access

All terminal access connections between the AEGN and Participants must have a secure Telnet 3270 connection (TLS connection) utilizing an AEGNS-approved software configuration to encrypt data and passwords.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.7 Network Test Simulator

Network Test Simulator is a Web-based application accessed through Knowledge Base that simulates Network processing of Authorization and data collection messages.

There are two (2) types of Network Test Simulator:

- A "Certification model" enables Participants to complete 'Phase 1 unattended testing' (as described in the *Network Specifications - Instructions* manual) without the need for a direct connection to the Network.
- A "Certification model with Developer's functionality" provides an additional capability to the Participant to modify some variables of the simulation for the purposes of Participant system development.

AEGNS provides and maintains the Network Test Simulator and is the sole owner of the Network Test Simulator. AEGNS provides subscription for the use of the Network Test Simulator to Participants or Authorized Processors, as applicable, in accordance with:

- The provisions of this manual
- The Network Specifications manuals
- Other applicable AEGNS manuals
- A Network Test Simulator Cover Page which must be signed by AEGNS and the relevant Participant or Authorized Processor

11.7.1 Network Test Simulator Definitions

The definitions included in this section describe terms that are specific only to policies and requirements for the Network Test Simulator. Some terms may be duplicates of terms used in other chapters and sections of this manual and defined in the "Definitions" chapter beginning on page 495. However, the terms defined in this section that are not included in the "Definitions" chapter beginning on page 495 apply only to the text in Section 11.7, "Network Test Simulator," on page 424 of this chapter, and the definitions are not to be applied to terms or text in any other chapter or section of this manual.

Table 11-2. Network Test Simulator Definitions

Payment Date	The day each month under Section 6.4.1.1, "Daily Activity Process," on page 273 (or its successor provision) on which Participant is required to settle with AEGNS for recurring fees (such as fees for the Network Test Simulator), which currently is the 26th of each month, or any other day designated and duly notified by AEGNS to Participant.
Service	The Network Test Simulator, together with any technical documentation supporting the Network Test Simulator, as well as new releases and updates to the Network Test Simulator, as available, along with any updates to the technical documentation which correspond to such updates and new releases.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11.7.2 Requirements

Participants must follow these requirements to be in compliance with the terms of Service.

11.7.2.1 Access to Service and Use

1. AEGNS grants to Participant a royalty-free, non-transferable, non-exclusive license to use the Service. Participant may only use the Service for the purposes set out herein.
2. Participant must commence the access provisioning process for the Service by submitting a request through the support center on Knowledge Base or sending an email to NTS.Support@aexp.com.
3. AEGNS will arrange for Participant to receive installation and second level operational support if so requested by Participant, but shall have no liability for such support. Any support shall be specified in the Online Help section of the Service.
4. Participant shall not copy or create derivative works using the Service provided in whole or in part, for any purpose. Participant shall not alter, modify, enhance or adapt the Service or attempt to reverse engineer, convert, translate, decompile, disassemble or merge the Service with any other software or materials.
5. No license granted hereunder shall be construed to convey, transfer, affect, alter or otherwise modify any rights of AEGNS and, except for the limited license to use the Service as specified herein, Participant obtains no rights whatsoever in or to the Service.
6. Participant shall not remove, alter or obscure any copyright or other proprietary notices relating to the Service.

11.7.2.2 Fee

1. The fees for the Network Test Simulator are set out in Table 10-12, “Network Test Simulator Fees,” on page 407 and payable as set out therein. The total amount of fee payable by Participant will vary depending on the Participant's election of the Developer's Functionality model and the number of log-ins desired, and shall be set out on the Web-Based Test Simulator Cover Page signed by AEGNS and Participant.
2. AEGNS may change the Annual Fees applicable to any Service at any time upon ninety (90) days' written notice as long as any increase in fees is generally applicable to all users of the Web-Based Test Simulator.

11.7.3 General

1. If Participant becomes aware of any actual, alleged or threatened claim or action that the Service, in whole or in part, or Participant's use thereof, infringes the rights of any third party, Participant shall immediately notify AEGNS providing copies of any papers or documents related to such claim which are in Participant's possession.
2. Participant agrees to pay all taxes levied against or upon the Service or its use hereunder, exclusive, however, of taxes based on AEGNS' income, which taxes shall be paid by AEGNS. If any tax for which Participant is responsible hereunder is paid by AEGNS, Participant will reimburse AEGNS upon receipt of AEGNS' proof of payment.
3. AEGNS warrants that the Service will be provided in accordance with its Documentation in all material respects.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4. PARTICIPANT UNDERSTANDS AND AGREES THAT AEGNS IS PROVIDING THE SERVICE TO PARTICIPANT "AS IS" AND ON AN "AS AVAILABLE" BASIS AND MAKES NO WARRANTY THAT THE SERVICE WILL BE UNINTERRUPTED, TIMELY OR ERROR-FREE, AND EXPRESSLY DISCLAIMS ALL OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OR OF NON-INFRINGEMENT. PARTICIPANT IS SOLELY RESPONSIBLE FOR ADEQUATE SAFEGUARDS AND PROTECTIONS OF ITS EQUIPMENT, PROGRAMS, INFORMATION, AND DATA OR ANY OTHER MATERIALS AND/OR INFORMATION THAT MAY BE AFFECTED BY THE SERVICE.
5. In no event shall: (i) either AEGNS or Participant be liable hereunder for indirect, special, incidental, punitive, speculative or consequential damages in connection with use of the Service, including, without limitation, damages resulting from loss of use, loss of data, loss of profits, loss of business or loss of goodwill, regardless of whether or not a party knows, has reason to know or has been advised of the possibility of such damages; or (ii) AEGNS be liable for direct damages in an amount greater than the fees payable by Participant to AEGNS for the Service.
6. Participant shall indemnify and hold AEGNS harmless from and against any and all liabilities, losses, costs, damages and expenses associated with any claim or action arising from: (i) Participant's (or its Authorized Processor's) unauthorized use of the Service or results from alterations, modifications or enhancements to the Service made without AEGNS' express written consent; (ii) Participant's (or its Authorized Processor's) use of the Service in combination with other equipment, software, materials, or data; or (iii) third-party claims arising out of breach of the terms set out in Section 11.7, "Network Test Simulator," on page 424. This provision will survive termination of the Participant's use of the Service.
7. AEGNS shall indemnify and hold Participant harmless from and against any and all liabilities, losses, costs, damages and expenses associated with any third-party claim or action arising from any actual infringement of a third party's patent, copyright or intellectual or industrial property right or any similar right (including, but not limited to, misappropriation of trade secrets) arising out of Participant's use of the Service in accordance with its Documentation.
8. If Participant's use of the Service is or is likely to be enjoined, AEGNS, in its discretion, may provide a non-infringing substitute, modify the Service to render it non-infringing, obtain a license for Participant to continue to use the Service or terminate Participant's use of the Service. The foregoing, as well as Section 11.7.2, "Requirements," on page 425 above, provides Participant's sole remedy for any claims of infringement or misappropriation. This provision will survive termination of the Participant's use of the Service.

11.7.4 Termination and Return of Materials

1. The terms set out in Section 11.7, "Network Test Simulator," on page 424 shall become effective on the Effective Date noted on the Network Test Simulator Cover Page, and continue thereafter until the termination of the Participant's use of the Services or the Participant Agreement.
2. Within ten (10) days following the termination of the Participant's use of the Service or the Participant Agreement, Participant shall return all copies and/or other materials and information created by or supplied to Participant as a result of the Participant's use of the Service. An officer of Participant shall certify compliance with the foregoing, in writing within ten (10) days of such termination.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

12 Exhibits

Exhibit 1. AEGNS Internet Marketing Communications Policies and Guidelines (IO/JV)

Independent Operator/Joint Venture Card Issuing Participants

Introduction

This section sets out policies of Global Network Services unit of American Express for publishing American Express-branded communications on the Internet and all interactive channels, which must be adhered to by all Global Network Services (GNS) Participants who operate the American Express Card Issuing Business as Independent Operators (IOs) or as part of a Joint Venture (JV), owned in part by an American Express Entity. Such IOs and JVs are referred to as "Participants" in this section.

Participants' American Express-branded Web pages that communicate information about American Express products and/or services ("Participant Site"), and all materials that mention such Participant Site, must meet certain criteria relating to legal requirements and disclosures, design, content, hyperlinking, security, and privacy. The Participant Site must be approved by GNS prior to publishing (launching) and before hyperlinks may be established to and/or from americanexpress.com. GNS reserves the right to shut down, or require the Participant to shut down, any non-compliant Participant Site within a period of 24 hours of GNS notifying the Participant that the site is non-compliant. GNS will not approve relaunch of the site until the site has been brought into compliance with American Express policies.

Questions regarding these Internet Policies and/or requests for Participant Site review and approval should be directed to your GNS Business Development Leader (BDL) who will interface with GNS Global Marketing.

Definitions

- Country Homepage (CHP) - The highest level page, in the American Express "look and feel," from which all other American Express product and service Web pages in the market can be accessed. The CHP is usually the first page that a user reaches when visiting an official American Express website in a market. American Express owns the CHP.
- Participant Site - Those Web pages built and/or hosted by the Participant (or third-party agency designated by the Participant) that contain American Express branding and describe American Express-branded products and services available to customers of the Participant.

Participant Site Disclosures and Legal Footers

The Participant's Legal Footer must be in local language and made accessible to visitors of the Participant Site via a hyperlink at the bottom of each and every website page. GNS provides Participants with a Legal Footer template for their site. This template must be modified in accordance with applicable local laws, and in accordance with actual Participant policies and practices. The document (titled Legal Footer Template) is located in the Marketing section of www.amexglobalnetwork.com/knowledgebase.

Note: The order should be as follows: (1) Website Rules and Regulations, (2) Trademarks, (3) Privacy Statement, and (4) About the Company.

- **Website Rules and Regulations**
  Participant Site content must comply with American Express Participants Website Rules and Regulations, as they may be amended by American Express from time to time, and which must be translated into and posted in local language(s).
- **Trademarks**
  Participant Site must list trademarks and service marks of American Express that have been licensed to the Participant.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Privacy Statement**
  A privacy statement/policy issued by the Participant must be posted on the Participant Site in local language(s) and must be kept updated to reflect changes in American Express' Privacy Principles and changes in the Participant Site.
- **About the Company (Participant as a Licensee of American Express GNS)**
  Participant Site must make clear that the Participant is a licensee of Global Network Services unit of American Express and issues American Express-branded Cards pursuant to agreement with GNS.

  Legal Alert Interstitial When Exiting Participant Site
  A Legal Alert message must be presented upon a visitor's exit from Participant Site and at any exit points to third-party sites. Following are two (2) possible scenarios and GNS' recommendations for the message (daughter windows are suggested).

  - **Upon visitor's exit from Participant Site to third-party site**
    "Please note that you are leaving <Participant name> American Express website, and the specific Rules & Regulations, Privacy Statement, and Corporate Entity Disclosures displayed on the site you are leaving are not applicable when linking to a third-party site."
  - **Upon visitor's exit from Participant Site to Participant's institutional site**
    "Please note that you are leaving <Participant name> American Express website and the specific Rules & Regulations, Privacy Statement, and Corporate Entity Disclosures displayed on the site you are leaving are not applicable when linking to <Participant name> institutional site."

Site Design

- **Look and Feel**
  The Participant Site must replicate the look and feel and experience standards of American Express-branded websites. To that end, Participants and/or their designated interactive agency must use American Express-issued design templates and follow GNS requirements to develop their site. The materials necessary to develop the Participant Site can be accessed through Knowledge Base (www.amexglobalnetwork.com/knowledgebase), or via other resources, about which GNS may notify Participants from time to time.

  As American Express-issued design templates are updated by GNS, the Participant Site will be required to reflect those changes. Participants will be given a reasonable amount of time to implement these changes and these changes are subject to review and approval by GNS.

  Participants and their third-party representatives/contractors (e.g., interactive agency) must cooperate closely with GNS during the Web development process. It will be each Participant's responsibility to ensure third-party compliance with the confidentiality obligations set out in the Independent Operator Agreement. Participants must require that third parties be bound by confidentiality standards equivalent to the obligations of the Participant.
- **Graphic Elements**
  Visual representation of an American Express-branded Card requires a photographic version. Line-art is not permissible. The American Express Card logo is not to be incorporated into drawings, cartoons or artistic depictions, unless provided by American Express. The Centurion figure is never to be used as a graphic device. Participants may, subject to GNS approval, include a Participant logo in conjunction with the "American Express" Blue Box logo in designated sections on the Participant Site. This logo must be consistent in relative size and position with use of Participant logos on card plastic.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Content**
  The Participant Site content, including all text and graphics, must be consistent with GNS interactive guidelines, and may not contain inappropriate language, imagery, or sounds. As with all American Express-branded communications, material published on the Participant Site must be characterized by high standards of good taste. While what constitutes good taste changes over time and varies by market, the test of good taste must be applied in good faith, and shall be subject to the discretion of GNS. Such decisions will be made without regard for what other Web publishers consider acceptable.

  Under no circumstances may the Participant Site contain, or link to, information that communicates in whole or in part, an analyst's report, news report, opinion, evaluation, or projection about American Express Company or its subsidiaries or affiliates or of the securities of American Express Company or its subsidiaries or affiliates, without prior written approval from GNS.

  Participants alone are responsible for ensuring all of the Participant Site content complies with any and all rules, regulations and/or laws in each country of the Territory in which they are located and in which they are providing products and/or services. American Express disclaims all liability and/or responsibility for legal compliance relative to any Participant Site content.
- **Maintenance and Post-Launch Engagement**
  Any marketing pages within the Participant Site must be submitted to GNS for review, and kept up to date at all times. If American Express notifies a Participant of incorrect or out of date information, the Participant must make the required changes within five (5) Business Days.

  It is highly recommended that Participants create and maintain one (1) website page for each Card product. Additionally, if a Participant's institutional site does not contain at least one (1) page per Card product, the Participant must direct traffic to the Participant's Site instead.
- **Language**
  All publicly accessible Web content, including the Participant's Legal Footer and disclaimers, must be published in the language(s) that is/are commonly used on similar professional/financial services websites in the Participant market. (In most instances, this will be the local language.)
- **Country Home Pages**
  GNS owns, and has the right to build and host, all Country Homepages (CHPs). GNS may, at its discretion, authorize Participants to build and host CHPs pursuant to a license agreement to be executed between GNS and such Participant(s) under certain circumstances, for example, when the Participant can demonstrate a compelling business need or when hosting of the CHP by AEGNS is not allowed under local law. In such instances, Participants are required to follow GNS interactive guidelines regarding CHPs and must make changes requested by GNS to said pages within forty-eight (48) hours. At its discretion, GNS may begin hosting CHPs previously hosted by the Participant. Participant Sites, as well as other third-party sites, approved by GNS may be linked to the CHP at the discretion of GNS.

  Use of a URL containing the name “American Express” is non-exclusive to any specific Participant. Participants utilizing the CHP may be required, at the sole discretion of GNS, to share the use of the CHP with other Participants or with American Express entities that do business in the relevant market.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **URLs, Domain Names and Email Address**
  Registering Uniform Resource Locators (URLs) and domain names that are associated in any manner with American Express or American Express Entities (e.g., americanexpress.be for Belgium) is expressly the sole province of American Express and American Express Entities. American Express reserves the sole right to grant use of the URLs and domain names containing the name "American Express" or "AMEX." Participants may use such URLs or domain names only to the extent authorized pursuant to a licensing agreement between American Express between the Participants.

  Participants using or having registered a URL or domain name containing "American Express," "AMEX," or a variation of the American Express name or a URL likely to be assumed to be associated with American Express or an American Express Entity, shall promptly, upon request, assign all rights to such URL to American Express, or an American Express-designated entity. Participants must execute licensing agreements and cooperate and assist American Express with obtaining consents required to effectuate such assignment from relevant authorities in the country.
  American Express will, at its sole discretion, authorize the use of an appropriate URL in marketing and promotional materials.

  A Participant wishing to utilize a URL other than americanexpress.<country> that includes "American Express," "AMEX," or a variation of the American Express name that is likely to be associated with American Express or an American Express Entity must submit a written request to GNS for review and approval. GNS reserves the sole right to determine the suitability of the proposed URL and if GNS deems appropriate, an American Express Entity will register such URL for said Participant's marketing and promotional materials.

  For the avoidance of doubt and customer confusion, Participants are not authorized to use "American Express" or any derivation thereof as part of the "@" sign of a Participant's email address.

Design Approvals

Before a Participant Site may be launched, the site must by reviewed and approved by GNS for compliance with American Express requirements (see also "Security Approvals," in this section). Participants should engage GNS Global Marketing early in their Web development process to help avoid delay in launch.

Prior to public launch and/or hyperlinking to/from americanexpress.<country>, Participants must publish their proposed Web content on a secure, non-publicly available platform, in accordance with GNS requirements, for GNS review and approval.

Following GNS approval, a Participant shall not materially alter the Participant Site without approval from GNS. GNS has the right to inspect the Participant Site to assure compliance with policies. Upon GNS request, Participant agrees to promptly remedy any non-compliant aspects of the Participant Site, and make all requested changes prior to re-publication of those aspects.

Cost/Pricing

Participants shall be responsible for all costs in connection with establishing, maintaining, and updating their Participant Site, including all costs related to GNS policy compliance and security approvals. GNS may also provide Participants with Web services, tools, and support, the costs of which may be passed on to the Participant, and may be subject to change at any time. Changes to recurring charges shall be announced at least three (3) months ahead of pricing change(s) taking effect.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Security

- **General Policies**
  The Participant Site must be protected against unauthorized access, accidental or unauthorized modification, disclosure, or destruction, using American Express standards as referenced in the IPCR (Information Protection Contract Requirements) appropriate to the level and sensitivity of the information being processed, stored, or transmitted. GNS, or an agent authorized by GNS, shall at Participant 's expense determine via a Vulnerability and Threat Assessment ("VTA"), that the Participant Site, or an added functionality on the site, meets these standards (as outlined under Security Approvals, Encryption, Configuration Management, Security Patches and System Updates, Authorization, Verification, Logout, Firewall Standards, and Logging Standards sections in this policy) prior to providing the Participant with the approval necessary to launch the Participant Site or functionality.
- **Security Approvals**
  Before a Participant Site may be launched, GNS must review and approve the site for compliance with American Express security requirements. During the development phase of a new Participant Site, or the addition of functionality on the Participant Site, GNS has the right to request specific site information to ensure that any data associated with the Participant Site will be properly secured. Participant Site must pass a security review of their systems, as well as a VTA to be conducted by GNS or an approved third-party vendor within thirty (30) days of the Participant Site launch. The costs of the VTA and any expenses associated with ensuring site security and compliance will be the responsibility of the Participant. Any vulnerabilities must be repaired in accordance with the policies set forth under "Vulnerabilities/Penalties" section.

  A Participant shall not make any changes to the site's infrastructure or functionality without obtaining additional GNS approval and VTA testing. Such reviews must be initiated prior to the planning and development of said changes to ensure that they comply with GNS security standards. Participants may be liable for charges for such reviews.

  GNS reserves the right to conduct periodic VTA reviews of Participant systems at any time, without notification, and at Participant expense. GNS approval does not constitute a guarantee that the Participant Site is secure against third-party intruder attempts. Each Participant is solely responsible, and bears all liability, for breaches of security on GNS-approved sites.
- **Encryption**
  An Encryption algorithm, approved by GNS, must be used to protect credit card numbers, telephone calling card numbers, login passwords, etc., as they traverse the network. These identifiers or parameters must not be sent over the Internet in clear text form. Encryption must be used for Web page Encryption. All confidential, proprietary, and secret data sent over open networks must be encrypted. See Section 2.4.8, "Encryption Data Security Requirements," on page 44 for details.

  All sensitive information (e.g., passwords, Account numbers, Tax ID numbers, etc.) stored on disk or in a database must be protected using approved cryptographic techniques.
- **Configuration Management**
  To accomplish proper configuration management, Internet connectivity network architecture must be completely documented and maintained including, but not limited to, all: hardware devices/components, firmware components, operating system and application software components, version/revision numbers of the above devices/components, physical and logical network addresses, and connecting circuit numbers.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Security Patches and Systems Updates
  All hardware and software systems that are used for the Participant Site must be regularly reviewed by the Participant. The Participant must determine whether any security updates, such as, for example, regular or continuing security patches intended to address vulnerability risks stemming from new technologies and other sources, meet the requirements set forth by GNS. Any security update must be evaluated, then applied and documented prior to implementation. If a GNS-issued update cannot be used, or an update does not meet American Express security/integrity requirements, the Participant must ensure that the necessary steps are undertaken to bring the update into compliance with GNS requirements. In the event that GNS discovers that any update has been implemented which is not in compliance with GNS requirements, GNS will notify the Participant of such non-compliance. GNS, at its discretion and in addition to any other remedies available to it, may require the Participant, at the Participant expense, to bring the update into compliance as soon as possible following the notice by GNS, but in no event later than seven (7) days from the notice.
- Authorization, Verification, and Logout
  Persons who have log-in access to secure areas of the Participant Site must have a User ID separate and unique from every other Person on the system. Participants must use industry-approved validation criteria to identify customers. Secure sessions must be either logged out by the user or must be timed out automatically. User access should be automatically denied after three (3) consecutive unsuccessful log-in attempts. Participants must promptly notify GNS upon the termination of access rights of any user, so that GNS can ensure that related User IDs are terminated.
- Firewall Standards
  All Participant Sites must be protected by firewalls and Intrusion Detection Systems (IDS), and all electronic communications of sensitive data (e.g., Cardmember Information) must occur only through American Express-approved gateways (e.g., TLS protocol). The system logs generated from the firewall(s) and IDS(s) must be reviewed on a continuing basis to detect any unauthorized entry attempts. Individual proxy accounts must be used on the firewall for "outbound" connections at all times. All non-essential networking or system services must be eliminated or removed from the firewall and disallowed by the firewall.
- Logging Standards
  American Express strongly encourages the best practice of logging/auditing events related to security, availability, and integrity of systems. Examples of such facilities are UNIX: syslog, process accounting, and auditing; NT: System, Security, and Application event logs; Web server access logs; and application-specific logs. Real-time replication of logs to a dedicated log-server is also strongly encouraged. Typical methods of log replication/consolidation include (but are not limited to) syslog, SNMP, and system management products.

  Each host system is responsible for logging any events of "priority" notice or higher. Logged information must include: a timestamp, facility or application, event, and result. The log format may follow the UNIX syslog format, or it may follow the Common Log format.

  Audit events may be generated by any number of system facilities, such as "kern," "mail," "auth," and others; and may pertain to any of a number of protocols, such as "HTTP" (hypertext transfer protocol), "FTP" (file transfer protocol), "SMTP" (simple mail transfer protocol), etc.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Passwords**
  Standard security protocols must be used with all IDs and passwords associated with Participant Site. Passwords must be protected on Participant computer systems using an approved Encryption algorithm and never displayed or stored in the clear. Access to encrypted password files must be prohibited. Passwords must not appear on the screen or in any logging file during the log-in process. The use of a cryptographically strong hash (with salt) is preferred to the use of symmetric Encryption of passwords.

  If passwords are sent to Cardmembers via printed mail, the user ID and password must be mailed separately. Passwords may only be sent to the Cardmember billing address. New or re-enabled User IDs must be assigned passwords that force the Cardmember to change the password after the first use. Passwords are required to be a minimum length of six (6) characters and contain at least one (1) alphabetic and at least one (1) numeric character. (Special characters such as $ and & are discouraged due to international variations.) It is strongly preferred that no arbitrary maximum length to a password be enforced.
- **Backup**
  In order to prevent interruption to service and to protect sensitive data, Participants must take appropriate steps to back up the Participant Site, related server data, Cardmember Information, transactional data, and other sensitive data. Back-up copies must comply with all security requirements that apply to Participant Sites.
- **Auditing**
  At any time and without additional notice, GNS reserves the right to conduct a complete audit and VTA of any Participant Site to ensure Participant Site compliance with applicable American Express policies and standards. The audits and VTAs will include network security assessments and may include physical, on-location assessments.
- **Vulnerabilities/Penalties**
  Participant Site security vulnerabilities, identified through GNS or third-party VTAs and/or other means, must be repaired by the Participant or the Participant's third-party vendor within a timeframe to be specified by GNS upon Participant notification. In addition, GNS may apply charges of up to $10,000 (USD) for every day the site is non-compliant, or may require that the Participant shut down the site entirely until such time that the site is compliant.
- **Hacking Incidents**
  In the event that a Participant Site has been defaced or security has been compromised, the Participant must notify GNS immediately, place the impacted pages "under repair," and shut down and segregate the affected areas of the site. Within forty-eight (48) hours of notification, GNS will conduct the necessary tests (see "Auditing") to determine the exact nature of the site vulnerabilities. The Participant may re-launch the site only after all vulnerabilities have been addressed and the Participant Site complies with all GNS security/integrity policies.

  If GNS notifies the Participant of the hacking incident(s) before the Participant has become aware of or notified GNS of the hacking incident(s), American Express will expect the impacted pages to be put "under repair" immediately, or the affected areas of the site shut down. Within forty-eight (48) hours of notification GNS will conduct the necessary tests (see "Auditing") to determine the exact nature of the site vulnerabilities. American Express will re-launch the site only after all vulnerabilities have been addressed and the Participant Site complies with all GNS security/integrity policies.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Marketing/Promotion

- **Site Promotion**
  In a market with one (1) Independent Operator, the Participant's marketing initiatives with American Express branding or general loyalty/usage objectives must direct customers to the American Express home page in their market via the top-level country-specific URL (e.g., www.americanexpress.be for Belgium). In a market with multiple Independent Operators, Participants must direct customers to the highest level URL that is exclusively used by the Participant.

  Participants' marketing initiatives with American Express product/service acquisition or specific loyalty/usage or product-specific branding objectives may drive customers directly to the page for the advertised initiative. All below-the-line advertising/direct marketing and print may drive traffic to deep pages using at most one (1) backslash (e.g., www.americanexpress.<country>/selects or www.americanexpress.<country>/blue. A maximum of twenty (20) characters may be used after the backslash. Words following the backslash should be intuitive to the customer (e.g., www.americanexpress.<country>/myaccount" can be used to promote "Check Your Account Details" instead of "www.americanexpress.com/acctviewapp.htm"). The use of URL redirects is recommended to help facilitate the use of intuitive keywords. The page that customers reach via URLs utilizing backslashes should include navigation links that allow access to the entire site.
- **Cross-Selling**
  The cross-sell area of a page are used to market targeted products and services to visitors. GNS reserves full rights to manage the cross-sell areas of the CHP and the Participant Site.

  Participants may implement cross-sell initiatives on the Participant Site only if they comply with GNS interactive guidelines, and if the products and services promoted via cross-sell do not violate policies regarding prohibited industries or sale of products and services related to the payment products of American Express competitors. Cross-sell messages from other American Express entities (e.g., Travel) must be allowed on the Participant Site as required by the Independent Operator Agreement or other agreement between GNS and the Participant. GNS reserves the right to require advance review and approval of all cross-sell messages planned for the Participant Site.
- **Establishing a Hyperlink**
  Participants may, subject to GNS approval, establish a hyperlink from the Participant Site to: (a) the American Express-owned CHPs, (b) online tools and services specifically provided by GNS for Participant use, (c) the Participant institution's main (corporate) homepage, and (d) third-party sites that meet American Express-approved Merchant/industry requirements, and offer benefits and services to Participant's Cardmembers. Participants wishing to establish other hyperlinks originating from the Participant Site must obtain written approval from GNS prior to linking.

  Links from the Participant Site to non-American Express-branded pages must open the non-American Express pages/sites in a separate browser window, and may not remove the visitor from the Participant Site. GNS reserves the right to review Participant links on an ongoing basis and to request: 1) the removal of any links it deems inappropriate or non-compliant; or 2) the addition of any links it deems appropriate. Upon notice from GNS, Participants must discontinue any inappropriate/non-compliant link(s) within three (3) Business Days. GNS may discontinue, at its own discretion, any americanexpress.com content or pages to which the Participant Site may be linked.

  Hyperlinks originating from American Express-owned pages may be established and be discontinued at any time at the sole discretion of GNS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Customer Service**
  The Participant Site should have a customer service hyperlink with "Contact Us"-type support and should include information about how Cardmembers or S/Es can contact their issuer or Acquirer (the Participant), such as an email address, mailing address, and/or phone number. Contact details for all generally available channels of support (e.g., telephone, mail) must be provided. Participant are strongly encouraged to provide customer service through all of these channels that is at least at the same level as customer service provided to Cardmembers/SEs through all other channels. Further, customer service should be consistent with GNS quality standards and with reasonable consumer/Merchant expectations of availability and speed in an Internet environment.

  Cardmembers and Merchants must be warned not to send sensitive personal or confidential information (e.g., Account numbers) through email unless a secure email protocol is used.

  GNS reserves the right to periodically audit support activity and require modifications as needed to maintain service levels that are appropriate for the American Express Brand and American Express Cardmembers and S/Es.

  In addition to the Contact Us link, it is also strongly recommended that the Participant Site include links for the Global Splash Page (Global Sites) and a site map on every page.
- **Email Communications**
  Participant must comply with all applicable sections of CAN-SPAM relevant to local laws and regulations. Email communications for American Express products and services may be sent to current Participant customers and potential prospects based on the following guidelines:

  a. **Approval**
     All email creative must be subject to GNS approval prior to sending.

  b. **Return information: "From" line phrase and return address format**
     The email "From" line should identify the Participant. The portion of the actual return address to the left of the "@" sign should be modified for each version of an email campaign, while the domain name to the right should always read "Participant/Affiliate Name" (e.g., Offer1234@participantbankname).

  c. **Format**
     Marketing Managers should create HTML and text (and possibly mobile phone/PDA) versions of the email message.

  d. **Length**
     Shorter email messages are generally more effective. Whenever possible, ensure that recipients do not need to scroll below the initial screen to see the primary offer. Use 800x600 resolution as a guideline. For newsletters, keep the total length under three (3) printed pages.

  e. **Subject line phrasing**
     While many email client software and Web-based services now display longer subject lines, as a rule of thumb, try to keep the subject line to 30 characters or less for maximum impact.

     Email may be used to supplement a direct mail campaign or can be incremental to marketing campaign in offline channels as long as the text has been modified in the email to ensure that the email message isn't merely replicating but complementing the other campaigns.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

f. **Information Handling**
Information must be classified based on the potential impact to the information owner and/or American Express as a result of unintended disclosure, corruption, or loss. The information owner must determine the information classification. For emails sent through a non-secure distribution channel, information classified as "sensitive" pursuant to the definitions below cannot be included anywhere in the body of the message.

American Express Data Classification Policy Definitions

Public (not sensitive) - Information that is intended for public consumption and distribution. The content or context of public information is not sensitive and requires no special security.

Internal (not sensitive) - Information that is used to support normal business operations, and is intended for use when conducting American Express-related business. Internal information is not defined as sensitive, although requires appropriate controls.

Restricted (sensitive) - Information that, if misused, could compromise American Express' competitive advantage, customer or employee privacy, or the legal or financial status of American Express. Restricted information is defined as sensitive, and requires appropriate controls. It is the default classification of Personally Identifiable Information (PII).

Secret (sensitive) - Information that, if misused, could seriously compromise American Express' competitive advantage, customer or employee privacy, or the legal or financial status of American Express.

g. **Branding/Trademarks**
Branded product and service names should stand out from the rest of the text. Use the appropriate ™, SM, and ® symbols the first time the trademarked name is mentioned. Use the © symbol for copyrighted material.

h. **Attachments**
Attachments are not permitted in email messages because of concerns about customer perception regarding security/virus issues.

i. **URL Links**
It is recommended that email messages have links to Web page(s), when applicable, for online fulfillment in order to maximize the interactive benefits of email.

j. **Opt-Out/Footer Language**
Participants should ensure appropriate opt-out disclosure. If the email message requires an additional disclosure in the footer, include the disclosure just in front of the opt-out language in the same paragraph.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

k. **Opt-In Requirements**
Participants may only send prospect email through Opt-In Email lists.

Examples of Opt-In Email Enrollment Practices	
Opt-In (Allowed)	**Opt-Out (Not Allowed)**
Unchecked box that users check to request third-party offers by email.	Prechecked box that users must uncheck if they do not want email with third-party offers.
Series of unchecked boxes that users select to indicate their preferences about the types of third-party offers they wish to receive. Users receive no email unless they check at least one (1) of these boxes.	Unchecked box that users must check if they do not want email offers.
Providing an email address to a service whose primary value proposition is to send subscribers offers from third parties (e.g., site that pays incentives for reading email offers).	Notification to registrants that by providing an email address, they will receive third-party email offers, if the site is not specifically positioned to the subscriber as a place to sign up for third-party offers (e.g., registering at American Express).

l. **Prospect Email**
All emails must include a link to a page at the Participant Site(s) that offers the Cardmember more information or fulfillment of advertised offers.

- **Cardmember Information**
Participants who capture information about visitors to the Participant Site must comply with any policy or statement issued by the Participant that represents how such information will be used. Participants are responsible for ensuring that information collection practices and statements are at all times in compliance with applicable laws.

  American Express reserves the right also to capture information about visitors to americanexpress.com who were redirected there from Participant Sites.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 2. AEGNS Internet Marketing Communications Policies and Guidelines (NCL)

Network Card Issuing Participants

Introduction

This section sets out policies of Global Network Services unit of American Express for publishing American Express-branded communications on the Internet and all interactive channels which must be adhered to by all Global Network Services ("GNS") Participants who operate the American Express Card Issuing Business and have a Network Card License ("NCL"). Such NCLs are referred to as "Participants" in this document.

Participants' Internet Pages that communicate information about American Express products or services, or that use American Express branding as defined in the Advertising, Marketing, and Public Relations chapters of the *Business and Operational Policies* ("BOP") manual and all materials that refer to such Internet Pages (collectively referred to as "Participant Page(s)"), must meet certain criteria relating to American Express branding, legal requirements and disclosures, content, hyperlinking, security and privacy. All Participant Page(s) content is subject, at GNS' option, to review and approval by GNS prior to being published, or, if already published, at any time.

This section addresses issues relating to American Express branding, content, and similar requirements. In addition, Participant Page(s) are subject to GNS review and approval regarding security and technical and operational issues. GNS reserves the right to reject the publication of any Participant Page(s) for any reason, including security, technical or operational concerns.

Questions regarding these Internet Marketing Communications Policies & Guidelines and/or requests for Participant Page(s) review or approval should be directed to the Participant's GNS Business Development Leader ("BDL").

Participant Disclosures

- **Website Rules and Regulations**
  Participants must create their own website rules and regulations posting them on and making them accessible to visitors of the Participant Page(s) via a hyperlink at the bottom of each and every website page. The Participant regulations must include sections 1, 2, 4 and 6 of the "American Express website Rules and Regulations" (at the end of this document). All other sections of the "American Express website Rules and Regulations" are encouraged to be used as a framework with which a Participant can develop their own guidelines. All regulations must be translated into and posted in local language.
- **Privacy Policy**
  In addition, any privacy policy issued by the Participant must be posted on the Participant Page(s) in local language(s). The Participant's Privacy Policy must be made accessible to visitors of the Participant Page(s) via a hyperlink at the bottom of each and every website page. The Participant's Privacy Policy must comply with applicable local laws and actual Participant practices.
- **Participant as a Licensee of American Express GNS**
  Participant Page must make clear that the Participant is a licensee of Global Network Services unit of American Express and issues American Express-branded Cards pursuant to agreement with GNS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Site Design

- **Look and Feel**
  Participants agree to develop their Participant Page(s) so that the Page(s) are not substantially similar to americanexpress.com in "look and feel" and are not likely to create confusion as to the origin of the page(s).
- **Graphic Elements**
  Visual representation of the Participant-issued [Participant Name] American Express-branded Card requires a photographic version of the Card artwork. Line-art is not permissible. All American Express logos are not to be incorporated into drawings, cartoons or artistic depiction, unless provided by American Express.

  The Centurion figure and filigree are never to be used as a graphic device.
- **Content**
  Participant Page(s) content including all text and graphics, must be consistent with the Marketing section on Knowledge Base and the *Business and Operational Policies* manual. It may not contain inappropriate language, imagery, or sounds. As with all American Express-branded communications, material published on the Participant Page(s) must be characterized by high standards of good taste. While what constitutes good taste changes over time and varies by market, the test of good taste must be applied in good faith, and shall be subject to the discretion of GNS. Such decisions will be made without regard for what other Web publishers consider acceptable.

  Under no circumstances may the Participant Page(s) contain, or link to, information that communicates in whole or in part, an analyst's report, news report, opinion, evaluation, or projection about American Express Company or its subsidiaries or affiliates or of the securities of American Express Company or its subsidiaries or affiliates, without prior written approval from GNS.

  Participants alone are responsible for ensuring all of the Participant Page(s) content complies with any and all rules, regulations and/or laws in the country or countries in which they are located and in which they are providing products and/or services. American Express disclaims all liability and/or responsibility for legal compliance relative to any Participant Page(s) content.
- **Maintenance and Post-Launch Engagement**
  Any marketing pages within the Participant Site must be submitted to GNS for review, and kept up to date at all times. If American Express notifies a Participant of incorrect or out of date information, the Participant must make the required changes within five (5) Business Days.

  It is highly recommended that Participants create and maintain one (1) website page for each Card product.
- **Language**
  All publicly accessible Web content, including the Participant's Privacy Policy and Website Rules and Regulations, must be published in the language(s) that is/are commonly used on similar professional/financial services websites in the Participant market. (In most instances, this will be the local language.)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **URLs, Domain Names, and Email Address**
  Registering URLs and domain names that are associated in any manner with American Express or American Express Entities *is expressly the sole province of American Express and American Express Entities*. American Express reserves the sole right to grant use of the URLs and domain names containing the name "American Express" or "AMEX." Participants may be granted an exception to use such URLs or domain names only to the extent authorized pursuant to a licensing agreement between American Express and the Participants.

  Participants using or having registered a URL or domain name containing "American Express," "AMEX," or a variation of the American Express name, or a URL likely to be assumed to be associated with American Express or an American Express Entity, shall promptly, upon request, assign all rights to such URL to American Express, or an American Express-designated entity. Participants must execute licensing agreements and cooperate and assist American Express with obtaining consents required to effectuate such assignment from relevant authorities in the country.

  Hyperlinks originating from American Express-owned page(s) may be established and be discontinued at any time at the sole discretion of GNS.

  For the avoidance of doubt and customer confusion, Participants are not authorized to use "American Express" or any derivation thereof as part of the "@" sign of a Participant's email address.

Development and Approval Process

Participants must require that any agency they use for interactive development be contractually bound to keep all American Express information strictly confidential.

Participants must submit copy and layout specifications for any proposed Participant Page(s) for review and approval by GNS at GNS' option, prior to public launch. Following GNS approval, a Participant shall not alter the usage of American Express trademarks on such Participant Page(s) without approval from GNS.

GNS has the right to periodically visit Participants' sites to assure compliance with standards, guidelines and policies. Participants agree to promptly cease use or decommission non-compliant Participant Page(s) upon GNS request, and to make designated changes or corrections prior to re-publication of said Participant Page(s).

Cost/Pricing

Participants shall be responsible for all costs in connection with establishing, maintaining and updating their Participant Page(s), including all costs related to GNS policy compliance.

GNS may also provide Participants with Web services, tools and support, the costs of which may be passed on to the Participant, and may be subject to change at any time. Changes to recurring charges shall be announced at least three (3) months ahead of pricing change(s) taking effect.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Security

- **General Policies**
  The Participant Page must be protected against unauthorized access, accidental or unauthorized modification, disclosure, or destruction, using American Express standards as referenced in the IPCR (Information Protection Contract Requirements) appropriate to the level and sensitivity of the information being processed, stored, or transmitted.
- **Encryption**
  An Encryption algorithm, approved by GNS, must be used to protect credit card numbers, telephone calling card numbers, login passwords, etc., as they traverse the network. These identifiers or parameters must not be sent over the Internet in clear text form. Encryption must be used for Web page Encryption. All confidential, proprietary, and secret data sent over open networks must be encrypted. See Section 2.4.8, "Encryption Data Security Requirements," on page 44 for details.

  All sensitive information (e.g., passwords, Account numbers, Tax ID numbers, etc.) stored on disk or in a database must be protected using approved cryptographic techniques.
- **Configuration Management**
  To accomplish proper configuration management, Internet connectivity network architecture must be completely documented and maintained including, but not limited to, all: hardware devices/components, firmware components, operating system and application software components, version/revision numbers of the above devices/ components, physical and logical network addresses, and connecting circuit numbers.
- **Security Patches and Systems Updates**
  All hardware and software systems that are used for the Participant Page must be regularly reviewed by the Participant. The Participant must determine whether any security updates, such as, for example, regular or continuing security patches intended to address vulnerability risks stemming from new technologies and other sources, meet the requirements set forth by GNS. Any security update must be evaluated, then applied and documented prior to implementation. If a GNS-issued update cannot be used, or an update does not meet American Express security/integrity requirements, the Participant must ensure that the necessary steps are undertaken to bring the update into compliance with GNS requirements. In the event that GNS discovers that any update has been implemented which is not in compliance with GNS requirements, GNS will notify the Participant of such non-compliance. GNS, at its discretion and in addition to any other remedies available to it, may require the Participant, at the Participant expense, to bring the update into compliance as soon as possible following the notice by GNS, but in no event later than seven (7) days from the notice.
- **Authorization, Verification, and Logout**
  Persons who have log-in access to secure areas of the Participant Page must have a User ID separate and unique from every other Person on the system. Participants must use industry-approved validation criteria to identify customers. Secure sessions must be either logged out by the user or must be timed out automatically. User access should be automatically denied after three (3) consecutive unsuccessful log-in attempts. Participants must promptly notify GNS upon the termination of access rights of any user, so that GNS can ensure that related User IDs are terminated.
- **Firewall Standards**
  All Participant Pages must be protected by firewalls and Intrusion Detection Systems (IDS), and all electronic communications of sensitive data (e.g., Cardmember Information) must occur only through American Express-approved gateways (e.g., TLS protocol). The system logs generated from the firewall(s) and IDS(s) must be reviewed on a continuing basis to detect any unauthorized entry attempts. Individual proxy accounts must be used on the firewall for "outbound" connections at all times. All non-essential networking or system services must be eliminated or removed from the firewall and disallowed by the firewall.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Logging Standards
  American Express strongly encourages the best practice of logging/auditing events related to security, availability, and integrity of systems. Examples of such facilities are UNIX: syslog, process accounting, and auditing; NT: System, Security, and Application event logs; Web server access logs; and application-specific logs. Real-time replication of logs to a dedicated log-server is also strongly encouraged. Typical methods of log replication/consolidation include (but are not limited to) syslog, SNMP, and system management products.

  Each host system is responsible for logging any events of "priority" notice or higher. Logged information must include: a timestamp, facility or application, event, and result. The log format may follow the UNIX syslog format, or it may follow the Common Log format.

  Audit events may be generated by any number of system facilities, such as "kern," "mail," "auth," and others; and may pertain to any of a number of protocols, such as "HTTP" (hypertext transfer protocol), "FTP" (file transfer protocol), "SMTP" (simple mail transfer protocol), etc.
- Passwords
  Standard security protocols must be used with all IDs and passwords associated with Participant Page. Passwords must be protected on Participant computer systems using an approved Encryption algorithm and never displayed or stored in the clear. Access to encrypted password files must be prohibited. Passwords must not appear on the screen or in any logging file during the log-in process. The use of a cryptographically strong hash (with salt) is preferred to the use of symmetric Encryption of passwords.

  If passwords are sent to Cardmembers via printed mail, the user ID and password must be mailed separately. Passwords may only be sent to the Cardmember billing address. New or re-enabled User IDs must be assigned passwords that force the Cardmember to change the password after the first use. Passwords are required to be a minimum length of six (6) characters and contain at least one (1) alphabetic and at least one (1) numeric character. (Special characters such as $ and & are discouraged due to international variations.) It is strongly preferred that no arbitrary maximum length to a password be enforced.
- Backup
  In order to prevent interruption to service and to protect sensitive data, Participants must take appropriate steps to back up the Participant Page, related server data, Cardmember Information, transactional data, and other sensitive data. Back-up copies must comply with all security requirements that apply to Participant Pages.
- Auditing
  At any time and without additional notice, GNS reserves the right to conduct a complete audit and VTA of any Participant Page to ensure Participant Page compliance with applicable American Express policies and standards. The audits and VTAs will include network security assessments and may include physical, on-location assessments.
- Vulnerabilities/Penalties
  Participant Page security vulnerabilities, identified through GNS or third-party VTAs and/or other means, must be repaired by the Participant or the Participant's third-party vendor within a timeframe to be specified by GNS upon Participant notification. In addition, GNS may apply charges of up to $10,000 (USD) for every day the site is non-compliant, or may require that the Participant shut down the site entirely until such time that the site is compliant.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Hacking Incidents**
  In the event that a Participant Page has been defaced or security has been compromised, the Participant must notify GNS immediately, place the impacted pages "under repair," and shut down and segregate the affected areas of the site. Within forty-eight (48) hours of notification, GNS will conduct the necessary tests (see "Auditing") to determine the exact nature of the site vulnerabilities. The Participant may re-launch the site only after all vulnerabilities have been addressed and the Participant Page complies with all GNS security/integrity policies.

  If GNS notifies the Participant of the hacking incident(s) before the Participant has become aware of or notified GNS of the hacking incident(s), American Express will expect the impacted pages to be put "under repair" immediately, or the affected areas of the site shut down. Within forty-eight (48) hours of notification GNS will conduct the necessary tests (see "Auditing") to determine the exact nature of the site vulnerabilities. American Express will re-launch the site only after all vulnerabilities have been addressed and the Participant Page complies with all GNS security/integrity policies.

Marketing and Promotion

- **Acquisition, Loyalty, and Usage**
  Participants' marketing initiatives with American Express product/service acquisition or specific loyalty/usage or product-specific branding objectives may drive visitors directly to the page for the advertised initiative.
- **Cross-Selling**
  The cross-sell area of a page is used to market targeted products and services to visitors. Participants may implement cross-sell initiatives on the Participant Page(s) containing products only if the products and services promoted via cross-sell do not violate policies regarding prohibited industries. GNS reserves the right to require advance review and approval on the basis of policy compliance of all cross-sell messages planned for the Participant Page(s).
- **Establishing a Hyperlink**
  Participants may, subject to GNS approval, establish a hyperlink from Participant Page(s) to: (a) the American Express-owned websites, (b) online tools and services specifically provided by GNS for Participant use, (c) Participant institution's main (corporate) homepage, and (d) third-party websites that meet American Express-approved Merchant/industry requirements, and offer benefits and services to Participant's Cardmembers.

  Participants wishing to establish hyperlinks originating from the Participant Page(s) may be subject to approval from GNS prior to linking.

  Hyperlinks from the Participant Page(s) to non-American Express-branded Page(s) must open the non-American Express Page(s)/sites in a separate browser window, and may not remove the visitor from the Participant Page(s). GNS reserves the right to review Participant hyperlinks on an ongoing basis and to request: 1) the removal of any hyperlinks it deems inappropriate or non-compliant or 2) the addition of any hyperlinks it deems appropriate. Upon notice from GNS, Participants must discontinue any inappropriate/non-compliant hyperlink(s) within three (3) Business Days.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- **Customer Service**
  Participant Page(s) should have a customer service hyperlink with "Contact Us"-type support. It should include information about how Cardmembers can contact the Participant, such as an email address, mailing address, and/or phone number. Contact details for all generally available channels of support (e.g., telephone, mail) must be provided.

  Participants are strongly encouraged to provide customer service through all of these channels that is at least at the same level as customer service provided to Cardmembers through all other channels. Further, customer service should be consistent with GNS quality standards and with reasonable consumer/Merchant expectations of availability and speed in an Internet environment.

  Cardmembers must be warned not to send sensitive personal or confidential information (e.g., Account numbers) through email unless a secure email protocol is used.

  GNS reserves the right to periodically audit support activity and require modifications as needed to maintain service levels that are appropriate for the American Express Brand.
- **Email Communications**
  Participant must comply with all applicable sections of CAN-SPAM relevant to country and local law. Email communications for American Express products and services may be sent to current Participant customers and potential prospects based on the following guidelines:

  a. **Approval**
  All email creative may be subject to GNS approval prior to sending.

  b. **Return Information: "From" Line Phrase and Return Address Format**
  The email "From" line should clearly identify the Participant (or Participant affiliate). The portion of the actual return address to the left of the "@" sign should be modified for each version of an email campaign, while the domain name to the right should always read "Participant/affiliate Name" (e.g., Offer1234@participantbankname).

  c. **Format**
  Marketing Managers should create HTML and text (and possibly mobile phone/PDA) versions of the email message.

  d. **Length**
  Shorter email messages are generally more effective. Whenever possible, ensure that recipients do not need to scroll below the initial screen to see the primary offer. Use 800x600 resolution as a guideline. For newsletters, keep the total length under three (3) printed page(s).

  e. **Subject Line Phrasing**
  While many email client software and Web-based services now display longer subject lines, as a rule of thumb, try to keep the subject line to 30 characters or less for maximum impact.

  Email may be used to supplement a direct mail campaign or can be incremental to marketing campaign in off-line channels as long as the text has been modified in the email to ensure that the email message isn't merely replicating but complementing the other campaigns.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

f. **Information Handling**
Information must be classified based on the potential impact to the information owner and/or American Express as a result of unintended disclosure, corruption, or loss. The information owner must determine the information classification. For emails sent through a non-secure distribution channel, information classified as "sensitive" pursuant to the definitions below cannot be included anywhere in the body of the message.

American Express Data Classification Policy Definitions

Public (not sensitive) - Information that is intended for public consumption and distribution. The content or context of public information is not sensitive and requires no special security.
Internal (not sensitive) - Information that is used to support normal business operations, and is intended for use when conducting American Express-related business. Internal information is not defined as sensitive, although requires appropriate controls.
Restricted (sensitive) - Information that, if misused, could compromise American Express' competitive advantage, customer or employee privacy, or the legal or financial status of American Express. Restricted information is defined as sensitive, and requires appropriate controls. It is the default classification of Personally Identifiable Information (PII).

Secret (sensitive) - Information that, if misused, could seriously compromise American Express' competitive advantage, customer or employee privacy, or the legal or financial status of American Express.

g. **Branding/Trademarks**
Branded product and service names should stand out from the rest of the text. Use the appropriate TM, SM, and ® symbols the first time the trademarked name is mentioned. Use the © symbol for copyrighted material.

Text emails should use approximations to those symbols: (TM), (SM), (R), and (C).

h. **Attachments**
Attachments are not permitted in email messages because of concerns about customer perception regarding security/virus issues.

i. **URL Links**
It is recommended that email messages should have links to Web page(s), when applicable, for online fulfillment in order to maximize the interactive benefits of email.

j. **Opt-Out/Footer Language**
Participants should ensure appropriate opt-out disclosure. If the email message requires an additional disclosure in the footer, include the disclosure just in front of the opt-out language in the same paragraph.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

k. **Opt-In Requirements**
Participants may only send prospect email through Opt-In Email lists.

Recognizing Opt-In Email on Third-Party Sites	
Opt-In	**Opt-Out**
Unchecked box that users check to request third-party offers by email.	Pre-checked box that users must uncheck if they do not want email with third-party offers.
Series of unchecked boxes that users select to indicate their preferences about the types of third-party offers they wish to receive. Users receive no email unless they check at least one (1) of these boxes.	Unchecked box that users must check if they do not want email offers.
Providing an email address to a service whose primary value proposition is to send subscribers offers from third parties (e.g., site that pays incentives for reading email offers).	Notification to registrants that by providing an email address, they will receive third-party email offers, if the site is not specifically positioned to the subscriber as a place to sign up for third-party offers.

l. **Prospect Email**
All emails must include a link to a page at the Participant Page(s) that offers the Cardmember more information or fulfillment of advertised offers.

- **Cardmember Information**
Participants who capture information about visitors to the Participant Page(s) must comply with any policy or statement issued by the Participant that represents how such information will be used. Participants are responsible for ensuring that information collection practices and statements are at all times in compliance with applicable laws.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 3. Confidentiality Letter

Dear Mr/s. :

This letter is being prepared in connection with your request to review the Card Issuer Agreement executed between (Issuer's Name) and American Express and related material and information (the "Card Issuer Agreement").

In order to cooperate with the request and to protect American Express and (Issuer's Name) interests, we require that your (company/firm) preserve as confidential all information of American Express and (Issuer's Name), and their respective parent, subsidiaries and affiliated companies which is obtained by any individual in your (company/firm) in any form in connection with your review of the Card Issuer Agreement. We also require that your (company/firm) agree to receive and maintain all information relating to the Card Issuer Agreement in trust and confidence and not, without first obtaining our prior written consent, disclose to any Person, firm or enterprise, or use for its own benefit or the benefit of others, any such information except for the purpose for which we have commissioned your services and is required by law.

Your acceptance of copies of the Card Issuer Agreement will constitute your agreement to the confidentiality requirements as set forth above.

Yours sincerely,

By:

Name:

Title:

Rev. BPR1099

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 4. Guaranty Agreement

GUARANTY dated as of [DATE_____, 20____] between [_____] organized and existing under the laws of _____ (the "Guarantor"), and American Express Limited, a corporation organized and existing under the laws of the State of Delaware, U.S.A. _____("American Express"). _____ ("LICENSEE") and American Express are parties to a Card Issuer Agreement dated as of [DATE ____, 20__], as modified and supplemented and in effect from time to time (the "Agreement"), providing, subject to the terms and conditions thereof, for certain payments to be made, and obligations to be performed, by LICENSEE to American Express.

To induce American Express to enter into the Agreement and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Guarantor has agreed to guarantee the Guaranteed Obligations (as hereinafter defined). Accordingly, the parties hereto agree as follows:

1. The Guarantor, as primary obligor and not merely as surety, hereby guarantees American Express the prompt payment in full of all of the indebtedness and other monetary liabilities and obligations of LICENSEE due or owing to, or in favor of or for the benefit of American Express or any American Express Entity (as defined in the Agreement) under the Agreement including, without limitation, amounts owed to American Express under the Agreement (the "Guaranteed Obligations") when and as due (whether at maturity, by reason of acceleration or otherwise), strictly in accordance with their respective terms. The Guarantor hereby further agrees that if LICENSEE shall fail to pay in full when due (whether at maturity, by reason of acceleration or otherwise) any and all of the Guaranteed Obligations, the Guarantor will promptly pay the same, without any demand or notice whatsoever, and that in the case of any extension of time of payment or renewal of any of the Guaranteed Obligations, the same will be promptly paid in full when due (whether at extended maturity, by reason of acceleration or otherwise) in accordance with the terms of such extension or renewal.
2. All payments by the Guarantor hereunder of the Guaranteed Obligations shall be made (a) to American Express at American Express' office at 200 Vesey Street, New York, New York 10285 on the due date thereof, in United States Dollars, in funds immediately available to American Express, or (b) if American Express so specifies in writing to the Guarantor, at the time and place and in the manner and type of funds specified in the Agreement. All payments due American Express hereunder, and all of the other terms, conditions, covenants and agreements to be observed or performed by the Guarantor hereunder, in each case whether in respect of the Guaranteed Obligations or otherwise, shall be made by the Guarantor without any reduction whatsoever including, but not limited to, any reduction for any setoff, recoupment, counterclaim (whether, in any case, in respect of any obligations owed by American Express to the Guarantor, LICENSEE or any other guarantor and, in the case of a counterclaim, whether sounding in tort, contract or otherwise) or tax.
3. The Guarantor's obligations hereunder are absolute and unconditional, present and continuing, unlimited and general, irrevocable, irrespective of the value, genuineness, validity, regularity or enforceability of the Agreement or any other agreement or instrument referred to herein or therein, or any substitution, release or exchange of any other guaranty of or collateral security for any of the Guaranteed Obligations, and to the fullest extent permitted by applicable law, irrespective of any other circumstances whatsoever that might otherwise constitute a legal or equitable discharge or defense of a surety or guarantor, it being the intent of this Section 3 that the obligations of the Guarantor hereunder shall be absolute and unconditional under any and all circumstances.
4. The obligations of the Guarantor hereunder shall not be reduced, limited or terminated, nor shall the Guarantor be discharged from any thereof, for any reason whatsoever (other than the indefeasible payment in full of the Guaranteed Obligations), including without limitation, any act or failure to act which (a) varies the risk of the Guarantor hereunder or (b) but for the provisions hereof, would, as a matter of statute or rule of law or equity, operate to reduce, limit or terminate the obligations of the Guarantor hereunder.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

5. The Guarantor hereby waives: (a) notice of acceptance of and intention to rely on this Guaranty Agreement and notice of the incurrence or renewal of the Guaranteed Obligations; (b) presentment, protest, demand for payment and notice of dishonor; (c) notice of any other nature whatsoever whether or not required by statute, rule or law; (d) any requirement that American Express take any action whatsoever (including demand for payment and legal action) with respect to any other Person or entity, including LICENSEE or any other guarantor, or any collateral for any of the Guaranteed Obligations; and (e) any and all other defenses, whether arising under any statute or at law or in equity, that would, but for this clause (e), be available to the Guarantor as a defense against or reduction of any or all of its liabilities and obligations hereunder. The Guarantor hereby agrees that until the payment and satisfaction in full of all Guaranteed Obligations, it shall not exercise any right or remedy arising by reason of any performance by it of Guaranteed Obligations hereunder, whether by subrogation or otherwise, against LICENSEE or any other guarantor of any of the Guaranteed Obligations or any collateral security for any of the Guaranteed Obligations.
6. The Guarantor agrees that American Express may, without notice to, or further consent of, the Guarantor and without in any way affecting the liability of the Guarantor hereunder: (a) renew, extend, modify, release or transfer the Guaranteed Obligations, the Agreement, any other guaranty of the Guaranteed Obligations and any rights under any of them or provided by law; and (b) exercise or refrain from exercising any right of American Express under the Agreement, any collateral security document, any other guaranty, or provided by law.
7. If, as a result of any LICENSEE bankruptcy, dissolution, reorganization, intervention, receivership, arrangement or liquidation (or proceedings similar in purpose or effect), or if for any other reason, any payment received by American Express in respect of the Guaranteed Obligations is rescinded or must be returned by American Express, the Guaranty Agreement shall continue to be effective as if such payment had not been made and, in any event, until the Guaranteed Obligations have been fully paid. In the event that any or all of the Guaranteed Obligations shall, in whole or in part, be or be determined to be or become, whether by operation of any present or future law or by order of any court or governmental agency, disallowed, invalid, illegal, void or unenforceable, such Guaranteed Obligations shall, for purposes of this Guaranty Agreement, nonetheless be deemed (a) to continue to be outstanding and in full force and effect and (b) if such is not already the case, to have become due and payable on the date of such disallowance, invalidity, illegality, voidness or unenforceability.
8. The Guarantor represents and warrants that (a) it is a [_____ / CORPORATION] duly organized, validly existing and in good standing under the laws of [PLACE OF INCORPORATION], (b) it has the power, and has taken all necessary action to authorize it, to execute, deliver and perform in accordance with its terms this Guaranty Agreement, and (c) this Guaranty Agreement has been duly executed and delivered by the Guarantor and is a legal, valid and binding obligation of the Guarantor, enforceable against the Guarantor in accordance with its terms.
9. The Guarantor hereby irrevocably: (a) submits in any legal proceeding arising out of, connected with, or relating to, this Guaranty Agreement to the exclusive jurisdiction of any court of competent jurisdiction sitting in the City and State of New York and agrees to suit being brought in such courts, as American Express may elect; (b) waives any objection that it may now or hereafter have to the venue of such proceeding in any such court or that such proceeding was brought in an inconvenient court; and (c) agrees to service of process in any legal proceeding by any means authorized by law. THE GUARANTOR AND AMERICAN EXPRESS HEREBY WAIVE TRIAL BY JURY IN ANY JUDICIAL PROCEEDING TO WHICH THEY ARE BOTH PARTIES INVOLVING ANY CLAIM RELATED TO THIS GUARANTY AGREEMENT OR THE AGREEMENT.
10. No action or omission by American Express shall constitute a waiver of any of the rights or remedies of American Express hereunder. Such rights and remedies are cumulative and not exclusive of any rights and remedies provided by law. This Guaranty Agreement shall not be modified except by a written instrument signed by the Guarantor and American Express.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

11. This Guaranty Agreement shall be binding upon the Guarantor and its successors and permitted assigns, and shall inure to the benefit of American Express and its successors, transferees, and assigns. American Express may assign any or all of the Guaranteed Obligations, and its rights and obligations under the Agreement and the transferee shall have the same rights hereunder with respect thereto as American Express. None of the rights and obligations of the Guarantor hereunder may be assigned or otherwise transferred without the prior written consent of American Express.
12. Any notice, designation, request, demand or the like hereunder may be given to the Guarantor or to American Express at their respective addresses set forth below or at such other address as may hereafter be specified in a notice designated as a notice of change of address. If to American Express at: GNS Risk Management, 200 Vesey Street, New York, NY 10285, U.S.A. If to the Guarantor, at: [ADDRESS]. Any request or demand or the like hereunder shall be in writing and shall be effective (i) on the date personally delivered to the party to which sent, (ii) on the date transmitted by a facsimile transmission, (iii) one (1) Business Day after delivery to an overnight courier service for overnight delivery or (iv) three (3) Business Days after mailing by first-class mail.
13. This Guaranty Agreement shall be a contract under, and be governed by, and construed and interpreted in accordance with, the laws of the State of New York without regard to conflicts of law principles.
14. Any provision of this Guaranty Agreement which is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof in that jurisdiction or affecting the validity or enforceability of such provision in any other jurisdiction.

    IN WITNESS WHEREOF, the parties hereto have caused this Guaranty Agreement to be executed by their duly authorized officers all as of the day and year first written above.

[NAME OF GUARANTOR]		[AMERICAN EXPRESS]	
By:		By:	
Name:		Name:	
Title:		Title:	

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 5. Secure Remote Commerce Terms and Conditions

Secure Remote Commerce (SRC) is an E-commerce checkout capability that creates a secure and consistent Cardmember checkout experience across digital channels, including Mobile Devices, web browsers, and other connected devices. Refer to Section 2.5.7, "Secure Remote Commerce," on page 70 for more information.

1. Definitions

Card Artwork	A photographic version of the visual representation of Participant's artistic designs present on the Card Image.
Card Image	A photographic version of the visual representation of the overall Participant-issued American Express-branded Card (excluding the American Express logo).
Digital Card	A digital representation of a payment Card used by an SRC System and/or Digital Card Facilitator, which may be hosted online or in a Cardmember device. A Digital Card contains data about the enrolled payment Card, and visually represents the PAN issued to the Cardmember.
Digital Card Facilitator	A role within the SRC ecosystem that provides a Cardmember with access to one or more Digital Cards and facilitates the checkout experience.
Digital Payment Application	A website or E-commerce application operated by an S/E or other Service Provider, where the Cardmember can complete the purchase of Goods or Services by participating in SRC.
Secure Remote Commerce (SRC)	An E-commerce checkout capability that creates a secure and consistent Cardmember checkout experience across digital channels, including Mobile Devices, websites, and other connected devices.
SRC Initiator	An SRC ecosystem role that supports checkout and/or the retrieval of Digital Card and payment data from the SRC System on behalf of a payment-enabled application.
SRC Participant	Any entity that is configured to participate in SRC. This can include entities playing the role of SRC Initiators, Digital Card Facilitators, Digital Payment Applications, or Issuers.
SRC System	A technical platform that facilitates E-commerce Transactions between Cardmembers, Digital Payment Applications, SRC Initiators, Issuers, and Digital Card Facilitators on behalf of one or more SRC programs.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2. Intellectual Property Rights Concerning Card Images and Card Artwork Associated with Secure Remote Commerce

Notwithstanding anything to the contrary in the Issuer's Participant Agreement or any existing Trademark License Agreement, by providing Issuer's Card Image(s), Issuer grants AEGNS a non-exclusive, non-transferable, non-assignable, royalty-free limited license to use Issuer's Card Image(s) and Card Artwork as provided in Section 2.5.7.3, "Issuer SRC Requirements," on page 71. Except as permitted herein, nothing in Section 2.5.7.3, "Issuer SRC Requirements," on page 71, conveys or restricts any interest in the intellectual property rights of Issuer or AEGNS. For the avoidance of doubt, both Issuer and AEGNS retain their rights with respect to any intellectual property, proprietary designations, patents, copyright registrations or trademark or service mark applications or registrations or such other protection as may be appropriate to the subject matter, and any extensions and renewals thereof.

3. Disclaimers

i. AEGNS makes no warranty or representation of any kind, express or implied, concerning SRC OBO Services or the operation or results of SRC.

ii. Issuers acknowledge that AEGNS' provision of SRC OBO Services does not constitute any assumption of fraud or other risk and that each Issuer is responsible for, and shall continue to bear, all the credit, fraud and other risks arising from Transactions conducted via SRC.

iii. In no event shall AEGNS be liable for direct damages in respect of the SRC OBO Services in an amount greater than the fees payable by the Issuer for such Services. In no event shall either party, its direct or indirect subsidiaries, controlled affiliates, agents, employees, or representatives be liable for any indirect, incidental, special, punitive, exemplary, or consequential damages of any kind, nor for lost profits or revenues, in connection with or arising out of AEGNS' provision of the SRC OBO Services.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 6. No Signature/No PIN Program Thresholds

The No Signature/No PIN Program allows an S/E to process a Transaction without obtaining an AEGNS-approved CVM if all of the requirements of the No Signature/No PIN Program are met, unless required by local law or regulation.

The content previously located in this section can be found in the No PIN Program and Expresspay Transaction Limits table in the *Live Terminal Parameters AEIPS & Expresspay Guide* available on Knowledge Base. Use the Knowledge Base Search function to locate the *Live Terminal Parameters AEIPS & Expresspay Guide*.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 7. European Economic Area Data Protection Model Contracts

Part A: Introduction

Explanatory Note

This Exhibit sets out the data protection provisions which shall apply to the transfer of or provision of access to Personal Data collected by a Participant established in the EEA (for example, information which relates to Cardmembers resident in Europe) to an American Express Entity established outside the EEA. The AEGN is operated by American Express Entities based outside of the EEA. Therefore, every time a Participant in the EEA sends a Transaction to the AEGN, it is sending data outside of the EEA and must comply with European data protection law when sending this data. The American Express Entities receiving such data outside the EEA must also comply with European data protection law when handling the data received.

Each relevant American Express Entity and each EEA Participant shall comply with the provisions in this Exhibit in order to ensure adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals (whether these are Cardmembers, employees or other individuals). All EEA Participants shall comply with applicable national data protection legislation (which implements the Data Protection Directive), in addition to the terms of this Exhibit.

The European Commission has developed model contracts in order to enable organizations to implement the requirements of European data protection law in a standardized way when sending and receiving data outside the EEA. The model contracts are available in a range of European languages at www.europa.eu.

AEGNS is including the European Commission's Controller to Controller-II (C2C-II) EU Model Contract terms in this Exhibit 7 as part of the obligations between American Express and the relevant EEA Participant. In the model contract terms, the American Express Entities are referred to as "Data Importers" and the EEA Participant is referred to as the "Data Exporter."

In addition to complying with this Exhibit, if required by any Supervisory Authority, each EEA Participant must enter into a stand-alone C2C-II EU Model Contract with the relevant American Express Entity, in which the EEA Participant shall be designated the Data Exporter and the American Express Entity the Data Importer.

SSAE 16 Audit

Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SSAE 16 audit represents that a service organization has been through an in-depth audit of its control objectives and control activities, which often include controls over information technology and related processes.

Every year, AEGNS has a SSAE 16 audit investigation conducted by Pricewaterhouse Coopers (or an auditing firm of equivalent stature) to review the operating effectiveness of more than 10 control objectives, including those to ensure that (a) data transmissions through the AEGN are secure, (b) logical access to production programs and data is only granted to authorized individuals, and (c) physical access to the AEGN infrastructure is restricted to authorized individuals and that administrative and operational procedures are in place for protection of physical assets. AEGNS shall make available to any EEA Participant that requests it a copy of its most recent SSAE 16 audit report (entitled "American Express Global Network Services Transaction Processing: Report on Controls Placed on Operation and Tests of Operating Effectiveness"), which is prepared on an annual basis.

Each EEA Participant acknowledges and agrees that, except where it can demonstrate otherwise to the reasonable satisfaction of AEGNS, the provision of the SSAE 16 audit report shall be deemed to satisfy any requirement pursuant to Part B of Exhibit 7 of the *Business and Operational Policies* manual to permit any EEA Participant to review or audit (or appoint a third party to review or audit) the Data Importer's facilities, data files, or Documentation.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Definitions and Interpretation

The Definitions of the capitalized terms used in this Exhibit are included at the end of Part B.

Reference in this Exhibit to "Data Importer" in the singular shall include a reference to each of the Data Importers in the event that there is more than one, for example, both American Express together with American Express Limited acting as joint Controllers which are Data Importers.

If there is an inconsistency between any of the provisions of this Exhibit, the other sections of this *Business and Operational Policies* manual*,* and a Participant Agreement respectively, the provisions of this Exhibit shall prevail in preference to the other sections of this *Business and Operational Policies* manual*,* and such Participant Agreement.

In addition to the provisions in respect of data security set out in this Exhibit, each Participant shall continue to comply with all security-related provisions of this *Business and Operational Policies* manual, which are integral to ensuring overall compliance with this Exhibit.

PART B – C2C-II EU Model Contract terms

Clause 1

Obligations of the Data Exporter

The Data Exporter warrants and undertakes that;

1. The Personal Data have been collected, processed and transferred in accordance with the laws applicable to the Data Exporter.
2. It has used reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under the clauses of Part B of this Exhibit.
3. It will provide the Data Importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the Data Exporter is established.
4. It will respond to inquiries from Data Subjects and the Supervisory Authority concerning Processing of the Personal Data by the Data Importer, unless the Parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Responses will be made within a reasonable time.
5. It will make available, upon request, a copy of Part B of this Exhibit to Data Subjects who are third-party beneficiaries under clause 3 of Part B of this Exhibit, unless Part B of this Exhibit contains confidential information, in which case it may remove such information. Where information is removed, the Data Exporter shall inform Data Subjects in writing of the reason for removal and of their right to draw the removal to the attention of the Supervisory Authority. However, the Data Exporter shall abide by a decision of the Supervisory Authority regarding access to the full text of Part B of this Exhibit by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Data Exporter shall also provide a copy of Part B of this Exhibit to the Supervisory Authority where required.

Clause 2

Obligations of the Data Importer

The Data Importer warrants and undertakes that:

1. It will have in place appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

2. It will have in place procedures so that any third party it authorizes to have access to the Personal Data, including processors, will respect and maintain the confidentiality and security of the Personal Data. Any Person acting under the authority of the Data Importer, including a Processor, shall be obligated to Process the Personal Data only on instructions from the Data Importer. This provision does not apply to Persons authorized or required by law or regulation to have access to the Personal Data.
3. It has no reason to believe, at the time of agreeing to comply with Part B of this Exhibit, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under the clauses of Part B of this Exhibit, and it will inform the Data Exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.
4. It will Process the Personal Data for purposes described in Appendix 2 to Part B of this Exhibit, and has the legal authority to give the warranties and fulfill the undertakings set out in the clauses of Part B of this Exhibit.
5. It will identify to the Data Exporter a contact point within its organization authorized to respond to inquiries concerning Processing of the Personal Data, and will cooperate in good faith with the Data Exporter, the Data Subject and the Supervisory Authority concerning all such inquiries within a reasonable time. In case of legal dissolution of the Data Exporter, or if the Parties have so agreed, the Data Importer will assume responsibility for compliance with the provisions of clause 1(e) of Part B of this Exhibit.
6. At the request of the Data Exporter, it will provide the Data Exporter with evidence of financial resources sufficient to fulfill its responsibilities under clause 3 of Part B of this Exhibit (which may include insurance coverage).
7. Upon reasonable request of the Data Exporter, it will submit its data Processing facilities, data files and Documentation needed for Processing to reviewing, auditing and/or certifying by the Data Exporter (or any independent or impartial inspection agents or auditors, selected by the Data Exporter and not reasonably objected to by the Data Importer) to ascertain compliance with the warranties and undertakings in the clauses of Part B of this Exhibit, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or Supervisory Authority within the country of the Data Importer, which consent or approval the Data Importer will attempt to obtain in a timely fashion.
8. It will Process the Personal Data in accordance with the data Processing principles set forth in Appendix 1 to Part B of this Exhibit.
9. It will not disclose or transfer the Personal Data to a third-party Controller located outside the European Economic Area (EEA) unless it notifies the Data Exporter about the transfer and:
    a. The third-party Controller processes the Personal Data in accordance with a Commission decision finding that a third country provides adequate protection; or
    b. The third-party Controller also agrees to be bound by the clauses of Part B of this Exhibit or enters into another data transfer agreement approved by a competent Supervisory Authority in the EU; or
    c. Data Subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards; or
    d. With regard to onward transfers of Sensitive Data, Data Subjects have given their unambiguous consent to the onward transfer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Clause 3

Liability and Third-Party Rights

1. Each Party shall be liable to the other Party (or Parties) for damages it causes by any breach of the clauses of Part B of this Exhibit. Liability as between the Parties is limited to actual damage suffered. Punitive damages (i.e., damages intended to punish a Party for its outrageous conduct) are specifically excluded. Each Party shall be liable to Data Subjects for damages it causes by any breach of third-party rights under the clauses of Part B of this Exhibit. This does not affect the liability of the Data Exporter under its data protection law.
2. The Parties agree that a Data Subject shall have the right to enforce as a third-party beneficiary this clause and clauses 1(b), 1(d), 1(e), 2(a), 2(c), 2(d), 2(e), 2(h), 2(i), 3(a), 5, 6(d) and 7 of Part B of this Exhibit against the Data Importer or the Data Exporter, for their respective breach of their contractual obligations, with regard to his Personal Data, and accept jurisdiction for this purpose in the Data Exporter's country of establishment. In cases involving allegations of breach by the Data Importer, the Data Subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer; if the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one (1) month), the Data Subject may then enforce his rights against the Data Importer directly. A Data Subject is entitled to proceed directly against a Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under the clauses of Part B of this Exhibit (the Data Exporter shall have the burden to prove that it took reasonable efforts).
3. Each Party shall perform its obligations under the clauses of Part B of this Exhibit at its own cost.

Clause 4

Law Applicable to the Clauses

Notwithstanding anything to the contrary in this *Business and Operational Policies* manual or the Participant Agreement, the clauses in Part B of this Exhibit shall be governed by the law of the country in which the Data Exporter is established.

Clause 5

Resolution of Disputes with Data Subjects or the Supervisory Authority

1. In the event of a dispute or claim brought by a Data Subject or the Supervisory Authority concerning the Processing of the Personal Data against either or all of the Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
2. The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Supervisory Authority. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
3. Each Party shall abide by a decision of a competent court of the Data Exporter's country of establishment or of the Supervisory Authority which is final and against which no further appeal is possible.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Clause 6

Termination

1. In the event that the Data Importer is in breach of its obligations under the clauses of Part B of this Exhibit, then the Data Exporter may temporarily suspend the transfer of Personal Data to the Data Importer until the breach is repaired or the contract is terminated.
2. In the event that:
    a. The transfer of Personal Data to the Data Importer has been temporarily suspended by the Data Exporter for longer than one (1) month pursuant to paragraph (a);
    b. Compliance by the Data Importer with the clauses of Part B of this Exhibit would put it in breach of its legal or regulatory obligations in the country of import;
    c. The Data Importer is in substantial or persistent breach of any warranties or undertakings given by it under the clauses of Part B of this Exhibit;
    d. A final decision against which no further appeal is possible of a competent court of the Data Exporter's country of establishment or of the Supervisory Authority rules that there has been a breach of the clauses of Part B of this Exhibit by the Data Importer or the Data Exporter; or
    e. A petition is presented for the administration or winding up of the Data Importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs, then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate the clauses of Part B of this Exhibit, in which case the Supervisory Authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the Data Importer may also terminate the clauses of Part B of this Exhibit.
3. Either Party may terminate the clauses of Part B of this Exhibit if: (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the Data Importer; or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.
4. The Parties agree that the termination of the clauses of Part B of this Exhibit at any time, in any circumstances and for whatever reason (except for termination under clause 6(c) of Part B of this Exhibit) does not exempt them from the obligations and/or conditions under the clauses as regards the Processing of the Personal Data transferred.

Clause 7

Description of the Transfer

The details of the transfer and of the Personal Data are specified in Appendix 2 to Part B of this Exhibit. The Parties agree that Appendix 2 to Part B of this Exhibit may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause 1(e) of Part B of this Exhibit. The Parties may execute additional annexes to cover additional transfers, which will be submitted to the Supervisory Authority where required. Appendix 2 to Part B of this Exhibit may, in the alternative, be drafted to cover multiple transfers.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Appendix 1 to Part B of this Exhibit 7

Data Processing Principles

1. Purpose limitation: Personal Data may be processed and subsequently used or further communicated only for purposes described in Appendix 2 to Part B of this Exhibit or subsequently authorized by the Data Subject.
2. Data quality and proportionality: Personal Data must be accurate and, where necessary, kept up to date. The Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data Subjects must be provided with information necessary to ensure fair Processing (such as information about the purposes of Processing and about the transfer), unless such information has already been given by the Data Exporter.
4. Security and confidentiality: Technical and Organizational Security Measures must be taken by the Controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the Processing. Any Person acting under the authority of the Controller, including a Processor, must not Process the data except on instructions from the Controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, Data Subjects must, whether directly or via a third party, be provided with the personal information about them that an organization holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter. Provided that the Supervisory Authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organizations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the Data Subject. The sources of the Personal Data need not be identified when this is not possible by reasonable efforts, or where the rights of Persons other than the individual would be violated. Data Subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organization may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A Data Subject must also be able to object to the Processing of the Personal Data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the Data Importer, and the Data Subject may always challenge a refusal before the Supervisory Authority.
6. Sensitive Data: The Data Importer shall take such additional measures (e.g., relating to security) as are necessary to protect such Sensitive Data in accordance with its obligations under clause 2 of Part B of this Exhibit.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the Data Subject at any time to "opt-out" from having his data used for such purposes.
8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a Data Subject or significantly affects a Data Subject and which is based solely on automated Processing of Personal Data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Data Importer shall not make any automated decisions concerning Data Subjects, except when:

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

a. (i) Such decisions are made by the Data Importer in entering into or performing a contract with the Data Subject, and
(ii) The Data Subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the Parties making such decision or otherwise to make representations to the Parties; or

b. Where otherwise provided by the law of the Data Exporter.

Appendix 2 to Part B of this Exhibit 7

Description of the Transfer

Data Subjects

The Personal Data transferred concern the following categories of data subjects:

- If the Data Exporter is a Card Issuer, individuals who have applied and/or have been issued with a payment account ("**Cardholders**") by the Data Exporter, which account may be used (via the use of a plastic Card and/or any other means) to purchase Goods and Services at Merchants (see third paragraph of this section) affiliated to the American Express network (or any other payment network owned and/or operated by American Express), obtain cash from locations such as ATM's and/or to otherwise have access to ancillary services ("**Card Service**"); and/or
- If the Data Exporter is a Commercial Card Issuer, individuals and, if relevant, legal entities whose information is necessary for the Data Exporter to be able to process the account applications of corporate / business clients ("**Corporate Clients**") and for the operation and administration of such accounts as set out in the first paragraph of this section. For example, Corporate Clients and their respective company directors/owners, and individuals with responsibility for managing such accounts on behalf of the Corporate Client.

Purposes of the Transfer(s)

The transfer is made for the following purposes:

- Storage of data outside of the EEA with access to and control over this data (and its onward transfer) to enable the Data Importer and its affiliates to perform services to and on behalf of the Data Exporter related to the operation of the Card Service and the servicing, as applicable, of Cardholders and Corporate Clients (i.e., Transaction routing and processing, reconciliation and settlement, customer servicing, dispute and Chargeback handling, risk and fraud management, accounting, auditing, billing, reconciliation, and collection activities, reporting, marketing and advertising, statistical and analytical activities, legal compliance, etc).

Categories of Data

The Personal Data transferred concern the following categories of data (in each case only to the extent that a Data Subject can be identified, directly or indirectly, from those data and other data which are in the possession of, or is likely to come into the possession of, a Controller or Processor):

- Financial or other personal data relating to Cardholders, which is collected in connection with their application and/or use of Cards/accounts and other Card Service ancillary services, and which may include, depending on the service, the Cardholder's name, address, incorporation details, private contact details (including telephone number and email address), employment and income information, bank account details, etc.
- Financial or other personal data relating to Corporate Clients, which is collected in connection with their application and/or use of accounts (e.g., Corporate Client accounts) and other Card Service ancillary services, and which may include, depending on the service, the name, address, incorporation details, private contact details (including telephone number and email address), employment and income information, bank account details, etc.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

- Financial or other personal data relating to company directors/owners, and individuals with responsibility for managing payment accounts on behalf of Corporate Clients, which is collected in connection with their application and/or use of Cards/accounts and other Card Service ancillary services, and which may include, their name, address, date of birth, private contact details (including telephone number and email address), employment and/or other financial information, etc.

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

- The Data Exporter and its affiliates, and its and their respective staff, accountants, auditors, or counsel;
- The Data Importer and its affiliates and its and their respective staff, accountants, auditors, or counsel;
- Processors appointed by the Data Importer or its affiliates;
- Third-party providers of Goods and Services (e.g., Merchants); and
- In the case of Cardholders issued a Card under the account of a Corporate Client, to the Corporate Client and/or its affiliates and its and their processors.

Sensitive Data

The Personal Data transferred concern the following categories of sensitive data:

N/A

Data protection registration information of Data Exporter (where applicable)

To be provided to AEGNS upon request.

.....

.....

Additional Useful Information (storage limits and other relevant information)

No additional information.

Contact points for data protection inquiries

American Express Limited	American Express Travel Related Services Company, Inc.
General relationship contact or as notified from time to time	General relationship contact or as notified from time to time

Data Exporter

General relationship contact or as notified from time to time

.....

.....

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Definitions for Part B of Exhibit 7

Applicable EEA Data Protection Law	The legislation protecting the fundamental rights and freedoms of individuals and, in particular their right to privacy with respect to the Processing of Personal Data applicable to a Controller in the country in the European Economic Area (EEA) in which the Controller is established.
Controller	The natural or legal Person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data; where the purposes and means of Processing are determined by national or European Community laws or regulations, the Controller or the specific criteria for his nomination may be designated by national or European Community law. This may be a Participant or an American Express Entity, as the context requires.
C2C-II EU Model Contract	Standard contractual clauses, approved by the European Commission Decision 2004/87/EC, for use when Personal Data is transferred outside the EEA from Controller to another Controller.
Data Exporter	A Controller who transfers Personal Data outside the EEA. This will be the Participant transferring Personal Data to an American Express Entity.
Data Importer	The Controller who agrees to receive from the Data Exporter Personal Data in accordance with the terms of Exhibit 7 and who is not subject to a third party's system ensuring adequate protection within the meaning of Article 25(1) of the Data Protection Directive. This will be the relevant American Express Entity.
Data Protection Directive or Directive 95/46/EC	Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data.
Data Subject	An identified or identifiable natural Person, including without limitation Cardmembers and Supplementary Cardmembers of an EEA Participant; an identifiable Person is one (1) who can be identified, directly or indirectly, in particular by reference to an identification number or to one (1) or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.
EEA	The EEA comprising the member states of the European Union together with Iceland, Liechtenstein, and Norway.
EEA Participant	A Participant who is established in the EEA or who uses equipment in the EEA to process Personal Data, in each case for the purposes of the Applicable EEA Data Protection Law.
Parties	The Data Exporter and Data Importer(s) (the Data Importers being American Express and American Express Limited (or any other relevant American Express Entity), as applicable).
Personal Data	Any information, including without limitation any information included in Cardholder Data and Cardmember Information, relating to a Data Subject who can be identified, directly or indirectly, from that information and other information which is in the possession of, or is likely to come into the possession of, a Controller or Processor.
Process or Processing	Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.
Processor	A natural or legal Person, public authority, agency, or any other body which Processes Personal Data on behalf of the Controller.
Sensitive Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Supervisory Authority	The competent data protection authority in the territory in which the Data Exporter is established.
Technical and Organizational Security Measures	Those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing, including without limitation the technical and organizational security measures set out in the Data Security Policy.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 8. Single Charge and VIP Stand-In Parameter Table

Regular

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

VIP

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		[illegible]		100
08		100		100
09		100		100
10		[illegible]		100
98		[illegible]		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
[illegible]		100		100
[illegible]		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

BIN(s) | Table

MCC Type	Local Amount	Auth Resp	Outbound Amount	Auth Resp
01		100		100
02		100		100
03		100		100
04		100		100
05		100		100
06		100		100
07		100		100
08		100		100
09		100		100
10		100		100
98		100		100

Sample

For information regarding the use of the Stand-In Authorization Service and this form please see Section 5.8, "Stand-In Processes," on page 256.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Instructions for Single Charge and VIP Stand-In Parameter Table

The Single Charge and VIP Stand-In Parameter Table is used when Global Network Services Authorization System (GNSAS) provides Stand-In for an Issuer for a single Transaction. GNSAS will send an approval message to the Acquirer and an Advice notification to the Issuer if the Authorization Request amount is within the guidelines of the parameter table. If a single charge is over the amount, GNSAS will decline the request.

The VIP Stand-In Parameter Table is used when the Cardmember is listed on the Network Exception File as a VIP Cardmember.

To request a Stand-In for a scheduled outage, an Issuer must be certified to send a Network Management Request (1804) message and to receive a Network Management Response (1814) message. Refer to the *Network Specifications - Authorization* manual for more information.

How to Complete the Stand-In Form

Looking at the form from left to right, the Single Charge information is entered into the table in the left hand columns under the applicable Local or Outbound section.

For Cardmembers who are indicated as a VIP in the Exception File, the information is keyed into the right side of the form under the applicable Local or Outbound section.

Step	Action
1.	Type the 6-digit BIN (Bank Identification Number) or range of numbers identifying the Issuer Institution. List each BIN that will have unique Stand-In parameters.
2.	Assign a unique table number for each unique BIN. Issuers can use table numbers 01-90. These table numbers are forwarded to GNSAS in the Network Management Request (1804) message during a Stand-In. **Note:** Stand-In Table 99 is the default table containing Stand-In Authorization parameter values. It is also used for unscheduled Stand-In.
3.	Type the Merchant Type Code.
4.	Type the U.S. Dollar amount for a single charge. If a single charge is over the specified amount, GNSAS will decline the charge. **Note:** Cash Disbursements must have a zero ($0) dollar amount.

Field Name and Definitions

The following table defines the fields on the Single Charge and VIP Stand-In Parameter Tables form.

Field Name	Definition
BIN(s)	A number assigned by AEGNS to uniquely identify the Issuer of American Express Cards. The first six (6) bytes of the Cardmember's Primary Account number for their American Express Card are the Bank Identifier Number (BIN) for the Issuer. During the Participant Setup process, specific Card products can be differentiated using bytes 7 and 8 of this field.
Table	A unique table number assigned by the Issuer for each unique BIN.
Local/Outbound	The Local and Outbound sections indicate the set of Stand-In parameters to be used by GNSAS during Stand-In. A Transaction is considered local when the S/E is located within the home country of the Cardmember. A Transaction is considered outbound when the S/E is located outside of the home country of the Cardmember. AEGNS does not provide Stand-In for On-Us Transactions from Independent Operators.

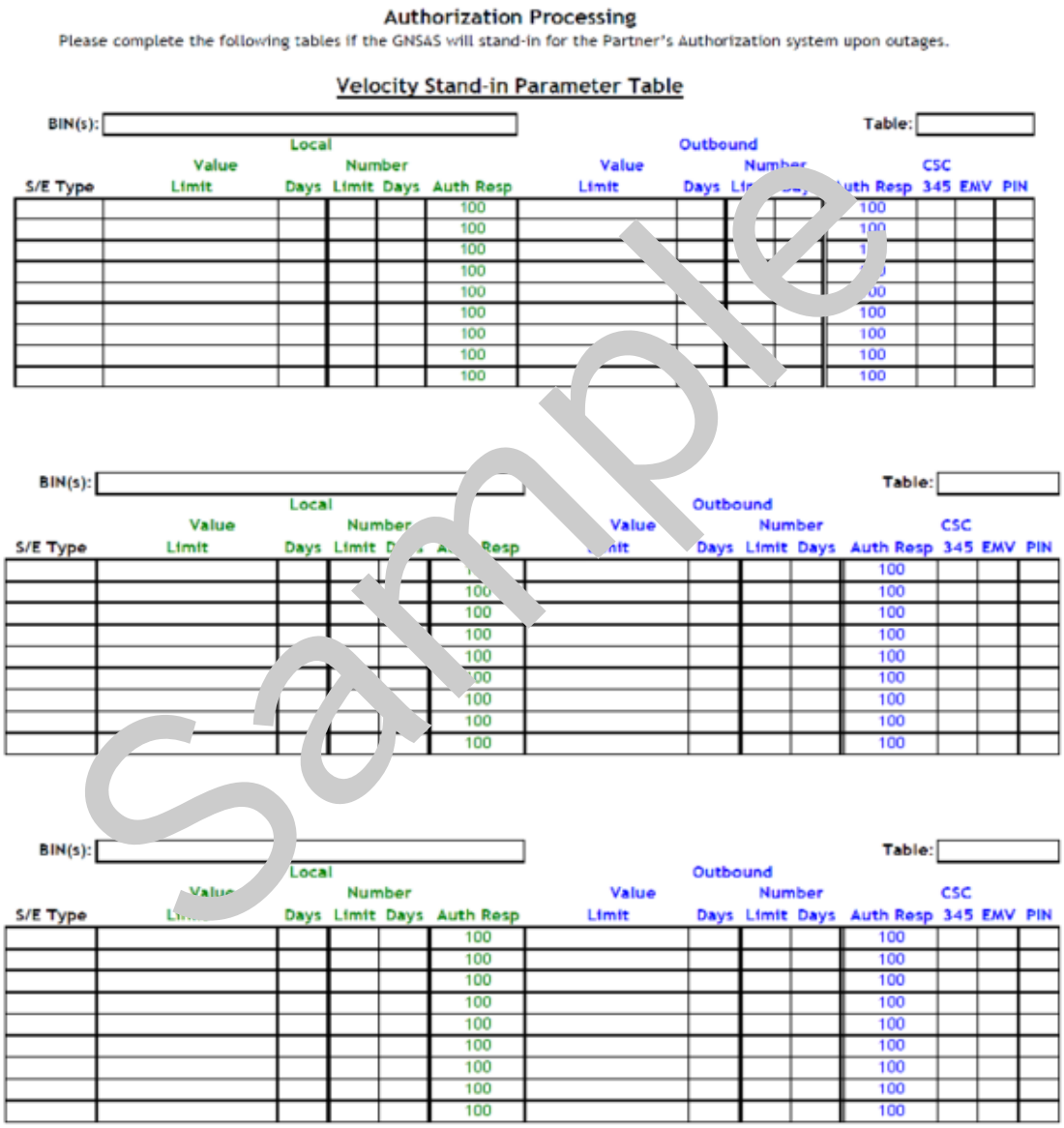
This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

<table>
<tr><th>Field Name</th><th>Definition</th></tr>
<tr><td>Merchant Type Code</td><td>Merchant Type Codes define a group of one (1) or more industry types based on Merchant Category Codes (MCCs).

<table><tr><th>Code</th><th>Description</th></tr><tr><td>01</td><td>Department Store/Retail/Mail Order</td></tr><tr><td>02</td><td>Travel</td></tr><tr><td>03</td><td>Auto/Boat Rental/Dealer</td></tr><tr><td>04</td><td>Restaurant</td></tr><tr><td>05</td><td>Oil & Gas</td></tr><tr><td>06</td><td>Lodging</td></tr><tr><td>07</td><td>Services</td></tr><tr><td>08</td><td>Air</td></tr><tr><td>09</td><td>Jewelry</td></tr><tr><td>10</td><td>Electronics</td></tr><tr><td>98</td><td>Cash Disbursement Provider</td></tr></table>
Refer to the *Codes Reference Guide* for a complete listing of Merchant Category Codes.</td></tr>
<tr><td>Amount</td><td>The U.S. Dollar amount for a single charge. If a single charge is over the specified amount, GNSAS will decline the charge.</td></tr>
</table>

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 9. Velocity-Based Stand-In Parameter Table



Authorization Processing

Please complete the following tables if the GNSAS will stand-in for the Partner's Authorization system upon outages.

Velocity Stand-in Parameter Table

BIN(s): Table:

	Local					Outbound						
	Value		Number			Value		Number		CSC		
S/E Type	Limit	Days	Limit	Days	Auth Resp	Limit	Days	Limit	Days	Auth Resp	345	EMV	PIN
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			

BIN(s): Table:

	Local					Outbound						
	Value		Number			Value		Number		CSC		
S/E Type	Limit	Days	Limit	Days	Auth Resp	Limit	Days	Limit	Days	Auth Resp	345	EMV	PIN
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			

BIN(s): Table:

	Local					Outbound						
	Value		Number			Value		Number		CSC		
S/E Type	Limit	Days	Limit	Days	Auth Resp	Limit	Days	Limit	Days	Auth Resp	345	EMV	PIN
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			
					100					100			

Sample

For information regarding the use of the Stand-In Authorization Service and this form please see Section 5.8, "Stand-In Processes," on page 256.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Instructions for Velocity-Based Stand-In Parameter Table

The Velocity-Based Charge Stand-In Table is used when GNSAS provides Stand-In for an Issuer on an accumulated amount basis and within a specific number of days. GNSAS will send an approval message to the Acquirer and an Advice notification to the Issuer if the Authorization Request is within the guidelines of the parameter table. If the request is outside of the guidelines, GNSAS will decline the request.

To request a Stand-In for a schedule outage, an Issuer must be certified to send a Network Management Request (1804) message and to receive a Network Management Response (1814) message. Refer to the *Network Specifications - Authorization* manual for more information.

How to Complete the Stand-In Form

The Velocity Stand-In Parameter Table form is used when the parameters have been set using an accumulated amount (vs. single Transaction amount) and incurred within a specified number of days.

Looking at the form from left to right, Local or Outbound sections are available.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1.</td><td>Type the 6-digit BIN (Bank Identification Number) or range of numbers identifying the Issuer Institution. List each BIN that will have unique Stand-In parameters.</td></tr>
<tr><td>2.</td><td>Assign a unique table number for each unique BIN. Issuers can use table numbers 01-90. These table numbers are forwarded to GNSAS in the Network Management Request (1804) message during a Stand-In.
Note: Stand-In Table 99 is the default table containing Stand-In Authorization parameter values. It is also used for unscheduled Stand-In.</td></tr>
<tr><td>3.</td><td>Type the S/E Type (Merchant Type Code). Each S/E Type must have an associated Stand-In amount as established by the Issuer, except for Merchant Type Codes 06, 07, 12, and 13, which must default to a Stand-In amount of zero ($0) dollars and decline.</td></tr>
</table>

Merchant Type Code	Velocity Codes Merchant Description	Velocity-Based Merchant Classification
01	Shop	A
02	Accommodations	B
03	Restaurant	C
04	Air/Rail/Telecommunications	D
05	Cash Disbursement Provider	E
06	Sight Draft	F
07	Check Cashing/Cash on Hand	G
08	Oil Company	H
09	Department Store	I
10	Mail Order	J
11	Car Rental	M
12	Universal	ABCDEFGHIJM
13	Cash Only	EFG
14	Retail Only	AIJ
15	Travel Related	BDM
16	Travel and Restaurant	BCDM
18	Shop and Department Stores	AI

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Step	Action
4.	Type the U.S. Dollar amount for each S/E Type (Merchant Type Code) Value Limit field. **Note:** Cash Disbursements must have a zero ($0) dollar amount.
5.	Type the number of days in which the allotted Value Limit is reset for velocity decisioning in the Value Days field.
6.	Type the accumulated number of Authorization Requests (regardless of the Transaction Amount) in the Number Limit field under which GNSAS is authorized to approve the Transaction.
7.	Type the number of days in the Number Days field to specify the time period during which a specific number of Charges (Number Limit) are allowed (velocity). For Outbound Charges, there are additional columns.
8.	Type "Y" for Yes or "N" for No to indicate if GNSAS should validate the 3-digit Card Security Code (3CSC) value.
9.	Type "Y" for Yes or "N" for No to indicate if GNSAS should validate the 4-digit Card Security Code (4CSC) value.
10.	GNSAS will always validate the 5-digit Card Security Code (5CSC), therefore the default is Yes.

The following table defines the fields on the Velocity-Based Charge Stand-In Parameter Tables form:

Field Name	Definition
BIN(s)	A number assigned by AEGNS to uniquely identify the Issuer of American Express Cards. The first six (6) bytes of the Cardmember's Primary Account number for their American Express Card are the Bank Identifier Number (BIN) for the Issuer. During the Participant Setup process, specific Card products can be differentiated using bytes 7 and 8 of this field.
Table	A unique table number assigned by the Issuer for each unique BIN.
Local/Outbound	The Local and Outbound sections indicate the set of Stand-In parameters to be used by GNSAS during Stand-In. A Transaction is considered local when the S/E is located within the home country of the Cardmember. A Transaction is considered outbound when the S/E is located outside of the home country of the Cardmember. AEGNS does not provide Stand-In for On-Us Transactions from Independent Operators. **Note:** The local vs. outbound indicator applies to the current Transaction only. This information is not retained on historical Transactions for the purpose of velocity-based stand-in. Both local and outbound Transaction requests contribute to all accumulated values.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Field Name	Definition
S/E Type (Merchant Type Code)	A parameter code that identifies the industry category of the Merchant (based on the MCC) where the Transaction took place. Merchant Types are used for velocity-based charge evaluation to support accumulation of all previous charge activity whether the Authorization was decisioned by the Issuer or in Stand-In. There are two (2) types of Merchant Type Codes; individual and grouped. **Individual (01-11)** A Merchant Type Code is used to define individual industry type Transactions. The value indicates the parameter to be used for a Transaction if it is in the allowable accumulated amount and incurred within a specified number of days. **Grouped (12-18)** A Merchant Type Grouped Code is used to consolidate multiple industry type Transactions. It assigns a set of parameters using one (1) code. The grouping is used to combine a number of industry types for the same value limit. The value indicates the parameter to be used for a Transaction if it is within the allowable accumulated amount and incurred within a specified number of days. The Merchant Type Grouped Code allows for value limits to be spread among a range of Merchant Types. For example, a value limit of $200 (USD) with a Merchant Type of 15 (Travel Related) will only allow $200 (USD) in spend for the combined three (3) Merchant Types represented in the grouping. There cannot be an individual and grouped Merchant Type Code on the form. **Note:** Each Merchant Type must be accounted for only once and without duplication for each Stand-In Table. For example, Merchant Type Codes 1 and 14 cannot appear in the same Stand-In Table since Merchant Type "A" Shop is included within each type code.
Value Limit	The accumulated Authorization Request amount (stated in U.S. Dollars) under which the GNSAS is authorized by the Issuer to approve the current Transaction. This value includes Authorizations decisioned by the Issuer and GNSAS in Stand-In for the time period.
Value Days	The number of days in which the allotted Value Limit is reset for velocity decisioning (Stand-In limit).
Number Limit	The accumulated number of Authorization Requests (regardless of Transaction Amount) under which GNSAS is authorized to approve the current Transaction. This value includes Authorizations decisioned by the Issuer and GNSAS in Stand-In for the time period.
Number Days	The number of days during which a specific number of Charges (Number limit) are allowed (velocity).
3CSC/4CSC (Optional)	Yes or No indication as to whether GNSAS should validate the Card Security Code (CSC) value.
5CSC (Mandatory)	Defaults to Yes as GNSAS always validates the CSC value.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Using the Value Limit, Value Days, Number Limit, and Number Days Field

- Use the Value Limit and Value Days fields to specify the maximum accumulated amount that GNSAS can authorize over a specified number of days. For example, if the Value Limit is $200 (USD) and the Value Days is 2, GNSAS can authorize Transactions up to $200 (USD) over a period of two (2) days.

  Example:

  Value Limit = $200

  Value Days = 2

- Use the Number Limit and Number Days fields to specify the maximum number of Transaction GNSAS is authorized to approve over a specified number of days. For example, if the Number limit is 5 and the Number Days is 3, the Network can authorize up to five (5) Transactions over a period of three (3) days.

  Example:

  Number Limit = 2

  Number Days = 4

$205 (USD) in Transactions during two (2) Stand-In days would be declined. Three (3) Transactions in four (4) days would be declined.

Note: For Transactions to be decisioned using the Velocity Parameter Stand-In Table, the Transaction would have already met the Single Charge Stand-In Table criteria.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 10. Benefit Participation Terms and Conditions

The Benefits Participation Terms and Conditions detail the relevant requirements, guidelines, restrictions, product and market eligibility, communication obligations, and terms and conditions that apply to Issuers when they extend American Express sourced benefits to Cardmembers. The Benefits Participation Terms and Conditions apply only to those benefits that are available at no additional cost to Cardmembers and Issuers.

1. Definitions

Benefit	A Card benefit provided by a Benefit Provider and offered by the Issuer to the Eligible Cardmembers, as set out in a Benefit Description Form.
Benefit Agreement	The agreement between a Benefit Provider and American Express, or an American Express Entity, pursuant to which a Benefit Provider agrees to provide a Benefit to Eligible Cardmembers.
Benefit Description Form	Any form governing a Benefit which details the terms and conditions that apply to such Benefit, as agreed between American Express and the Benefit Provider in the relevant Benefit Agreement.
Benefit Provider	Any company that provides a Benefit to the Eligible Cardmember, as set out in a Benefit Description Form.
Eligible Cardmembers	Cardmembers of the Issuer to whom the Benefit applies, as set out in a Benefit Description form.
Loyalty Program	Any loyalty program of a Benefit Provider pursuant to which Eligible Cardmembers are entitled to particular treatment and/or benefits, according to their status level in the loyalty program.
Marketing Assistance	Any marketing assistance which shall be provided by the Issuer in accordance with the Benefit Participation Terms and Conditions, and the Benefit Description Forms.
Platform	An electronic database or other digital platform as indicated by American Express where the Issuer can access and download the Benefit Description Forms for the available Benefits.

2. American Express Obligations

i. American Express shall facilitate access and notify the Issuer of the availability of certain Benefits in the Territory and shall provide the Issuer with the Benefit Description Form for each such Benefit. Notification of Benefits and distribution of Benefit Description Forms may take any of the following forms, as applicable and available at the time of notification: (a) letter or email from American Express to the Issuer with Benefit Description Form attached; (b) notice on the Platform of the introduction of a new Benefit with Benefit Description Form available for download; or (c) other ad hoc notification method that may be available permitting distribution of the relevant Benefit Description Form.

ii. American Express reserves the right to add or remove Benefits upon reasonable notice to the Issuer.

iii. American Express shall grant the Issuer access to the Platform, if applicable, for no more than two (2) authorized users, such authorized users to be indicated by the Issuer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

3. Issuer's Obligations

i. In consideration of American Express' facilitating and notifying the Issuer of each Benefit, the Issuer shall perform the various obligations of the Issuer as set out in the corresponding Benefit Description Form.

ii. A Benefit shall only be made available to the Eligible Cardmembers holding the Card types set out in a Benefit Description form, and the Issuer must offer the Benefit to all Eligible Cardmembers holding such Card types.

iii. The Issuer shall provide the Marketing Assistance set out in each Benefit Description Form, through the communication channels, and at the times set out in such Benefit Description Form. All Marketing Assistance is subject to approval by American Express and/or the Benefit Provider, as indicated in each Benefit Description Form and as detailed in Section 3.10, "Issuer Access to American Express Sourced Benefits," on page 213 of the *Business and Operational Policies* manual. The marketing material that is used in connection with the Marketing Assistance shall not mislead Cardmembers into believing that American Express, or any American Express Entity, is the issuer of the Card or the provider of any Good or Service being marketed by Issuer.

iv. The Marketing Assistance shall be provided by the Issuer at no charge to American Express or the Benefit Provider. The Issuer is responsible for the performance of and payment for all of the solicitation, advertising, marketing, mailing costs, and all other costs in connection with the communication, advertising, and delivery of the Benefit. The Issuer shall market the Benefit as benefits related to American Express Cards issued by the Issuer and not services or features incidental to or representative of any other non-American Express-branded Cards.

v. In the event a Benefit is available on the Platform, the Issuer shall comply with the terms and conditions of the Platform as indicated within such Platform. Furthermore, the Issuer agrees to name two (2) authorized users for the Platform and to indicate the same to American Express. Only such authorized users may access the Platform.

4. Loyalty Program

i. The Issuer shall implement and advise Eligible Cardmembers of the enrollment procedure, as indicated in the relevant Benefit Description Form. The Issuer acknowledges and agrees that such enrollment procedure may require Eligible Cardmembers and/or the Issuer to share information regarding such Eligible Cardmembers with American Express and/or a Benefit Provider for the purpose of completing enrollment in the Benefit Provider's Loyalty Program.

ii. The Issuer shall communicate to Eligible Cardmembers the Loyalty Program's terms and conditions and where they can be found.

iii. The Issuer acknowledges and agrees that once a Cardmember enrolls in a Loyalty Program, the Benefit Provider will be entitled to communicate with such enrolled Cardmember as it would any other enrollee of the Loyalty Program.

iv. The Issuer acknowledges and agrees that if a Cardmember fails to comply with the terms of a Loyalty Program or ceases to be an Eligible Cardmember, the Benefit Provider shall have the right to exclude the Cardmember from such Loyalty Program.

5. Notification of Complaints and Customer Service

The Issuer shall inform Eligible Cardmembers to direct any questions or complaints they may have with regard to any Benefit to the Issuer or the respective Benefit Provider and not to American Express or an American Express Entity. In order to maintain a high level of customer servicing, the Issuer and American Express shall inform the other, in writing, of any significant oral or written Cardmembers' complaints concerning a Benefit. In the case of complaints to the Issuer related solely to a Benefit provided by a Benefit Provider, the Issuer shall provide the Eligible Cardmember with the customer service contact details of the Benefit Provider as described in the relevant Benefit Description Form. The Issuer shall cooperate with the Benefit Providers, as reasonably necessary, to assist in handling complaints related to the provision of the Benefits.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6. Disclaimer and Relationship

i. American Express' role in relation to the Benefits is one of facilitation. American Express shall not be liable to the Issuer, and the Issuer shall have no recourse against American Express, for any costs, expenses, claims, losses or other damages incurred by the Issuer and arising in connection with a Benefit Provider failing to provide, or to adequately provide, a Benefit to Eligible Cardmembers or to the Issuer for the benefit of its Eligible Cardmembers, or to fulfill any obligations of Benefit Provider contemplated in the Benefit Agreement.

ii. Access to the Benefits is provided by American Express "as is" without warranty of any kind, either express or implied.

iii. In the conduct of the activities related to the Benefits, the Issuer shall be acting as its own principal and not as an agent of American Express.

7. Indemnification

The Issuer shall indemnify, defend, and hold American Express, American Express Entities and the Benefit Provider, their respective parents, subsidiaries, affiliates, successors and assigns harmless from all third-party claims, demands, actions, suits or proceedings, liabilities, losses, civil penalties, assessments, costs, damages and defense costs and fees assessed against American Express, American Express Entities and/or the Benefit Provider, their parents, subsidiaries, affiliates, successors or assigns arising out of the Issuer's performance (or lack of performance) of its obligations related to the Benefits including, but not limited to, the provision of the Marketing Assistance.

8. Third-Party Beneficiary Rights

i. The Issuer shall be entitled, under the principle of third-party rights, to seek appropriate remedies or enforce against Benefit Provider(s) the rights and benefits conferred upon the Issuer under the Benefit Agreement, and each Benefit Provider shall be entitled, under the principle of third-party rights, to seek appropriate remedies or enforce against the Issuer the rights and benefits conferred upon such Benefit Provider under the Benefit Agreement - in both cases as if such Benefit Agreement had been entered into by such Benefit Provider and the Issuer in the first instance.

ii. American Express shall provide to the Issuer a redacted copy of the relevant Benefit Agreement upon request from the Issuer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 11. AEGNS ATM Exception/First Presentment (DR) and Reversal (CR)

TO: _____

_____

_____

FROM: _____

_____

_____

Amount in U.S. Dollars: $ _____ Date of Adjustment: _____

USD FXCF: $ _____

We are issuing a * debit * credit adjustment for the following reason:

☐Transaction **NOT** settled to ATM Acquirer, but Cash dispensed to Cardmember. SUPPORT ATTACHED=> ☐

The ATM Acquirer must submit the request for this type of adjustment no later than thirty (30) days from the original Network Processing Date (ATM Transaction date).

☐Transaction settled to ATM Acquirer but Cash not dispensed

The ATM Acquirer may only submit the request for this type of adjustment between one hundred and five (105) and one hundred and thirty five (135)[1] days from the Network Processing Date. This is to allow for the Issuer Retrieval Request Notification within one hundred and five (105) days of the Presentment in order to avoid duplicate credit processing to the Cardmember via the disputes process and Exhibit 11.

For more information, refer to Section 7.3.3, "Disputes Process Transaction Life Cycle," on page 286 and the Network Specifications manuals.

continued on next page

1. This adjustment must be processed within thirty (30) days, starting on the 105th day from the Network Processing Date.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

☐See additional information below

Additional Information: _____

_____

_____

Cardmember Number: _____

Date and Time Dispense Took Place: _____

ATM Number and Network Name: _____

Sequence Number: _____

Requested/Dispensed Amount: _____

Issuer Currency Equivalent (including FX charges when applicable): _____

ATM Suspense Reference Number: _____

Reference Number: _____

Note: If the ATM Acquirer experienced a processing issue involving more than five (5) Transactions, it must provide all the relevant details via a spreadsheet (rather than multiple Exhibit 11 documents). Additionally, the ATM Acquirer must include the data elements indicated above, and clarify whether it is a debit/credit adjustment.

Approvals

	Originator	Approver	Level
Initial/Date			
Name: (Print)			

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ATM Exception First Presentment & Reversal Form

The ATM Exception First Presentment and Reversal Form is used to detail Cardmember and Transaction information for ATM Transactions that have failed to dispense any or all funds, or for supporting electronic Transactions that have not been presented to the ATM Financial Control Report for payment.

The ATM Exception First Presentment and Reversal Form includes Cardmember ATM details which are necessary to issue the appropriate debit or credit adjustment for ATM Transactions previously unsettled (e.g., Transaction NOT settled to ATM Acquirer, but Cash dispensed to Cardmember) or reversed (e.g., Transaction settled to ATM Acquirer, but Cash was not dispensed to Cardmember). This form is generated by the AEGN Acquirer and the net amount is included on the Daily Settlement Advisement as a separate line item. The single line item includes all relevant Transaction fees. The Daily Settlement Advisement Daily Settlement Advisement is supported by individual ATM Exception First Presentment and Reversal Forms for every Transaction.

Dispensed, but not Settled/Billed-In this instance, the Issuer has not been debited or has been debited incorrectly by the Network. Global ATM Disputes (GATM) will raise an ATM Exception/First Presentment and Reversal Form.

GATM can be contacted as follows:

Global ATM Disputes
Email: GlobalATMDisputes@AEXP.com

Table 12-1 ATM Exception First Presentment and Reversal Form Field Definitions

Column	Definition	Obtained From	Completed By
Amount U.S. Dollars	The amount of the dispense in U.S. Dollars.	Originator of the form	ACQUIRER
Date of Adjustment	Date the Adjustment is initiated.	Originator of the form	ACQUIRER
USD FXCF	Specifies the foreign exchange conversion fee (FXCF) in U.S. Dollars.	GATM	ACQUIRER
Additional Information	Free format text for any additional information provided.	Originator	ACQUIRER
Cardmember Number	Cardmember number	GATM Report	ACQUIRER
Date and Time Dispense Took Place	The date (day/month/year) and time of day the dispense took place.	GATM-EMEA Report	ACQUIRER
ATM Number and Network Name	ATM number and the name of the Network where the dispense took place.	GATM Report	ACQUIRER
Sequence Number	The sequence number of the ATM where the dispense took place.	GATM Report	ACQUIRER
Requested/Dispensed Amount	Amount dispensed or requested in the currency of the ATM.	GATM Report	ACQUIRER
Issuer Currency Equivalent	The dispensed amount or requested amount in the currency of the Issuer. This will have the FX factor added on if the dispensed amount was not in the currency of the Issuer.	GATM Report	ACQUIRER
ATM Suspense Reference Number	An internal AEGN reference number used for accounting purposes.	GATM Report	ACQUIRER
Reference Number	Specifies a unique number assigned to track the adjustment.	Assigned by GATM	ACQUIRER
Approvals	The name and level of AEGNS approvers.	Person(s) completing this section	ACQUIRER

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 12. AEGNS Card Recovery Award Form

To initiate a request for a Card Recovery Award, please complete this form and email it to the Card Issuer and copy gnsfraud@aexp.com. Please include "recovered Card" in the subject line of the email.

Acquirer Name: _____

Org ID: _____

Date Submitted: _____

Item	Card Issuer Name	Issuer Fraud/Security Contact Name for Lost/Stolen/Recovered Cards	Card Account Number	Card Recovery Date	S/E Name
1					
☐ $50: Pick Up request received from Issuer ☐ $100: Card recovered as a result of a Code 10 call ☐ Other (Provide Detail) ☐ $20: Handling Fee for returned Card Additional Information:_____					
2					
☐ $50: Pick Up request received from Issuer ☐ $100: Card recovered as a result of a Code 10 call ☐ Other (Provide Detail) ☐ $20: Handling Fee for returned Card Additional Information:_____					

TOTAL AMOUNT REQUESTED _____

FOR INTERNAL USE ONLY

Date: _____

The Card Recovery Award Advice Form is used by Network Acquirers to detail "Pick up Card" activity on behalf of Network Issuers. A submitted Card Recovery Award Form should only have recovered Card information for a single Issuer.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

For recovered Cards, the following amounts are awarded.

- A reward of $50 for Cards recovered after an S/E receives a "Pick up Card" response to an Authorization Request.
- A reward of $100 for Cards recovered after an S/E has been advised to recover the Card as a result of a Code 10.

Once the AEGNS Card Recovery Award Form is received by the AEGN, the net recovery amount will be included on the Daily Activity Report and/or Daily Settlement Advisement of respective Participants as part of miscellaneous ad hoc fees.

For Cards issued by American Express, American Express may choose to compensate Acquirers directly (e.g., check) - outside of the AEGNS settlement process.

Table 12-2 Card Recovery Award Claim/Recovery Advice Form Field Definitions

Column	Definition	Completed By
Card Issuer Name	Name of the Bank Issuer of the recovered Card	ACQUIRER
Issuer Fraud/Security Contact Name for Lost/Stolen/Recovered Cards	Name of the Issuer contact who approved the Card Recovery Award	ACQUIRER
Card Account Number	Card Account Number	ACQUIRER
Card Recovery Date	Date the Card was recovered by the S/E	ACQUIRER
S/E Name	Name of the S/E who recovered the Card	ACQUIRER

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 13. Reserved

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 14. AEGNS CDCRP Issuer Claim Form

A. Participant Information

Filing Date _____

Filing Network Issuer Name _____

Filing Network Participant IIN # _____

Issuer Contact Name _____ Title _____

Issuer Contact Phone _____ Email _____

B. Card Data Compromise Information

Issuer Notification Date _____

Compromise Reference Number _____

Compromise Event Window _____ through _____

C. Issuer Impact

Total Number of Unique Card Accounts compromised _____

Amount of Compensation Sought $ _____

D. Fraud Practices

Using the space provided, please describe your compliance to the fraud mitigation practices found in the "Security and Fraud" chapter beginning on page 375 of the *Business and Operational Policies* manual.

Note: Issuers filing a claim will need to provide AEGNS with the details of all fraudulent Transactions that occurred during the Compromise Event Window. This information should be provided using the 9324 Data Collection Message layout. When applicable, the On-Us transactional information will need to be provided using the appropriate file format.

On-Us file layout should summarize the following data elements at the Account level for each month of the Compromise Event Window:

- Transaction Count
- Amount

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 15. Dynamic Fraud Management Network Services Terms and Conditions

Dynamic Fraud Management Network Services (DFMNS) are available to all Issuers, as per Section 8.10.3.1, "Dynamic Fraud Management," on page 393.

1. Definitions

Dynamic Fraud Management Network Services (DFMNS)	A set of fraud Authorization tools that include a Fraud Probability Score and Recommendation Code assessed for each Eligible Transaction. The results of the evaluation (i.e., Eligible Transactions that have a higher fraud risk) are displayed to Issuers through WINTER and, for certified Issuers, through the Authorization message.
Eligible Transaction	All POS Transactions except: • Transactions occurring during system downtimes or outages that prevent AEGNS from providing an Issuer the DFMNS • On-Us Transactions
Fraud Probability Score	A 5-byte numeric value on an Eligible Transaction that indicates to the Issuer the probability of fraud.
Gross Fraud Rate	Total Gross Fraud reported to the Network over the Total Billed Business, excluding On-Us, ATM, and fees.
Issuer Override Request (IOR)	A feature available to Issuers through FraudNet that enables an Issuer to submit a request to suspend DFMNS decline Authorization Responses for specific Card Account Numbers during a period defined by the Issuer.
Recommendation Code	A 3-byte numeric value on an Eligible Transaction which corresponds to a description of the fraud risk associated with the Transaction. Refer to the *Codes Reference Guide* Fraud Indicator section for a complete list.
WINTER	A FraudNet application that allows Issuers to view Eligible Transaction details including Fraud Probability Score and Recommendation Code.

2. Provision of Dynamic Fraud Management Network Services

Each Issuer will receive Dynamic Fraud Management Network Services (DFMNS) as provided for in Section 8.10.3.1, "Dynamic Fraud Management," on page 393 and Section 8.10.3.1.3, "Dynamic Fraud Management Network Services Use," on page 394."

3. Reporting

AEGNS will provide Issuers with a list of Eligible Transactions that may have a higher fraud risk via WINTER, on a real-time basis.

4. Changes to Dynamic Fraud Management Network Services

Changes to the Dynamic Fraud Management Network Services (DFMNS), including to the method for calculating Fraud Probability Scores or to the Recommendation Code, may be made at the discretion of AEGNS in order to address changing fraud patterns in the Network. AEGNS will not implement any changes to DFMNS during the holiday freeze period, which generally occurs annually from late November through the end of December.

5. Intellectual Property Rights

AEGNS represents and warrants that DFMNS, and any components or derivatives thereof, are the sole and exclusive property of AEGNS. Unless otherwise expressly set forth in this Exhibit 15, neither AEGNS nor Issuer shall acquire, as a result of this Exhibit 15 and/or activities performed herein, any right or interest in intellectual property rights of the other party.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

6. Confidentiality

DFMNS and any components or derivatives thereof shall be deemed to be AEGNS Information for purposes of the Confidentiality section of the Participant Agreement. An Issuer may not use DFMNS for the benefit of any third party or for portfolios other than the Issuer's American Express® Card portfolio.

7. Disclaimers

i. AEGNS makes no warranty or representation of any kind, express or implied, concerning DFM Network Services or the results of DFMNS. AEGNS is not liable for any Eligible Transaction declined or not declined whether as a result of the operation of DFMNS or otherwise.

ii. Issuers acknowledge that AEGNS' provision of DFMNS does not constitute any assumption of fraud risk and that each Issuer is responsible for, and shall continue to bear, all the credit and fraud risks arising from Eligible Transactions.

iii. In no event shall AEGNS be liable for direct damages in respect of the DFMNS in an amount greater than the fees payable by the Issuer for such Services. In no event shall either party, its direct or indirect subsidiaries, controlled affiliates, agents, employees or representatives be liable for any indirect, incidental, special, punitive, exemplary, or consequential damages of any kind, nor for any lost profits or revenues, in connection with or arising out of AEGNS' provision of the DFMNS.

8. Indemnification

i. AEGNS shall indemnify an Issuer from intellectual property claims arising from such Issuer's use of DFMNS, provided that such use is in accordance with the terms of this Exhibit 15 (and any mutually agreed additions hereto), and that such claims do not arise as a result of the negligence of such Issuer.

ii. Each Issuer shall indemnify AEGNS from any claims arising from AEGNS' use of such Issuer's Information in connection with this Exhibit 15, provided that such use is in accordance with the terms of this Exhibit 15 (and any mutually agreed additions or deletions hereto), and that such claims do not arise as a result of the negligence or misconduct of AEGNS.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 16. Reserved

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 17. Floor Limit Table

Table 12-3 Floor Limits–Alphabetical Order by Country (All Countries)

Country	Currency Code	Hotel	Travel	Car Rental	Restaurant	Retail	Petrol	Internet
Australia	AUD	1000	750	250	300	200	200	0
Japan	JPY	300000	150000	50000	30000	30000	50000	0
New Zealand	NZD	1000	1000	500	500	300	150	0
All others (markets not listed)	USD	0	0	0	0	0	0	0

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 18. AEGNS Good Faith Form

A. Participant Information

Filing Network Participant Name: _____

Filing Network Participant IIN/AIN#: _____

Receiving Network Participant Name: _____

Receiving Network Participant BIN (IIN/AIN)#: _____

Cardmember Account Number: _____

S/E Number: _____

B. Transaction Information

Good Faith Transaction will be:

Debited to: Issuer ☐ Acquirer ☐

Credited to: Issuer ☐ Acquirer ☐

First Presentment Network Processing Date (MM/DD/CCYY): _____

Original Transaction Amount _____ Currency Code _____

Good Faith Amount USD _____

Good Faith Amount CM _____ CM Currency Code _____

Good Faith Amount S/E _____ S/E Currency Code _____

Financial Reference Number (Optional) _____ Network TID# _____

C. Documentation

Supply copies of pertinent Documentation required to support the Good Faith request. The Network TID should appear on all documents. Check documents included. **All copies must be legible.**

Forms/Exhibits		Supporting Documentation	
AEGNS Good Faith Form	☐	Copy of Receiving Participants Authorization	☐
		Copy of latest dispute Transaction in life cycle:	
		- First Chargeback attached, OR	☐
		- Second Presentment attached, OR	☐
		- Final Chargeback attached	☐

Additional Information/Comments: _____

D. Filing Network Participant Information - By signing below, Participant certifies that all information contained herein is true and correct.

Prepared By: _____ Title: _____

Authorized By: _____ Title: _____

Authorized Signatures _____ Date Prepared: _____

Email Address: _____

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

This form is referenced in Section 7.11.2, "Good Faith Filing Procedures," on page 364.

Good Faith Form Instructions

This form is used by Participants to file a Good Faith request.

1. Complete all sections (must be legible).
2. Attach supporting Documentation (must be legible).
3. Mail original copy to:

   AEGNS Arbitration Committee
   American Express (India) Private Limited
   Network Policy Compliance Team
   14th Floor, Tower-C
   Building No. 5
   DLF Cyber City, Phase - III
   Gurgaon - 122002 (Haryana)
   India

4. Retain a copy of all mailings.

Table 12-4 Network Good Faith Form Definitions

Field Name	Definition
A. Participant Information	
Filing Network Participant Name	Name of Participant filing the Good Faith.
Filing Network Participant AIN or BIN (IIN) #	Acquirer Identification Number or Issuer Identification Number assigned to filing Participant by AEGNS.
Receiving Network Participant Name	Name of the receiving Participant.
Receiving Network Participant AIN or BIN (IIN) #	Acquirer Identification Number or Issuer Identification Number assigned to the receiving Participant by AEGNS.
Cardmember Account Number	Assigned Account number for Cardmember.
S/E Number	Assigned number for S/E.
B. Transaction Information	
Good Faith Transaction will be debited to Issuer or Acquirer	Select a box in order to process debit to the proper Participant.
Good Faith Transaction will be credited to Issuer or Acquirer	Select a box in order to process credit to the proper Participant.
First Presentment Network Processing Date	Date First Presentment Transaction Processed by the Network (MM/DD/CCYY format).
Original Transaction Amount	Amount of original Transaction submitted to the Network
Currency Code	Alpha Currency Code of original Transaction submitted to the Network.
Good Faith Amount USD	U.S. Dollar amount of the Good Faith Transaction.
Good Faith Amount CM	Cardmember amount of the Good Faith Transaction.
CM Currency Code	Alpha Currency Code of Cardmembers Good Faith Amount.
Good Faith Amount S/E	S/E amount of the Good Faith Transaction.
S/E Currency Code	Alpha Currency Code of the S/E's Good Faith Amount.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 12-4 Network Good Faith Form Definitions (continued)

Field Name	Definition
Financial Reference Number (Optional)	Optional field - not required by AEGNS.
Network TID	Network Transaction Identification Number of the Good Faith Transaction.
C. Documentation	
Documentation	All forms/exhibits/supports listed in this section must be included as part of the Good Faith filing.
D. Filing Network Participant Information	
Filing Network Participant Information	Print the contact information and sign the form as indicated. Obtain an Authorized signature.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Exhibit 19. Neutrality Principles for Conducting Merchant Acquiring Business

Acquirers shall adhere to the following principles in dealing with Local Network Card Issuers and their Cardmembers with regard to Local S/E offers and promotions:

1. Whenever possible, existing S/E offers and network programs shall be leveraged for Local Network Cards.
2. Network usage programs (e.g., destination and industry programs) shall be developed by Acquirer to include as targets for the programs all relevant Cardmembers, including Local Network Cardmembers. All Issuers shall be permitted to participate in network usage programs that are relevant to their Card base at each Issuer's discretion. If Acquirer charges for access to a network usage program, it shall charge all Issuers on the same terms.
3. Acquirer shall be responsible for sourcing and developing relevant merchant offers for Local Network Card Issuers and their Cardmembers, and shall bear all costs associated with sourcing and developing such offers.
4. If a program or offer idea was originated and funded by a specific Card marketing group or Issuer, it shall not be available to any other Issuer.
5. Copy and creative must clearly communicate which Cards are eligible for the program. When a network program is open to all Issuers, only the Blue Box shall be used as a symbol for universal acceptance.
6. If a network usage program/offer is based on specific criteria, it shall be made available only to Issuers that provide data to support segmentation for their Cardmember base to appropriately target the program or participate in an alternative process that enables ease of execution (e.g., if an offer is targeted at males over 30 who have household incomes of greater than $75,000 (USD), only Issuers that have the ability to provide data that supports this segmentation scheme, or can provide and easily execute a work-around, may participate).
7. Network programs/offers may have a particular geographic scope as long as all Issuers falling within the scope may participate.
8. All above-the-line advertising related to the merchant network shall include only the Blue Box and not differentiate among Issuers or Card product group including network sponsorships.
9. There shall not be any discrimination among Card products at the point-of-sale with respect to POS decals.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

13 Abbreviations and Acronyms

13.1 Abbreviations and Acronyms

The abbreviations and acronyms in this glossary apply to all sections of the *Business and Operational Policies* manual.

Table 13-1. Abbreviations and Acronyms

2FA	Two Factor Authentication
3CSC	3-digit Card Security Code
4CSC	4-digit Card Security Code
4DBC	4-digit Batch Code
5CSC	5-digit Card Security Code
AAV	Automated Address Verification
ACS	Access Control Server
AEGN	American Express Global Network
AEGNS	American Express Global Network Services
AEIPS	American Express ICC (Integrated Circuit Card) Payment Specification
AES	Advanced Encryption Standard
AEVV	American Express Verification Value
AIN	Acquiring Institution Number
AIP	Application Interchange Profile
AMEX	American Express Travel Related Services Company, Inc.
AML	Anti-Money Laundering
APAC	Asia Pacific
API	Application Programming Interface
APN	Acquiring Institution Processor Number
APO	Army Post Office
ARC	Airline Reporting Corporation
ASV	Approved Scanning Vendor
ATF	Anti-Terrorist Financing
ATM	Automated Teller Machine
BDK	Base Derivation Key
BIN	Bank Identification Number
CAPK	Certification Authority Public Key

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 13-1. Abbreviations and Acronyms (continued)

CAT	Customer Activated Terminal
CDCRP	Cardholder Data Compromise Recovery Process
CDCVM	Consumer Device Cardholder Verification Method
CSCK	Card Security Code Key
CIF	Cards In Force
CIT	Cardmember-Initiated Transaction
COTS	Commercial off-the-shelf
CPQR	Consumer-Presented Quick Response
CRU	Central Rating and Underwriting Team
CSC	Card Security Code
CVM	Cardholder Verification Method
DAF	Daily Activity File
DAP	Daily Activity Process
DAR	Daily Activity Report
DCF	Digital Card Facilitator
DCSC	Dynamic Card Security Code
DDA	Dynamic Data Authentication
DFMNS	Dynamic Fraud Management Network Services
DNS	Domain Name System
DPA	Digital Payment Application
DPP	Deferred Payment Plan
DSP	Data Security Policy
EC	European Commission
ECI	Electronic Commerce Indicator
ECR	Emergency Card Replacement
EEA	European Economic Area
EFT	Electronic Funds Transfer
EIRP	American Express Enterprise Incident Response Program
EMEA	Europe/Middle East/Africa
EMV	Europay, Mastercard, and Visa
ET	Eastern Time
EU	European Union

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 13-1. Abbreviations and Acronyms (continued)

FIE	Foreign International Establishment
FLS	Fraud Liability Shift
FNP	Filing Network Participant
FPO	Fleet Post Office
FTG	Fraud to Gross
GDMP	Global Disputes Monitoring Program
GNSAS	Global Network Services Authorizations System
HCE	Host Card Emulation
IATA	International Air Transport Association
ICC	Integrated Circuit Card
iCSC	Integrated Circuit Card Security Code
ID	Identification
ID&V	Identification and Verification
IIN	Issuer Identification Number
IND	Issuer Notification Date
IOR	Issuer Override Request
IOP	Issuer Originated Payment
IP	Internet Protocol
ISM	Internal Service Metric
ISO	International Organization for Standardization
ISP	Internet Service Provider
IVPN	Internet Virtual Private Network
KEK	Key Encrypting Key
KYC	Know Your Customer
LCM	Life Cycle Management
LCOL	Lower Consecutive Offline Limit
LMK	Local Master Key
LUK	Limited Use Key
LUPC	Limited-Use Payment Credentials
MAC	Message Authentication Code Key
MCC	Merchant Category Code
MDK	Master Derivation Key

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 13-1. Abbreviations and Acronyms (continued)

MIS	Management Information Services
MIT	Merchant-Initiated Transaction
MNA	Multinational Account
MPI	Merchant Plug-In
mPOS	Mobile Point of Sale
MPQR	Merchant-Presented Quick Response
MST	Magnetic Secure Transmission
NAV	Name and Address Verification
NCL	Network Card License
NFC	Near Field Communication
OTP	One-Time Password
P2P	Peer-to-Peer Payment
P2PE	Point-to-Point Encryption
PAR	Payment Account Reference
PAN	Primary Account Number
PANDA	Pre-Authorization Network-based Dynamic Authentication
PCI DSS	Payment Card Industry Data Security Standard
PCP	Participant Communication Platform
PCSC	Printed Card Security Code
PEK	PIN Encryption Key
PFI	Payment Card Industry Forensic Investigator
PII	Personally Identifiable Information
PIN	Personal Identification Number
POC	Point of Compromise
POS	Point of Sale
QR	Quick Response
ROC	Record of Charge
RNP	Receiving Network Participant
SAQ	Self-Assessment Questionnaire
SAR	Suspicious Activity Report
SCA	Strong Customer Authentication
S/E	Service Establishment

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 13-1. Abbreviations and Acronyms (continued)

SOC 1	Service Organization Controls 1
SOC 2	Service Organization Controls 2
SRC	Secure Remote Commerce
SRCi	Secure Remote Commerce Initiator
SSAE16	Statement on Standards for Attestation Engagements16
SVDF	Stored Value Digital Facility
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAT	Transit Access Terminal
TDEA	Triple Data Encryption Algorithm
TID	Transaction Identifier (changed from "Transaction Identification Number")
TLS	Transport Layer Security
TRID	Token Requestor ID
TSP	Token Service Provider
TVR	Terminal Verification Results
UIR	Urgent Investigation Request
URL	Uniform Resource Locator
VAT	Value-Added Tax
VBU	Valid Billing Unit
VIP	Very Important Person
VRU	Voice Response Unit
WFIS	Worldwide Fraud Information System
WINTER	WINdow To Early Referrals
ZCV	ZIP Code Verification
ZMK	Zone Master Key
ZPK	Zone PIN Key

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

14 Definitions

14.1 Definitions

The definitions in this glossary apply to all sections of the *Business and Operational Policies* manual. Wherever a term is capitalized it has the meaning shown in this glossary.

Table 14-1. Definitions

4 Digit Batch Code (4DBC)	The number printed on a Card identifying the production batch of the Card.
Access Control Server	The Access Control Server is a component of SafeKey that operates in the Issuer domain. It verifies whether Authentication is available for a Card number and performs Payer Authentication for given Transactions.
Account	An account established by an Issuer with a Person upon the issuance of one (1) or more Cards.
Account Card	Account Card functionality enables a Card to be linked to a current account, deposit account, or other similar account. A Charge is deducted from the linked account on a delayed basis, generally fifteen (15) days after the Transaction Date. An Account Card is not a Debit Card.
Account Data	Account Data has the meaning contained in the current "PCI DSS Glossary, Abbreviations and Acronyms" and, as of the date of this publication, consists of: Cardholder Data and/or Sensitive Authentication Data.
Account Status Check	A type of Authorization Request that is used to ask an Issuer to indicate if the Account represented by the Account number on the message is valid. The Account Status Check is used, for example, by transit authorities to check the status of an account associated with the processing of Transactions at Transit Access Terminals.
Acquirer	Any entity (including, without limitation, American Express and American Express Entities) authorized by American Express or an American Express Entity to engage in the Merchant Acquiring Business.
Acquirer Reference Number	A component of one (1) or more of the Network's financial Transaction messages containing the reference data supplied by an Acquirer for its own Transaction matching.
Acquirer's Rate	The percentage of the Merchant Discount received by an Acquirer on Charges.
Acquiring Institution Number (AIN)	The unique identification number assigned to an Acquirer by AEGNS.
Action Code	A code provided in the POS Authorization Response (1110) message indicating the Issuer's disposition for the Transaction.
Action Plan	A sequence of steps that must be taken or activities that must be performed by a Participant in order to correct a deficiency that prevents the Participant from adhering to one (1) or more of the policies in the *Business and Operational Policies* manual.
Address Verification	An Authorization option that allows an S/E to verify the Cardmember address information.
Advance Deposit or Payment Program	A program which allows a participating S/E to recover some or all of the revenue lost when reserving facilities or Services for a Cardmember who made an advance commitment for their use but does not arrive to utilize them and does not cancel within cancellation requirements.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Advanced Payment Product	A payment method (including, but not limited to, a Chip Card or a Mobile Device) that uses emerging technology, such as EMV, Expresspay, or Expresspay Mobile, or an Account number that interacts with POS devices to initiate AEIPS or Expresspay Transactions.
Advice	A message in which the sender notifies the receiver of an activity that has been taken, requiring no approval but requiring a response.
AEGN Manual	See "American Express Global Network Manuals (AEGN Manuals)" on page 496.
AEIPS	American Express ICC (Integrated Circuit Card) Payment Specifications.
AEIPS Application	An application residing on a Chip Card that is used in the initiation of an AEIPS Transaction at an AEIPS-compliant POS device.
Affinity Card	A Co-Branded Card which is typically marketed to Persons who are members of an organization (e.g., a university alumni association or a professional association), or who have an association with an organization, where a significant feature of such Card are special benefits (e.g., charitable donations, discounted fees) given to such organizations or their members who are Cardmembers.
Affinity Partner	An organization (e.g., professional association) which is not an Issuer and which participates in marketing an Affinity Card with an Issuer pursuant to an agreement with an Issuer and whose name, logo, tradename, trademark, or service mark appears on the Affinity Card issued.
Aggregated Transaction	The combining of two (2) or more individual purchases incurred on the same Card Account number and S/E number into one (1), larger Transaction.
Agreement	See "Participant Agreement" on page 514.
American Express (AMEX)	American Express Travel Related Services Company, Inc.
American Express Brand	The American Express name, trademarks, service marks, logos and other proprietary designs and designations, and the imagery owned by American Express and its parent, subsidiaries and affiliates and the goodwill associated with all of the foregoing and with all the Goods and Services now and in the future provided, marketed, offered, or promoted by an American Express Entity.
American Express Card	See "Card" on page 499.
American Express Enterprise Line	A Card that follows the established Card design, positioning, and core features set out in the American Express Card design and marketing guidelines. Formerly referred to as an "American Express Format Card" or "Centurion Line Card."
American Express Entity	American Express or any entity controlling, controlled by or under common control with American Express.
American Express Format Card	See "Blue Box Line" on page 499.
American Express Global Network (AEGN) or Network	A global payments platform comprised of communication systems and operational infrastructure that enables payments processing and services that support Participants, Merchants, Cardmembers, and the American Express Brand.
American Express Global Network Manuals (AEGN Manuals)	The set of publications distributed to Acquirers and Issuers by AEGNS. The AEGN Manual(s) may be modified or otherwise amended by AEGNS from time to time.
American Express Global Network Services (AEGNS)	The business division of American Express responsible for managing the business relationship with Acquirers and Issuers which operate pursuant to a license from an American Express Entity.
American Express ICC Payment Specification	The preferred American Express specification for implementing payment Cards using integrated circuit technology.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

American Express Information	American Express Information means confidential information of American Express and American Express Entities.
American Express SafeKey®	American Express SafeKey® is an industry-standard Authentication method that, when employed by Issuers, Cardmembers, Acquirers, and Internet S/Es, provides greater security for Internet Transactions. Also see SafeKey.
American Express Verification Value (AEVV)	A cryptographic value derived by the Issuer during authentication. The AEVV can provide evidence of the results of payment Authentication during an online purchase.
Americas	AEGNS includes the following as Americas: United States, Canada, and Latin America/Caribbean.
Amex Shared ATM Network	All third-party ATMs (i) to which Cardmembers have access under agreements between an American Express Entity and the ATM owners or network operators and (ii) for which AMEX is required to settle for ATM transactions with the ATM owner or the network operators.
Anonymous Non-Reloadable Prepaid Card	A Prepaid Card which is not reloadable, and where the identity of the purchaser is not validated by the Card Issuer.
Annual EMV Attestation	A declaration of the S/E's status of PCI DSS-related compliance for EMV Transactions in the form that is available at: https://portal.securetrust.com.
Application Interchange Profile (AIP)	The Application Interchange Profile (AIP) stored on the chip contains data used by the Chip-Enabled Device to determine if the Chip Card supports offline data Authentication.
Approval Code	A code provided by an Issuer, an Issuer's Authorized Processor, or by the AEGN during Stand-in Authorization to indicate that the Authorization Request has been approved.
Approval Rate	An Issuer's number of Approval responses as a percentage of all POS Authorization Requests processed, to include Stand-In.
Approved Scanning Vendor (ASV)	A vendor approved by the PCI Security Standards Council to validate adherence to certain PCI Data Security Standard requirements by performing system vulnerability scans. A list of Approved Scanning Vendors is available by accessing www.pcisecuritystandards.org.
Arbitration	The procedure used to resolve issues between Acquirers and Issuers regarding Network policies and determine responsibility for the disputed item.
Arbitration Filing	A formal filing by an Acquirer to the AEGNS Arbitration Committee.
Attempt	An American Express SafeKey Authentication type where the S/E requested to Authenticate the Cardmember and a proof of Attempt, as evidenced by the AEVV value, was returned by either the Issuer or the AEGN, as evidenced by the ECI value on the POS First Presentment (1240) message.
ATM Acquirer	An American Express Entity or other Person authorized by an American Express Entity to acquire Transactions by Cardmembers at ATMs.
ATM Agreement	The Agreement between a Participant and an American Express Entity whereby Cardmembers other than a Participant's Cardmembers gain access to the Participant ATM Network or the Participant Shared ATM Network.
ATM Balance Inquiry	A Transaction at an ATM to request the balance of a demand deposit, current, savings, or other similar account.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

ATM Transaction	(i) An attempted or completed Cash Advance, Cash Withdrawal, or other activity, such as ATM Balance Inquiry or PIN management (to the extent AMEX or an American Express Entity elects, at its option on behalf of Issuers, to adopt and support such other activity), (ii) conducted at an ATM of the Amex Shared ATM Network, Participant Shared ATM Network, or Participant ATM Network through the use of a Card, and (iii) initiated with a PIN associated with such Card.
Authentication	The SafeKey process by which a Cardmember is validated based on certain criteria such as security questions or alternative Authentication mechanisms. It is also the process in which a Cardmember participates in SafeKey to secure an Internet Transaction.
Authentication Data	All Authentication-level data associated with the SafeKey Authentication process.
Authorization/Authorized	An S/E obtaining an Approval for a Transaction or an Issuer's approval of a Transaction to a Card Account number range assigned to the Issuer.
Authorization Adjustment	The Authorization Adjustment message allows Acquirers and their S/Es to adjust the Transaction amount when the final Transaction amount is lower than the amount previously authorized. This allows the Issuer to release any hold on available funds on a Cardmember's account for excess amounts authorized without waiting to receive the Presentment message containing the final Transaction amount.
Authorization Expiration	The number of days an approved Authorization is valid, before another Account Status Check or Authorization is required.
Authorization Fraud Control Questionnaire	The questionnaire that AEGNS uses to evaluate the fraud controls Issuers have in place to prevent fraud on Eligible Transactions processed on the AEGNS Network.
Authorization on Credit	Authorization on Credit is functionality that allows Acquirers to send refund Authorization Request messages to Issuers.
Authorization Request	The message sent from Acquirer to Network and Network to Issuer requesting Authorization.
Authorization Response	The message sent from Issuer to Network and Network to Acquirer in response to an Authorization Request.
Authorization Reversal	Authorization Reversal is a message that can be system-generated or initiated by S/Es. System-generated Authorization Reversals are initiated when either the Acquirer or the Network receives an approval from the Issuer but were unable to complete the Transaction. System-generated Authorization Reversals are generally generated due to late arriving approvals or problems after receipt of the approval. S/E POS-initiated Authorization Reversal allows cancellation of a previously approved Transaction amount. The reversed Transaction must not be submitted to the Network for Settlement.
Authorized Currency	The currency for which a Participant is authorized by AEGNS to operate as an Issuer, an Acquirer, or both.
Authorized Processor	A third-party company to the extent that it has been engaged by an Acquirer or Issuer, and certified by AEGNS to perform processing services on behalf of the Acquirer or Issuer.
Automated Address Verification (AAV)	A Network feature that allows an Acquirer to electronically verify the Cardmember's address information through the Authorization process.
Automated Teller Machine (ATM)	An unattended terminal which, among other things, is capable of dispensing cash when accessed with a payment card or other account access device with the use of a PIN.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Bank Holiday	A day when the Settlement Bank of either the Acquirer or the Issuer and/or AEGNS is closed for business.
Bank Identification Number (BIN)	A 6-digit number identifying the Issuer Institution. It is also used as the first six (6) digits of a Card Account number issued by the Issuer, or the first six (6) digits of a Token.
Batch Processing	A type of data processing operation and data communications transmission where related Transactions are grouped together and transmitted for processing, usually by the same computer and under the same application. The process is generally considered as non-real-time data traffic comprising large files and is used where response time is not critical.
Beta Test	A live operational and systems test for each type of Card an Issuer proposes to issue.
Bill Payment Provider	An S/E that is engaged by Cardmembers to pay a bill on their behalf. Bill Payment Providers charge the Cardmembers' Account and pay the End Beneficiary identified in the bill using another method, such as bank transfer, check, or wire.
Billing(s)	The aggregate of amounts on all Cardmember statements with inclusions and exclusions as defined in the Participant Agreement.
Blind Count Reconciliation	A dual-control verification process wherein two (2) different individuals independently verify the number of items being added without knowing the other's results.
Blue Box	The American Express Blue Box logo.
Blue Box Decal	A decorative sticker, electronic screen picture, or laminated plastic or metal picture displaying a printed design of the Blue Box.
Blue Box Line	A Card or Account number issued by a Person other than American Express or an American Express Entity on which the name, logo, or indicia of American Express occupies 25% or less of the front and back of the Card. Also referred to as "Network Card," "NCL Card," or "Blue Box Line Card."
Brand Protection	Policies and procedures designed to protect the American Express Brand and Participants against exposure to regulatory, financial, and brand risks associated with Illegal or Brand Damaging Activity.
Brand Protection Assessment	The Brand Protection Assessment is a risk-based assessment questionnaire and process used to identify potential gaps in acquiring practices. A Brand Protection Assessment includes: 1) Completion of a Brand Protection Assessment questionnaire. 2) Correction of any deficiencies as determined by AEGNS. The status of any remediation activities must be provided to AEGNS upon request. 3) Written confirmation from AEGNS that the Brand Protection Assessment has been completed, deficiencies have been corrected to the satisfaction of AEGNS and the Acquirer is approved, subject to all other requirements of the *Business and Operational Policies* manual, to acquire S/Es in industries or participating in activities listed in Table 2-11, "Restricted Industries Requirements," on page 95.
Business Day	A day on which all parties to a transaction and/or an event are open to do business.
Card	A payment Card bearing an American Express trademark or logo and issued by an Issuer, or an Account number issued by an Issuer, in any form factor, which can be used to purchase Goods and Services from S/Es on the AEGN, to make payments between Persons, and/or to obtain financial services at ATMs.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Card Artwork	A photographic version of the visual representation of Participant's artistic designs present on the Card Image.
Card Image	A photographic version of the visual representation of the overall Participant-issued American Express-branded Card (excluding the American Express logo).
Card Issuing Business	The business engaged in by an Issuer whereby the Issuer: 1) Issues Cards to their customers pursuant to an agreement with the customers; 2) Authorizes their Cardmembers to charge purchases of Goods and Services by means of the Card at S/Es or to access cash at ATMs; 3) Accepts and settles Charges and other Transactions transacted by their Cardmembers, which have been captured and processed by an Acquirer; 4) Either by itself or through a processor certified and approved by AEGNS, renders statements of Account to their Cardmembers; and 5) Renders related services to Cardmembers.
Card-on-file	The storage of a Cardmember's PAN and associated data by or on behalf of an S/E in support of Billing Services, including, but not limited to, Recurring Billing Transactions.
Card Not Present	Any Transaction in which the Cardmember and Card are not present at the Point of Sale (e.g., Internet, mail order).
Card Present	Any Transaction in which the Cardmember and Card or Mobile Proximity Payment Device (MPPD) are present at the Point of Sale (e.g., a retail store).
Card Production Security Assessor (CPSA) Company	A security organization that has been qualified by the PCI Security Standards Council to validate an entity's adherence to the *PCI Card Production and Provisioning Logical Security Requirements* and *PCI Card Production and Provisioning Physical Security Requirements.* A list of CPSA Companies is available at www.pcisecuritystandards.org.
Card Production Vendor	A vendor that provides card production and all processes related to the manufacturing and personalization of Cards.
Card Security Code (CSC)	Any of several values printed or encoded on the Card and used for fraud prevention in Authorizations, including: the Printed Card Security Code (PCSC), the 5-digit Card Security Code encoded within the magnetic stripe (5CSC), and the 5-digit Card Security Code encoded within the magnetic stripe equivalent on Chip Cards (iCSC). See also "One-Time Password (OTP)" on page 514.
Card Security Code Key (CSCK)	A Cryptographic Key used to create Card Security Codes that are placed on the magnetic stripe, chip, or Card.
Cardholder Data	Cardholder Data has the meaning contained in the current *PCI Data Security Standard Glossary, Abbreviations and Acronyms* (refer to www.pcisecuritystandards.org), and, as of the date of this publication, it includes the following elements: • The full Primary Account Number (PAN) by itself, or • The full PAN plus any of the following: - Cardholder Name - Expiration Date - Service Code
Cardholder Data Compromise Recovery Process (CDCRP)	The Cardholder Data Compromise Recover Process (CDCRP) is the exclusive remedy for Issuers to recover from an Acquirer the incremental fraud losses and operational costs associated with a Data Compromise Event.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Cardholder Verification Method (CVM)	The method by which Cardmember verification is performed to ensure that the Person presenting the Card or Mobile Device is the Person to whom the application was issued.
Cardless Account	A Cardless Account is an Account created by an Issuer for which no physical card is issued.
Cardmember	A Person who has entered into an agreement and established an Account with any Issuer, or is authorized on an Account.
Cardmember Documentation	Documentation that Issuers obtain from their Cardmembers. This Documentation is then supplied to the Acquirer in support of a Chargeback.
Cardmember Information	Information about Cardmembers arising from their application for and/or use of a Card, including and without limitation, their Cardmember Account number, Account status, effective date, cancellation date (if applicable), type of Card (consumer, small business, etc.), rewards program indicator, rewards program type, city, country subdivision code, country code, postal code, gender, date of birth, address change date, marketing preferences, and fee services/enrollments.
Cardmember-Initiated Transaction	A Transaction that involves direct participation of the Cardmember.
Cards in Force (CIF)	Total number of non-cancelled Cards issued by a particular Issuer as of the end (or beginning, when stated) of a given period.
Caribbean Countries	AEGNS includes the following as Caribbean Countries: Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Bermuda, Bonaire and Sint Eustatius and Saba, British Virgin Islands, Cayman Islands, Curacao, Dominica, Grenada, Haiti, Jamaica, Montserrat, St Kitts-Nevis, St. Lucia, Saint-Martin, Sint Maarten (Dutch part), St. Vincent and the Grenadines, Saint-Barthelemy, Trinidad and Tobago, Turks and Caicos Islands.
Cash Advance	The receipt of cash from an ATM displaying the American Express logo, by a Cardmember using their Credit Card or Charge Card.
Cash Disbursement	The manual disbursement of cash to AEGN Participant Cardmembers by a Cash Disbursement Provider.
Cash Disbursement Provider	Branch locations of Participants that have been certified to process Cash Disbursements.
Cash Withdrawal	The receipt of cash from an ATM displaying the American Express logo by a Cardmember using their Debit Card.
Central Rating and Underwriting Team (CRU)	An internal team within AMEX's risk management group that provides credit risk assessments on all institutional counterparties (including Participants) that have exposure with AMEX. The credit assessment is derived from an analysis of the counterparty's financial operations, its competitive position, strength of management, long term strategy, and the overall economic environment in which the company operates.
Certification	The verification of a Participant's ability to send and/or receive all files and messages used by AEGNS (or new or modified features introduced since the Participant originally certified) prior to gaining full access to the AEGN.
Change of Control	A material change in the beneficial control or ownership (i.e., 15% or more) of a Participant, whether such change is through transfer of shares, merger, consolidation, sale, or merger of assets or otherwise.
Charge Card	A Card for which the full amount outstanding on the Account each month is required to be paid by the Cardmember on receipt of their statement.
Charge or Charges	The total price, including all applicable taxes and gratuities, for the purchase of Goods or Services for which the Cardmember has indicated an intent to pay with the Card.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Chargeback	An amount which an Issuer is entitled to collect from an Acquirer in accordance with the Network Chargeback policy as detailed in the "Chargeback Policies" chapter beginning on page 280.
Chargeback Reason Code	ISO code indicating the reason a Transaction was charged back.
Check Digit Routine	A calculation that is performed on the Cardmember Account number in an effort to ensure that numbers were not transposed or mis-keyed.
Chip Card	A Card with an embedded chip containing AEIPS and/or Expresspay Applications that, when used at a Chip Card-enabled terminal, interacts with the terminal to initiate AEIPS or Expresspay Transactions.
Chip-Enabled Device	A card acceptance device that is: i. Capable of reading and/or processing a magnetic stripe and chip on a Card for the purpose of performing a service such as obtaining an Authorization or processing a payment; or ii. Used to communicate with the Chip Card during a Transaction. It also provides the Chip Card with power and timing.
Ciphertext	Data that has been enciphered and has no apparent meaning or context (for example: 77~#aB3&_zrTx813").
Clearing	The process of routing, editing, and summarizing Transaction data between an Acquirer and an Issuer via the AEGN to facilitate posting of a Cardmember's Account and reconciliation of a Participant's Settlement position.
Clearing Center	Clearing Center means the facility or facilities designated by American Express for the handling and processing of Charges, settlement of accounts between and among Issuers and Acquirers, coordination of international fraud control, and performance of all other international clearing house functions for the operation of the Network.
Co-Branded Card	A Card that contains the name, trademark or logo of a Co-Branding Partner in addition to the name, trademark or logo of American Express and the Issuer and that is jointly marketed by the Issuer and the Co-Branding Partner where a significant feature of the Card is special benefits (i.e., rewards) given to Cardmembers.
Co-Branding Partner	A company, typically a non-bank (e.g., airline, automobile manufacturer) which is not an Issuer and which actively participates in marketing a Co-Branded Card with an Issuer, and whose name, logo, trade name, trademark or service mark appears on the Co-Branded Card issued.
Code 10	A code provided by an S/E during an Authorization Request, whether or not an Authorization was required, to indicate that the S/E has suspicions concerning the Cardmember, the Card, the circumstances of the sale, or any combination thereof.
Commercial off-the-shelf (COTS) Device	A Mobile Device (e.g., smartphone or tablet) that is designed for mass-market distribution, and is not designed specifically for payment processing.
Commercial Products	A Card or Account number issued by an Issuer to business customers for business-related expenditures. Commercial Products include Corporate Cards, Corporate Purchasing Cards, and Business Cards as described in the "Product Features and Specifications" chapter beginning on page 125.
Compelling Evidence	Additional types of Documentation provided by the Acquirer to demonstrate the Cardmember participated in the Transaction, received Goods or Services, or benefited from the Transaction.
Compliance	The procedure used to resolve issues between Acquirers and Issuers regarding a violation of the policies in the *Business and Operational Policies* manual.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Compliance Filing	A formal filing by either Acquirer or Issuer to the AEGNS Arbitration Committee.
Confirmed Fraud	Fraud is defined as Confirmed Fraud when an Issuer verifies with the Cardmember that a Transaction(s) is fraudulent or when the Issuer has otherwise determined that a Transaction(s) was completed as a result of the fraudulent use of a Card.
Consumer Device Cardholder Verification Method (CDCVM)	An Issuer-approved, AEGNS-recognized Cardholder Verification Method whereby the Cardmember's credentials are verified on a Mobile Device.
Consumer-Presented Quick Response (CPQR)	A Transaction where a Cardmember uses the Issuer application on a Mobile Device to generate a Quick Response (QR) Code that is scanned by the S/E at a POS device.
Contactless	A term used to describe a Transaction environment in which a Card or Mobile Device is enabled with a radio frequency component to communicate with a radio frequency-enabled POS device to initiate a Transaction.
Copyright-Infringing Products	Any products which are copies made without the consent of the Rights-Holder or Person duly authorized by the Rights-Holder and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under laws applicable to the Issuer, Acquirer, Cardmember, or S/E.
Corporate Card Client	A legal entity that has entered into an agreement and established a Corporate Card Account with any Issuer of Corporate Cards.
Cost of Funds	Interest or associated costs (as a rate) paid by a financial institution to continue servicing the business function following late or non-settlement.
Counterfeit Trademark Products	Any products, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such products, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the Rights-Holder of the trademark in question under laws applicable to the Issuer, Acquirer, Cardmember, or S/E.
Credentials-on-File	Any Cardmember account data, including, but not limited, to PAN or Token, that is stored by S/Es.
Credit	An amount to be credited to a Cardmember's Card Account.
Credit Card	See "Revolving Credit Card" on page 517.
Credit Card Refund Notice	A document that is issued by an airline or travel agent when a ticket is returned for a refund to be evidenced by a Credit on a Cardmember's Card Account.
Cryptographic Key	A secret value which works with a unique algorithm to either Encipher the text or Decipher the Ciphertext.
Cryptoperiod	The time span during which a specific Cryptographic Key is authorized for use.
Cumulative Spend Protection Threshold	The maximum value of one (1) or more aggregated transit Transactions that can be settled against an approved Authorization and protected from Chargebacks.
Customer Activated Terminal (CAT)	An unattended POS device that dispenses a product or provides a service paid for with a Card (e.g., gasoline pump upon activation by a valid Card).
Daily Activity File	A flat file that contains transaction level activity for an organization's settlement and transaction reconciliation process. The flat file enables Participants to create custom reports.
Daily Activity Process	A process that provides Participants with a consolidated source of data for use during the auto-reconciliation or settlement process.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Daily Activity Report	A report that summarizes all daily activities for all Issuer IINs and Acquirer AINs associated with one (1) organization for one (1) reporting period. The Daily Activity Report is used for reconciliation and settlement.
Daily Activity Reporting	Daily Activity Reporting is a general term used to describe all the reporting provided by AEGNS for Participant Settlement reconciliation. This term incorporates the Daily Activity Process.
Daily Settlement Advisement	A document created by the AEGN for certain Participants used to augment the Daily Activity File in cases in which the Participant needs additional calculations on settlement not automatically performed by the AEGN.
Data Certificate	Cryptogram sent in the ICC system-related data to ensure that a genuine Card was used and the message data had not been altered.
Data Compromise	Unauthorized use of or unauthorized access to Cardholder Data and/or Sensitive Authentication Data, including payment-related Cryptographic Keys, that results in the misuse of such information or the reasonable possibility that the misuse of such information will occur.
Data Compromise Event	Data Compromise that meets the criteria for Cardholder Data Compromise Recovery Process (CDCRP).
Data Compromise Event Window	The period of time in which incremental fraud may be recovered by an Issuer under CDCRP. This period is calculated as follows: up to 365 days prior to and thirty (30) days following the date the last notification of the potentially involved Account numbers in a Data Compromise was sent by AEGNS to the Issuer.
Data Security Policy (DSP)	A set of comprehensive policy requirements designed to protect Cardholder and Sensitive Authentication Data—collectively known as Account Data—whenever such data is stored, processed, or transmitted.
Debit Card	A Card that accesses a demand deposit, current, savings, or other similar Account. A Transaction is settled from the accessed Account. An Account Card or a Prepaid Card is not a Debit Card.
Decipher	The act of converting Ciphertext to its original Plaintext, using a cryptographic algorithm and a key.
Declined Authorization Protection	The maximum amount that can be settled following a declined Authorization for an Expresspay Transaction occurring at a Transit Access Terminal.
Deferred Billing	A single Transaction completed for which the total amount is billed in installments.
Deferred Payment Plan (DPP)	An optional network service which permits Charges to be billed in equal installments rather than in one (1) total billing.
Delayed Authorization	An Authorization Request submitted after a Transaction has completed and the Cardmember has left the S/E with the Goods or Services.
Delayed Billing	An additional amount which the Cardmember has agreed may be billed to his/her Card Account after he/she has accepted the Original ROC because of purchases of Goods or Services made by the Cardmember which could not be determined by the S/E at the time the Cardmember accepted the ROC. AEGN policies allow Delayed Billing only by car rental, cruise line, and lodging establishments, and only in situations where the final audit is not available until after the Cardmember has accepted the ROC.
Delayed Delivery	A Delayed Delivery Transaction occurs when a Cardmember makes a deposit or down payment for a purchase and the remainder of the purchase is made in a second Transaction when the Goods are shipped or delivered.
Deny List	An S/E-maintained list of Card Account numbers used to deny access to the transit service following a declined Authorization and to reinstate access following a subsequent Authorization approval.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

De-tokenization	The process of redeeming the Token for its associated PAN.
Digital Card	A digital representation of a payment Card used by an SRC System and/or Digital Card Facilitator, which may be hosted online or in a Cardmember device. A Digital Card contains data about the enrolled payment Card, and visually represents the PAN issued to the Cardmember.
Digital Card Facilitator	A role within the SRC ecosystem that provides a Cardmember with access to one or more Digital Cards and facilitates the checkout experience.
Digital Goods or Services	Digital merchandise or services downloaded or accessed via Internet or another file transfer process (e.g., movies, apps, games, virus scanning software).
Digital Payment Application	A website or E-commerce application operated by an S/E or other Service Provider, where the Cardmember can complete the purchase of Goods or Services by participating in SRC.
Digital Wallet Application-initiated Transaction	A type of Digital Wallet Payment where a Transaction is initiated by a digital wallet utilizing a merchant application within a Mobile Device, and not through the Contactless interface. This Transaction type is identified in the POS Authorization and Presentment messages with the "Z" value in Position 6 and "5" value in Position 7 of the Point of Service Data Code field.
Digital Wallet Contactless-initiated Transaction	A Type of Digital Wallet Payment where a Transaction is initiated by a digital wallet within a Mobile Device through the Contactless interface at an Expresspay-enabled POS Device. Issuers may identify this Transaction type by the "Y" value in Position 6 of the Point of Service Data Code field in the POS Authorization and Presentment messages.
Digital Wallet Magnetic Secure Transmission (MST) Transaction	A type of Digital Wallet Payment where a Transaction is initiated by a digital wallet within a Mobile Device through MST. This Transaction type is identified in the POS Authorization Request (1100) message by the Service Code value of 141.
Digital Wallet Payment	A Digital Wallet Contactless-initiated Transaction, Digital Wallet Application-initiated Transaction, or Digital Wallet Magnetic Secure Transmission (MST) Transaction conducted through a digital wallet, operated by an AEGNS-recognized Digital Wallet Program Provider that resides on a Mobile Device.
Digital Wallet Program	An AEGNS-recognized digital wallet program that supports enablement of Digital Wallet Payments or Expresspay Mobile Transactions initiated from Mobile Devices.
Digital Wallet Program Provider	A third-party provider that operates a Digital Wallet Program.
Disputes Process Transaction Life Cycle	The steps of the Transaction Life Cycle involved in processing Charge or Credit Transactions as viewed from the perspective of the Network when the Transaction has been disputed by the Issuer or Cardmember.
Document Type	Identifies the type of support required for a Retrieval Request Notification.
Documentation	Any supporting information provided by a Cardmember, Acquirer, Issuer, or S/E such as a Cardmember letter, copy, itemized Documentation, Original ROC, ROC, Substitute ROC, or Transaction Log.
Double Byte Character	A single character requiring two (2) bytes of data.
Dynamic Card Security Code (DCSC)	A dynamic code created by the AEGN and used in place of the PCSC. The Dynamic Card Security Code (DCSC) enables the AEGN to validate the Transaction during the POS Authorization Request (1100) message. Dynamic Card Security Code is a form of Dynamic Data.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Dynamic Data	An AEGN-generated Transaction-unique value used for Authorization. The AEGN validates the Dynamic Data in the POS Authorization Request (1100) message on behalf of the Issuer.
Dynamic Data Authentication (DDA)	A type of offline data Authentication in which the Chip-Enabled Device validates the data stored on the Card's chip based on a digital signature provided by the Card. The digital signature is unique for each Transaction. DDA provides added security during the Transaction by authenticating the validity of both the chip data and the Card itself.
Dynamic Fraud Management Network Services (DFMNS)	A set of fraud Authorization tools including a Fraud Probability Score and Recommendation Code assessed for each Eligible Transaction. The results of the evaluation (i.e., Eligible Transactions that have a higher fraud risk) are displayed to Issuers through WINTER and, for certified Issuers, through the Authorization message.
Dynamic Token	Tokens generated for a limited time use.
E-commerce	Electronic commerce is the buying or selling of physical or Digital Goods or Services using the Internet or an electronic network.
E-commerce Transaction	The purchasing of physical or Digital Goods or Services using the Internet, an application, or electronic network on either a personal computer or Mobile Device including, but not limited to, Internet Transactions or Digital Wallet Application-initiated Transactions.
E-ticket	An airline ticket purchased by mail, telephone, or the Internet which is provided to the Cardmember by electronic means; either through the Internet or another file transfer process.
Eastern Time (ET)	The time of the 5th time zone west of Greenwich that includes the eastern United States.
Electronic Commerce Indicator (ECI)	A data element related to American Express SafeKey indicating the outcome of SafeKey Authentication.
Eligible Transaction	All POS Transactions except: • Transactions occurring during system downtimes or outages that prevent AEGNS from providing an Issuer the DFM Network Services • On-Us Transactions
Emergency Card Replacement (ECR)	The process of replacing a Card for a Cardmember when he or she has reported that the original Card has been lost or stolen and a replacement is needed on an emergency basis.
EMV	Europay, MasterCard, Visa, and American Express. A term that is used to refer to the specifications developed by these four (4) bodies.
EMV Mode	An Expresspay Transaction mode that uses EMV-compliant processes both between the Card and Terminal and between the Terminal and the Acquirer.
Encipher	The act of converting Plaintext to Ciphertext, using a cryptographic algorithm and a key.
Encryption	Encryption has the meaning contained in the current International Organization of Standards (ISO) (refer to www.iso.org), and, as of the date of this publication, includes the act of enciphering, i.e., rendering of text (Plaintext) unintelligible (Ciphertext), by means of an encoding mechanism. Plaintext can be understood by any entity (e.g., a Person, a computer, or a process). Once transformed into Ciphertext, no entity can process or understand the data until the Ciphertext is correctly deciphered.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

End Beneficiary	A third-party entity that receives payments from an Indirect Acceptor. The End Beneficiary does not receive Card information from the Indirect Acceptor. An End Beneficiary may also separately be an S/E that directly accepts the Card.
Enhanced Functionality	The minimum product functionality required of Participants to qualify for the global and multinational Corporate client segment.
Enhanced Global Management Information System (eGMIS)	A process that enables the transmission of certain contractually required data files from Issuers of Corporate Cards for employees of Multinational Key Account companies to the AEGN.
Ethical Hacking	Ethical Hacking, performed by "white hats" or skilled computer experts, is the use of programming skills to determine vulnerabilities in computer systems.
European Economic Area (EEA)	European Economic Area combines the countries of the European Union (EU) and member countries of the European Trade Association. The purpose of the European Economic Area is the participation in the European market trade and movement, without having to apply to be one (1) of the EU member countries.
European Union (EU)	The European Union is a political and economic union of member states that are located primarily in Europe. It operates an internal (or single) market which allows free movement of goods, capital, services, and people between member states.
Exception	A written consent by AEGNS that approves a Participant's non-compliance with a specific requirement within the B*usiness and Operational Policies* manual or other related documents (see Section 1.4, "Related AEGNS Manuals, Guidelines, and Resources," on page 3).
Exception File	A file of Account numbers to be used by the Network during Stand-In Authorization, for which the Issuer has predetermined either an Authorization decision of denial (i.e., negative status) or requires special handling (i.e., VIP).
Expiration Date	The year and month on which a Card expires.
Expired Card	A Card for which the Expiration Date appearing on the front of the Card or encoded on the magnetic stripe has passed.
Expresspay	Expresspay is a program within American Express for facilitating Contactless Transactions between a Chip Card or Mobile Device containing an Expresspay Application and an Expresspay-enabled POS Device.
Expresspay Application	An application residing on a Chip Card or Mobile Device that is used in the initiation of an Expresspay Transaction at an Expresspay-enabled POS Device.
Expresspay Mobile	An AEGNS-approved service that is enabled by an Issuer and its Mobile Entities, including, as applicable, Service Providers. A mobile version of Expresspay where the Expresspay application is hosted in a secure element of a Mobile Device, or a software-based version of Expresspay Mobile where an Expresspay Mobile Host Card Emulation (HCE) Application resides in the operating system of a Mobile Device and is capable of transacting over a Contactless interface.
Expresspay Mobile Host Card Emulation (HCE)	A software-based version of Expresspay where an Expresspay Mobile HCE Application resides on the operating system (the "host") of a Mobile Device and communicates with a server system (the "cloud") that houses payment credentials, to facilitate Expresspay Mobile Transactions.
Expresspay Mobile Host Card Emulation (HCE) Application	An application residing in the operating system of a Mobile Device that contains one (1) or more Expresspay Mobile HCE Cards.
Expresspay Mobile Host Card Emulation (HCE) Card	A software-based Expresspay Card, residing in the Expresspay Mobile HCE Application, capable of being used to conduct Expresspay Mobile HCE Transactions.
Expresspay Mobile Transaction	An Expresspay Transaction initiated by a Mobile Device as a method of payment.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Expresspay-enabled POS Device	A POS device that is AEGNS Expresspay certified.
Expresspay Transaction	An Expresspay Transaction is a Contactless Transaction initiated by the use of an Expresspay-enabled Card or Mobile Device at an Expresspay-enabled POS Device.
External Service Metric	External Service Metrics are subjective measurements that are gathered from customer satisfaction surveys.
Fallback	When an AEIPS Transaction cannot be completed in a Chip-Enabled Device utilizing chip technology, the Chip-Enabled Device then reads the magnetic card stripe.
Fee Detail Section	A section within the Daily Activity Report which summarizes all fees and charges in accordance with contractual exhibits and AEGNS standard fee schedules to be settled within the Net Settlement.
Fictitious and/or Collusive S/E	An S/E whose sole purpose of accepting American Express Cards is to defraud, or conspire with other S/Es, employees, or a fraudulent Cardmember to defraud the Acquirer or Issuer.
File Acknowledgment	A notice sent by the AEGN to the Participant or their Authorized Processor to validate acceptance or rejection of an outcleared file after editing and validation is complete.
First Chargeback	The process an Issuer initiates to move financial liability from itself to an Acquirer on a previously submitted Presentment.
Final Chargeback	A second Chargeback, by the Issuer to the Acquirer, of the original Transaction, in response to a Second Presentment.
Financial Transaction	A Transaction clearing through the AEGN that has a direct Settlement impact associated with the Transaction.
First Presentment	The first time an Acquirer submits a Transaction to the Issuer through the Network. The First Presentment follows the Authorization Request and Authorization Response in the Transaction Life Cycle.
Floor Limit, Network	The amount of a Transaction requiring Authorization set for specific industry categories and geographic regions by AEGNS and to be used by Acquirers when setting S/E Floor Limits.
Floor Limit, S/E	A maximum monetary amount for a single Transaction, at or above which the S/E must obtain an Authorization before completing the Transaction. At their own financial risk, Acquirers may set individual S/E Floor Limits to amounts different from those specified by AEGNS.
Foreign Currency Factor	A percentage, as set out in the Participant Agreement, assessed by AEGNS on the processing of a Transaction made in a currency different from the currency in which the Cardmember's Card is denominated.
Foreign International Establishment (FIE)	A Multinational Account that has entered into an agreement with an American Express Entity covering locations in more than one (1) country under which it forwards Charges directly to an American Express Entity for payment or otherwise has payments for all of its operations handled on a globally uniform basis.
Fraud Full Recourse	The right of the Issuer to send a Chargeback to the Acquirer without a Retrieval Request Notification for Transactions incurred at an S/E which is a High Risk S/E according to the risk indicator in accordance with the Network Chargeback policy.
Fraud Liability Shift (FLS)	A shift in financial liability for fraudulent Transactions that occurs if certain requirements are met.
Fraud Probability Score	A 5-byte numeric value on an Eligible Transaction that indicates to the Issuer the probability of fraud.
Fraud Repository	The AEGN fraud reporting database used by Participants to electronically enter S/E and Cardmember fraudulent Transaction data.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Fraud to Gross (FTG)	The ratio of fraudulent Transactions as compared to total Charge volume, provided that both volume amounts are in the same currency. For S/Es and Acquirers, FTG is calculated on total gross sales volume and volume of fraudulent Transactions at an individual S/E (S/E FTG) or at all their S/Es (Acquirer FTG), excluding fraudulent S/E applications and non-received fraud. For Issuers, the FTG is calculated on total gross billed business volume and volume of fraudulent Transactions on their Card Accounts.
Fraudulent Application	An application for a Card Account submitted by an individual with the intent to defraud an Issuer using another individual's personal information in such application.
Fraudulent S/E	A Merchant that provides fraudulent information during the set up process with the intent of defrauding American Express or the Acquirer, or a Merchant whose S/E volume is comprised, or mostly comprised, of unauthorized or fraudulent Transactions including, but not limited to: • Billing Cardmembers for unauthorized Charges • Imprinting, swiping, or keying additional Transactions for unauthorized Charges before returning the Card to the Cardmember, or using stolen Account information while the Cardmember retains possession of their Card • Keying in an unauthorized Transaction after being given a stolen Account number by a collusive Participant
Fulfillment	The Documentation supplied by the Acquirer to support a Retrieval Request from the Issuer.
Fulfillment Notification	The message sent by an Acquirer in response to a Retrieval Request Notification (1642) message from an Issuer which indicates the action to be taken by the Acquirer.
Fully Authenticated	An American Express SafeKey Authentication type where the Cardmember's SafeKey was approved by the Issuer or the AEGN as evidenced by the ECI value on the POS First Presentment (1240) message.
Funding	See *Load*.
Funds Exchange	The process where Participants transfer funds based on the net value of the financial Transactions cleared for a given day or period.
Gambling S/E	An S/E registered with MCC 7801 (government-licensed online casinos), MCC 7802 (government-licensed horse/dog racing), or MCC 7995 (includes casino chips, gambling services, Internet gambling sites, bingo, and off-track betting and wagers at race tracks).
Geolocation	The process of finding, determining, and providing the geographic position of electronic devices through the use of methods such as GPS or IP address.
Geolocation Compliance	A set of controls and tools designed to ensure accuracy and validity of an electronic device's Geolocation, including methods to detect and block the use of location spoofing tools and address known vulnerabilities.
Global Disputes Monitoring Program (GDMP)	A program monitored by AEGNS to ensure Participants monitor their dispute rates and do not exceed acceptable levels of disputes.
Good Faith	An exchange between two (2) Participants, where one (1) Participant to a Transaction contacts the other Participant requesting an exchange of full or partial funds be accepted.
Goods	Tangible commodities manufactured or produced for sale (e.g., wares, merchandise).
Gross Fraud Rate	Total Gross Fraud reported to the Network over the Total Billed Business, excluding On-Us, ATM, and Fees.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Hardware Master Storage Key	A key used to protect all other keys in a Participant's Hardware Security Module (HSM) environment, including, but not limited to, Local Master Keys (LMKs), Hardware Security World, and Master Storage Keys (MSKs).
High Risk S/E	An S/E designation assigned by AEGNS indicating that certain Transactions conducted at the S/E may be charged back to the Acquirer under Fraud Full Recourse Chargeback rights.
Host Card Emulation (HCE)	A term used to describe the capability of a Mobile Device to provide NFC Card emulation by routing NFC messages to the operating system of the Mobile Device.
Host Stand-In	A Network service that provides Authorization services on behalf of the Issuer, based on Issuer parameters, when the Issuer is unavailable to the host.
Identification and Verification (ID&V)	A set of methods used to provide a Token Assurance Level set by the TSP, and provided to the Issuer.
Illegal or Brand Damaging Activity	Advertising or intending to handle or sell illegal or brand damaging Goods or Services where there is association with the American Express Brand or where the American Express Blue Box logo is displayed. Examples include but are not limited to: • The sales of Infringing Products • Unlawful sales of pharmaceutical products • Unlawful sales of tobacco and electronic smokeless tobacco products • Prohibited gambling activities • S/Es engaged in activities or practices that are deceptive or misleading or that reflect unfavorably upon the good name, goodwill, reputation, or image of AMEX or any American Express Entity, or that in any way are contrary to applicable law • Transactions related to child pornography, bestiality, or rape
Imprint	Cardmember data transferred from a Card to a Transaction receipt to complete a Transaction. An Imprint may be an electronic Imprint or a manual Imprint. A manual Imprint is the imprint of the embossed data taken with a manual imprinter. A pencil rubbing or photocopy of the Card is not considered proof of a valid Imprint.
Inbound Fraud to Gross (IFTG)	When complete On-Us sales volume and/or fraudulent Transaction volume data is unavailable, the Network will default to the Inbound Fraud to Gross Ratio. Inbound FTG is defined as the aggregate of Transactions processed by the Network, excluding all On-Us Transaction activity. IFTG is the ratio of fraudulent Transactions as compared to total charge volume of Transactions that are processed by the Network, provided that both volume amounts are in the same currency. Inbound FTG is calculated on gross Network sales volume and the Network volume of fraudulent Transactions for both individual S/Es (S/E IFTG) and multiple S/Es at the Acquirer level (Acquirer IFTG), excluding Fraudulent Applications and non-received fraud. For Issuers, the Inbound Fraud to Gross Ratio is calculated on gross billed business volume and the volume of fraudulent Transactions on their Card Accounts that are processed by the Network.
Indirect Acceptor	A payment intermediary that contracts with an Acquirer to facilitate payments to third-party End Beneficiaries. The Indirect Acceptor accepts the Card, but does not send Card information to the End Beneficiary.
Infringing Products	Includes Copyright-Infringing Products and Counterfeit Trademark Products sold over the Internet.
Installment Payment Provider	An S/E offering Cardmembers the ability to pay for purchases made at an End Beneficiary in installments over a fixed period.
Inter Center Shipment File	The file of ATM cash and POS Charge Transactions that is presented by the Acquirer to Issuers via the AEGN.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Internal Service Metric	Internal Service Metrics are objective measurements of Services that impact customer satisfaction.
International Organization for Standardization (ISO)	The international body that develops and publishes standards for industry.
Internet	The global system of interconnected computer networks that use the Internet protocol suite to link billions of devices worldwide.
Internet Electronic Delivery	Delivery, to the Cardmember, via Internet download or another file transfer process, of Digital Goods or Services purchased on the Internet or an electronic network.
Internet Physical Delivery	Delivery, to the Cardmember, via mail, shipping services, or courier to a physical address, of Goods or Services purchased on the Internet.
Introductory Offer	A free or reduced cost trial, promotion, or other similar offer for a limited period of time that allows Cardmembers to try a product or service before receiving a Charge for the regular price of the product or service.
Issuer	Any entity (including, without limitation, American Express and American Express Entities) authorized by American Express or an American Express Entity to issue a Card and to engage in the Card Issuing Business.
Issuer Declaration	An Issuer statement certifying in detail how the conditions for the Chargeback have been met.
Issuer Identification Number (IIN)	A unique 11-digit number assigned by AEGNS to an Issuer to identify Transactions belonging to that Issuer. The first 6 digits of the IIN is the Bank Identification Number (BIN).
Issuer Notification Date (IND)	The date AEGNS notifies an Issuer of its claim eligibility under CDCRP.
Issuer Originated Payment (IOP)	Transactions initiated by Cardmembers, using a payment solution provided by their Issuer to send funds to pay Service Establishments (S/Es).
Issuer Override Request	A feature available to Issuers through FraudNet that enables an Issuer to submit a request to suspend Dynamic Fraud Management decline Authorization Responses for specific Card Account Numbers during a period defined by the Issuer.
Issuer Processor Number	The unique identification number assigned by AEGNS to the designated Authorized Processor for an Issuer.
Issuer's Rate	The difference, which may be expressed as a percentage, between the face amount of a Charge and the price which the Issuer pays upon presentment of a Charge to such Issuer.
Key Encrypting Key (KEK)	A key used to protect all other keys while in transit between two trusted parties, including, but not limited to, Zone Master Keys (ZMKs) and Zone PIN Keys (ZPKs).
Know Your Customer	Know Your Customer (KYC) is the due diligence that Participants must perform to correctly identify their customers (Cardmembers and/or S/Es) in order to minimize the risk of Cards being used for money laundering or terrorist financing.
Launch Date	The date on which an Issuer issues and markets to the public (other than to one of its employees or agents) the first Card of each type of Card such Issuer is authorized to issue. The date shall follow the completion of the applicable Beta Test.
Life Cycle Management	Activities related to the ongoing management of Cardmember Account information, including updates and changes, that may have a direct impact on Transactions and digital capabilities.
Limited Use Key (LUK)	Limited use data utilized to conduct an Expresspay Mobile HCE Transaction or Digital Wallet Payment Transaction.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Limited Use Payment Credential (LUPC)	Limited-use data utilized to conduct an Expresspay Mobile HCE Transaction or Digital Wallet Payment Transaction.
Load	Adding a sum of money onto a Prepaid Card.
Local Network Card	A Card that has been issued by a Local Network Card Issuer.
Local Network Card Issuer	An Issuer, other than an Acquirer, that has been authorized to issue Local Network Cards in the Territory.
Local S/E	An S/E doing business in the Territory with which the Acquirer has executed a contract, but excluding Multinational Accounts.
Lost Ticket Application	A document completed by a Cardmember or by a travel agent on behalf of the Cardmember to request a Credit for a lost airline ticket.
Lower Consecutive Offline Limit (LCOL)	This Issuer-set parameter indicates the maximum number of consecutive offline Transactions, for the Chip Card application, allowed in a terminal with online capability.
Mail/Telephone/Internet Transactions	Transactions for which there was no face-to-face contact between the S/E and Cardmember and where the Transaction information and Card Account number were collected by the S/E through the mail, over the telephone, or via the Internet.
Marketplace	An S/E that offers their prominently branded platform (website or mobile application), for Cardmembers to browse and purchase from multiple End Beneficiaries. Cardmembers pay for their purchases on the same platform.
Master Key	A Cryptographic Key used to derive all other Encryption keys or a group of keys.
Merchant	See "Service Establishment (S/E) (aka Merchant or Card Acceptor)" on page 518.
Merchant Acquiring Business	The business engaged in by an Acquirer whereby the Acquirer: i. Recruits and acquires S/Es pursuant to contractual arrangements with such S/Es, to enable such S/Es to accept Cards as payment for Goods and Services; ii. Transfers and settles Charges and other Transactions transacted by its S/Es, which have been authorized and accepted by an Issuer; iii. Renders statements of account to its S/Es; and iv. Renders related services to S/Es.
Merchant Category Code (MCC)	A 4-digit code used to identify the industry in which the S/E is doing business.
Merchant Discount	The percentage or the portion of each Charge which S/Es are obligated to pay an Acquirer for accepting Cards.
Merchant-Initiated Transaction	A Transaction that is initiated by the S/E through use of Credentials-on-File, based on a prior agreement between Cardmember and S/E, without direct participation from the Cardmember.
Merchant Plug-In	The Merchant Plug-In is software that exists in the Acquirer domain, which is incorporated into the S/E's Web storefront. It provides functions related to SafeKey on behalf of the S/E.
Merchant-Presented Quick Response (MPQR)	A Transaction initiated by a Cardmember using the Issuer application on a Mobile Device to capture a Merchant-Presented QR Code.
Message Reason Code	Code used to describe the reason associated with a First and Final Chargeback, Retrieval Request Notification, File Acknowledgment, ATM & POS, and Reversal requests.
Minimum Chargeback Amount	The smallest monetary amount, in U.S. Dollars, that may be disputed by Participants using the Chargeback procedures as specified in the "Chargeback Policies" chapter beginning on page 280.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Mobile Device	An Issuer-approved and AEGNS-recognized electronic device (including, but not limited to, a mobile telephone, tablet, or wearable device) that is enabled to initiate digital payments. Mobile Device is also referred to as a "Mobile Proximity Payment Device (MPPD)" in some related AEGNS manuals, guidelines, and resources.
Mobile Entities	Any entity that is involved with development or deployment of Digital Wallet Programs. Examples of Mobile Entities include, but are not limited to, trusted service managers, mobile network operators, Digital Wallet Program Providers, secure element providers, host card emulation vendors, and mobile handset manufacturers.
Mobile Passcode	A form of Issuer-defined CVM optionally supported in a user interface within a Mobile Device.
Mobile Point of Sale (mPOS)	A commercial off-the-shelf (COTS) device, such as a mobile phone or a tablet, that can be used as a POS. The mPOS may use integrated Contactless or may be used in conjunction with a Card reader.
Monthly Authorization Request Volume	The average monthly volume of Authorization Requests sent to the Issuer in the preceding calendar year for existing Issuers and the average forecasted monthly volume for new Issuers.
Multinational Accounts (MNAs)	Service Establishments (S/Es) that have locations both inside and outside the Territory, requiring American Express to coordinate servicing and other customer relationship matters on a regional or global basis and being any S/Es designated as such in writing by American Express.
Net Settlement	The net amount due from or to a Participant as a direct result of all Financial Transactions cleared, accepted, and processed within the timeframe designated each day for Settlement. Net Settlement includes all Financial Messages, fees, and Issuer's/Acquirer's/Network Rate calculations made on said Transactions in accordance with contractual exhibits and AEGNS standard fee schedules.
Network	See "American Express Global Network (AEGN) or Network" on page 496.
Network Assessment Library	A series of reports that provide information on the effectiveness of the Network internal control environment and key systems utilized by and in support of Participants.
Network Fees	The amount of commission and fees Participants pay for marketing, operational, and other services provided directly or indirectly by AEGNS.
Network Floor Limit	See "Floor Limit, Network" on page 508.
Network Processing Date	The date a Transaction is accepted by the AEGN. For the purpose of Chargebacks, the Network Processing Date is day zero.
Network Rate	The difference, which may be expressed as a percentage, between the face amount of a Charge and the amount that the Acquirer receives from the AEGN for the Presentment.
Network Test Simulator	A Web-based, on-demand tool used to facilitate Phase I (unattended) testing/Certification, performed by Participants prior to obtaining full access to the AEGN.
No Show Reservation Program	A program that guarantees payment to hotel S/Es of one (1) night's rate should the Cardmember not utilize the reservation or cancel in the proper timeframe for facilities or services reserved in advance of use. This program may also be referred to as the "Assured Reservation Program."
No Show Reservation Transactions	Charges which an S/E is permitted to submit in accordance with its contract with an Acquirer which allow an S/E to recover some or all of the revenue lost when reserving facilities or Services for a Cardmember who makes advance commitment for their use but who does not utilize them. These Transactions may also be referred to as "Assured Reservation Program" Transactions.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Non-Financial Transaction	A Transaction clearing through the AEGN that does not have a direct impact to Settlement associated with the Transaction.
Offline	An operating mode in which no direct connection is made to a central computer facility.
Offline Authorization	An Authorization in which a chip-enabled Card evaluates data based upon information loaded onto the Card during the Card personalization process, and responds to the terminal with a Decline or Approval decision and a cryptogram.
Offline PIN	A form of CVM where the PIN entry is validated by the AEIPS chip and the validation results are returned to the terminal.
Online Authorization	An Authorization in which the S/E has submitted an Authorization Request to the Issuer for decisioning.
Online PIN	A form of CVM where the Acquirer sends an encrypted PIN value in the Authorization Request for validation by the Issuer.
On-Us Transaction	A Transaction where the Issuer and the Acquirer are the same entity, including ATM Transactions by an Issuer's Cardmember at an ATM in such Issuer's Participant ATM Network.
One-Time Password (OTP)	A One-Time Password (OTP) is a dynamic code provided by the Issuer to the Cardmember. Issuers may utilize OTPs at their discretion as an added source of protection against fraud, typically in the place of a PCSC for Card Not Present Transactions.
Organization Identifier	The unique identifier assigned by AEGNS to the Participant organization that is sending or receiving Outclear/Inclear files to/from the Network.
Original ROC	The ROC retained by the S/E at the time of the Transaction.
Original Transaction Identifier	A Transaction Identifier (TID) that links a Merchant-Initiated Transaction (MIT) to the Authorization Response returned by the AEGN for a Cardmember-Initiated Transaction or a Cardmember's request to store credentials.
Partial Authorization	An Authorization requested by an S/E and approved by an Issuer for a partial amount—less than the total amount of the purchase.
Participant	An entity which is an Issuer, Acquirer, or both.
Participant Agreement	The agreement between a Participant and an American Express Entity whereby such Participant is permitted to issue Cards and/or to contract with S/Es to accept the Card for purchases of Goods or Services and to transfer and settle such Charges with the Acquirer.
Participant ATM Network	The entire network of online ATMs operated by the Participant including any new ATMs which the Participant may add to such network.
Participant Communication Platform (PCP)	FraudNet functionality used to deliver notification of major fraud events to Participants. Detailed information on the FraudNet PCP system can be found in the *GNS FraudNet User Guide.*
Participant Shared ATM Network	All networks of online ATMs of banks and third parties inside the Territory that the Participant has access to or may gain access to under agreements with third-party owners or operators, other than Amex Shared ATM Network ATMs.
Payment Account Reference	Non-financial reference generated by AEGNS that is associated with a Primary Account Number (PAN). PAR can be utilized by Acquirers and their S/Es to link the PAN and associated Tokens
Payment Facilitator (previously referred to as Payment Aggregator or Payment Service Provider)	A provider of Payment Services. A Payment Facilitator is an entity that contracts with an Acquirer to provide Payment Services to other Merchants, enabling them to accept the Card. The Merchants may or may not have a direct relationship with Acquirers of American Express Global Network Services (AEGNS).

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Payment Facilitator Agreement	A Merchant Agreement between an Acquirer and Payment Facilitator containing their respective rights, duties, and obligations for participation in the Acquirer's American Express Program.
Payment Services	Payment-related service provided by S/Es in connection with Transactions between Cardmembers and Sponsored Merchants.
Payment Token	A Token that may be used to initiate payment Transactions.
Peer-to-Peer Payment (P2P)	A service offered through a payment application that enables a transfer of funds to and from its registered users. This does not include a transfer of funds with the intention of purchasing Goods or Services.
Person	An individual, corporation, partnership, trust, association, or any other legally recognized entity or organization.
Personal Identification Number (PIN)	A four (4) to twelve (12) character secret code that allows an Issuer to positively identify the Cardmember for the purpose of approving an ATM or POS Transaction.
Personally Identifiable Information (PII)	Personally Identifiable Information (PII) is any piece of information which can potentially be used to uniquely distinguish or trace an individual's identity, such as their name, date and place of birth, mother's maiden name, address, email address, personal phone number, etc., including any other personal information which is linked or linkable to an individual such as an Account number.
PIN Bypass	A program allowing a cashier or Cardmember at a chip/PIN terminal to pro-actively bypass the PIN entry to prevent high Authorization declines due to a Cardmember's inability to remember their PIN.
PIN Key	Cryptographic Keys used to protect PINs including, but not limited to, PIN Encryption Keys (PEKs) and ZPKs.
Plaintext	Understandable data, such as letters and numbers, whose meaning and context is clear to the reader (for example: a name or a street address).
Point of Compromise (POC)	An S/E from which Cardholder Data and/or Sensitive Authentication Data (Account numbers and/or magnetic stripe data) obtained from Cardmember Transactions at the S/E's location is subsequently used fraudulently.
Point of Sale (POS)	Point of Sale (POS) device has the meaning contained in the current *PCI Data Security Standard Glossary, Abbreviations and Acronyms* (refer to www.pcisecuritystandards.org), and, as of the date of this publication, it includes the following elements: hardware and/or software used to process payment Card Transactions at S/E locations.
Point-to-Point Encryption	A security standard that requires Credit Card information to be encrypted instantly upon the initial swipe or dip, and then securely transferred directly to the payment processor before it can be decrypted and processed.
Prepaid Card	A Card for which the balance amount is pre-loaded onto the Card and will be reduced as the Card is used by the Cardmember.
Prepaid Card Authorization with Balance Return	An Authorization Response by an Issuer that includes the outstanding balance on a Prepaid Card.
Prepaid Card Balance Inquiry	A request for the outstanding balance on a Prepaid Card, submitted on behalf of a Cardmember by an S/E, as part of an Authorization Request sent to an Issuer.
Prepaid Card Balance Return	An Authorization Response returned by an Issuer that includes the remaining balance on a Prepaid Card.
Prepaid Card Partial Authorization with Balance Return	An Authorization Request approved for a partial amount—up to the existing balance on a Prepaid Card but less than the total amount of the purchase, where the Authorization Response also provides the subsequent remaining balance on the Prepaid Card.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Preprinted ROC	An Acquirer-approved Record of Charge (ROC) with preprinted S/E name, number, and information for use by S/Es who cannot be supplied an Imprinter or POS device.
Presentment	The submission of Transaction data to the Network by Acquirers.
Primary Account Number (PAN)	A series of digits used to identify a customer Account or relationship. The assigned number identifies the Issuer and Cardmember Account.
Printed Card Security Code (PCSC)	A 3-digit number printed on the back of the Card (3CSC) or a 4-digit number printed on the front of the Card (4DBC/4CSC).
Product Enhancement	Products and Services sold or provided to Issuers with the assistance or consultation of AEGNS, for provision to Cardmembers as a feature of the Card.
Program Administrators	An individual or group of employees designated by a Corporate Card Client as its administrator of the overall Corporate Card program on its behalf.
Program Indicator	A field on the POS First Presentment (1240) message indicating to Issuers that the Transaction qualifies for special S/E programs or other types of programs that potentially shift liability and/or contain special operating rules.
Program Progress Reports	Reports required to be submitted by Participants on a regular basis, containing information related to their GNS Issuer and/or Acquirer Business.
Prohibited Country and Region	A country or region against which economic sanctions have been imposed by the U.S. government. Participants are prohibited from engaging in any American Express-related business with or in such countries or regions.
Promotional Program	An optional AEGN feature that facilitates marketing campaigns that drive spend and loyalty by closing the redemption loop in local S/E commerce.
Proof of Delivery	A receipt of delivery that is signed by the Cardmember or an authorized recipient at the valid address of the Cardmember.
Qualified Security Assessor	A company certified by the PCI Security Standards Council as being qualified to assess compliance to the PCI DSS standard. A list of Qualified Security Assessors recognized by the PCI Security Standards Council is available by accessing www.pcisecuritystandards.org.
Qualitative Service Assessment	A qualitative assessment of a Participant's Cardmember and/or Service Establishment customer servicing.
Quick Response (QR) Code	A two-dimensional static or dynamic machine-readable barcode containing data that can be extracted and used for a specific purpose, such as enabling a digital payment.
Real Currency	The financial currency unit issued and regulated by a national monetary authority as the sole legal tender of an internationally recognized country or monetary union, and customarily used and accepted as a medium of exchange for Goods and Services or monetary value transfer.
Recommendation Code	A 3-byte numeric value on an Eligible Transaction that corresponds to a description of the fraud risk associated with the Transaction. Refer to the *Codes Reference Guide* Fraud Indicator section for a complete list.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Record of Charge (ROC)	The receipt for a Cardmember's Charge, Credit, or ATM Transaction containing the details of any Transaction carried out at an ATM or at the POS. The form the ROC may take depends upon the method and equipment used to capture the details of the Card and Transaction and may differ from the following examples. i. It may be an imprinted form, which carries an Imprint of the raised letter and numbers on a Card, plus the handwritten Transaction information recorded by the S/E. It may include the signature of the Cardmember. ii. It may be a paper receipt printed by a POS device printer and may be signed by the Cardmember. iii. It may be the log entries made when an ATM dispenses cash. AEGNS uses the following terms to refer to a ROC: Original ROC, Substitute ROC, Transaction Log, and Copy.
Recurring Billing	The billing method for periodic Transactions for a product or service agreed to in writing by the Cardmember (e.g., membership fees to health clubs, magazine subscriptions, insurance premiums).
Refund/Exchange Notice	A Document issued by an airline or travel agent when a ticket is exchanged for another ticket and a refund is due or additional funds must be collected from the Cardmember.
Reload	Adding replacement or additional sums of money onto a Prepaid Card.
Remote Stand-In (RSI)	A Network service that provides Authorization services to the Issuer via a remote system, based on remote system parameters, when the host system is unavailable. System parameters are established by Acquirer market and include S/E and Card product limits.
Retention Period	The minimum period of time that the Acquirer or their S/E must retain either original or legible reproduction Documentation for the purposes of supporting the Settlement, Retrieval, and Chargeback processes.
Retrieval Request	The request for either an Original ROC or a legible reproduction of the ROC or other Documentation as identified in the Transaction data of the original Presentment of the Transaction.
Retrieval Request Notification	The message sent by an Issuer to request either an Original ROC or a legible reproduction of the ROC or other Documentation as identified in the Transaction data of the original Presentment of the Transaction.
Revolving Credit Card	A Card for which only a predetermined percentage or minimum amount, rather than the full amount, of the outstanding balance is required to be paid by the Cardmember each month, with interest being charged on the unpaid balance on such Account.
Rights-Holder	A natural or legal Person, or entity, having the legal standing and authority to assert a copyright or trademark right.
Risk-Mitigating Technologies	Technologies and devices approved by AEGNS and used to protect Cardholder Data and Sensitive Authentication Data by making it unreadable or unusable by unauthorized parties. These technologies may include, but are not limited to, EMV, PCI-listed P2PE solutions, P2PE solutions approved by a Qualified Security Assessor, and Tokenization.
SafeKey	The Cardmember's password utilized to authenticate the Cardmember during the American Express SafeKey Authentication process.
Second Presentment	The second time a Transaction is presented from an Acquirer to the Issuer through the Network following a First Chargeback and with additional Documentation or information refuting the Chargeback.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Secure Remote Commerce (SRC)	An E-commerce checkout capability that creates a secure and consistent Cardmember checkout experience across digital channels, including Mobile Devices, websites, and other connected devices.
Security Domain Master Key	A key used as the foundation of a security domain on customer devices (e.g., IoT, mobile, Chip Card), including, but not limited to, Chip Master Keys (CMKs) and Global Platform Domain Keys.
Self-Assessment Questionnaire (SAQ)	A self-assessment tool created by the Payment Card Industry Security Standards Council, LLC, intended to evaluate and attest to compliance with PCI DSS.
Sensitive Authentication Data	Sensitive Authentication Data has the meaning contained in the current *PCI Data Security Standard Glossary, Abbreviations and Acronyms* (refer to www.pcisecuritystandards.org), and as of the date of this publication, it includes the following elements: • Full magnetic stripe data or equivalent on a chip, or • Card Identification Number (also known as PCSC), or • PIN The Primary Account Number (PAN) is the defining factor in the applicability of the PCI DSS requirements. The PCI DSS requirements are applicable if a PAN is stored, processed, or transmitted.
Sensitive Authentication Data Key (SAD)	A Cryptographic Key used in the generation or validation of Sensitive Authentication Data (e.g., Card validation codes/values, EMV cryptograms, etc.). Sensitive Authentication Data Keys include, but are not limited to, Card Security Code Keys (CSCKs), Master Derivation Keys (MDKs), and Issuer Public Keys (IPKs).
Sensitive Authentication Data Protection Key	A Cryptographic Key used to provide confidentiality, integrity, or Authentication of SAD at rest or in transit, including, but not limited to, Base Derivation Keys (BDKs), PIN Encryption Keys (PEKs), Message Authentication Code (MAC), Data Encryption Keys (DEKs), and Zone PIN Keys (ZPKs).
Service Code	A 3-digit number used in magnetic stripe mode Transactions that specifies acceptance requirements and limitations for a magnetic stripe-read Transaction.
Service Establishment (S/E) (aka Merchant or Card Acceptor)	Any Person that has entered into a contract with an Acquirer wherein such entity agrees to: • Permit any Cardmember to charge purchases of Goods and Services at or from such entity by means of the Card, and • Transfer such Charges to an Acquirer.
Service Metric	A means to track, measure, and report monthly on Cardmember (CM) and Service Establishment (S/E) Service Performance.
Service Organization Controls 1 (SOC 1)	A report (also known as Statement on Standards for Attestation Engagements16 (SSAE16)) on controls at a service organization that is relevant to user entities' internal control over financial reporting.
Service Organization Controls 2 (SOC 2)	A report on a business' non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy.
Service Performance Online	A Web-based service used to submit monthly Service Metric Reports. This service can be found on Knowledge Base.
Service Provider	Any entity to which Cardholder Data and/or Sensitive Authentication Data is provided, including those involved in the processing, storage, transmission, and/or switching of Transaction data, Cardholder Data, and/or Sensitive Authentication Data, such as Authorized Processors, third-party processors, vendors, Mobile Entities, or their agents, representatives, or subcontractors.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Services	Useful labor that does not provide a tangible commodity and which satisfies some customer demand (e.g., telephone service, airline tickets/travel, meals, professional services).
Settlement	The process by which the Network computes the net totals that will be used for Funds Exchange between Acquirers and Issuers.
Settlement Bank	The financial institutions used by Participants and AEGNS to effect the receipt and transmission of funds on their behalf. In the case of AEGNS, this includes the unit designated by AEGNS to provide Daily Settlement Advisement to Participants.
Settlement Bank Earnings Credit Rate	The percentage a Participant pays to borrow funds.
Settlement Day	A day on which the Settlement Bank of either the Acquirer or the Issuer and AEGNS are open for business.
Split Shipment Transactions	A Split Shipment Transaction occurs when a Cardmember makes a single purchase of multiple Goods and the Goods are delivered to the Cardmember in multiple shipments.
Split Tender	The use of more than one (1) form of payment for a single purchase.
Sponsored Merchant	An S/E that enters into a Sponsored Merchant Agreement with a Payment Facilitator.
Sponsored Merchant Agreement	The standard agreement between Payment Facilitators and Sponsored Merchants that must be entered into in order for a Payment Facilitator to conduct Payment Services for Sponsored Merchants.
SRC Initiator	An SRC ecosystem role that supports checkout and/or the retrieval of Digital Card and payment data from the SRC System on behalf of a payment-enabled application.
SRC Participant	Any entity that is configured to participate in SRC. This can include entities playing the role of SRC Initiators, Digital Card Facilitators, Digital Payment Applications, or Issuers.
SRC System	A technical platform that facilitates E-commerce Transactions between Cardmembers, Digital Payment Applications, SRC Initiators, Issuers, and Digital Card Facilitators on behalf of one or more SRC programs.
Staged Digital Wallet	An S/E with a payment platform that allows Cardmembers to use a Card to fund a purchase in real time to an End Beneficiary.
Stand-In Authorization	Services offered by the Network whereby Authorization Requests are processed by the Network on behalf of the Issuer. See "Host Stand-In" on page 510 and "Remote Stand-In (RSI)" on page 517.
Standard Card	Cards that offer core benefits and services as specified by AEGNS.
Standard Functionality	The minimum product functionality required of Participants to qualify for the mid-sized and large national Corporate client segment.
Static Token	A Token that may be used across multiple Transactions completed with a unique PAN.
Strong Customer Authentication	Transaction Authentication involving at least Two Factor Authentication (2FA), where a breach of one (1) factor does not compromise the reliability of others. Factors include: • Knowledge: Something known only to the user (e.g., PIN) • Possession: Something the user possesses (e.g., Card) • Inherence: Something the user is (e.g., biometrics)

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Stored Value Digital Facility (SVDF)	An S/E-offered feature that allows funds to be loaded into a digital wallet for subsequent payments. This includes purchases of Goods and Services at single or multiple payment acceptors.
Submission Frequency	The maximum number of days that transit Transactions can be aggregated before submission is required.
Substitute ROC	A copy of the Original ROC created from the data captured for the Transaction. The Cardmember signature is not included unless it was electronically captured at the POS.
Supplementary Cardmember	A Cardmember who is issued a Card based upon an Account established by another Cardmember, at the request of that other Cardmember. Supplementary Cardmembers may also be referred to as "additional Cardmembers."
SWIFT	SWIFT (Society for Worldwide Interbank Financial Telecommunication) is the industry-owned co-operative supplying secure, standardized messaging services and interface software to nearly 8,000 financial institutions in 206 countries and territories.
Swiped Transaction	A Card Present Transaction initiated by "swiping" the Card's magnetic stripe through a POS device's Card reader.
System Outage	Interruption of network systems services due to a computer system failure, telecommunications failure, or regularly scheduled downtime.
Tax Withheld Date	The date on which taxes have been withheld from fees and assessments due to an American Express Entity under the Participant Agreement, in accordance with applicable law in the Participant's Territory.
Territory	The geographic area where the Participant has been authorized by an American Express Entity to conduct the Card Issuing and/or Merchant Acquiring Business.
Token	A surrogate value that replaces the PAN.
Token Assurance Level	A value determined as a result of the ID&V process that provides a confidence level as to the Token-to-PAN binding.
Token BIN Range	A specific BIN range assigned only for the purpose of issuing Tokens.
Token Domain	A set of rules that define the types of Transactions for which a Payment Token may be used.
Token Domain Restriction Controls	Token Domain-related controls established based on information made available to the TSP during the Token Requestor registration process.
Token Generation	The process of creating a Token based on a unique PAN.
Token Life Cycle Management	Activities related to the ongoing management of Tokens and existing business-as-usual processes throughout the Transaction Life Cycle.
Token Mapping	The process of assigning a Token to the original PAN.
Token Request	The process by which a Token Requestor submits a request to a Token Service Provider for a Token.
Token Requestor	An entity that initiates requests that PANs be tokenized, by submitting Token Requests to a Token Service Provider.
Token Requestor ID (TRID)	An 11-byte code pairing Token Requestor with Token Domain.
Token Service	A system that comprises the key functions that allow for Token Generation, Token Mapping, establishing of a Token Assurance Level, and all processes needed to support the processing of Tokens, including De-tokenization, throughout the Transaction Life Cycle.
Token Service Provider (TSP)	An entity that provides a Token Service.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Token Vault	A repository for the Token-to-PAN Mapping as well as other attributes required during Transaction processing.
Tokenization	The process by which the PAN is replaced by a surrogate value called Token.
Total Fraud to Gross (FTG)	The ratio of all fraudulent Transactions as compared to total charge volume, provided that both volume amounts are in the same currency. FTG is calculated on total gross sales volume and the total volume of fraudulent Transactions for both individual S/Es (S/E FTG) and multiple S/Es at the Acquirer level (Acquirer FTG), excluding Fraudulent Applications and non-received fraud. For Issuers, the FTG is calculated on total gross billed business volume and fraudulent Transaction volume on their Card Accounts.
Transaction	A Charge, Credit, Cash Advance (or other cash access), or ATM Transaction completed by the means of a Card.
Transaction Certificate	A digital signature comprised of Issuer-selected data objects, generated by the Chip Card during the Transaction Authorization process. The Transaction Certificate enables the Issuer to verify that critical chip data was not changed prior to Card validation.
Transaction Date	The date the Cardmember and S/E completed the Transaction or the date the Cardmember completed the Transaction at an ATM. For telecommunication Transactions, it is the date of Presentment of the summary bill. For Mail/Telephone/Internet Transactions, it is the date the Goods are shipped.
Transaction Identifier	A unique number assigned by the Network or Authorization system which identifies a Cardmember Transaction throughout its life cycle.
Transaction Life Cycle	The steps involved in processing Charge or Credit Transactions as viewed from the perspective of the AEGN.
Transaction Log	An electronic record of the details of a Charge or Credit Transaction residing on a Network, Acquirer, or Issuer system.
Transit Access Terminal (TAT)	An Expresspay-enabled POS Device that, when "tapped" by an authenticated Expresspay Card, allows the Cardmember access to the transit system.
Transport Layer Security (TLS)	Transport Layer Security (TLS) is a security protocol that allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint Authentication and communications privacy over the Internet using cryptography. TLS can be used to create a secure communication channel between mail servers. When devices such as mail servers communicate, TLS ensures that no third party may eavesdrop or tamper with the message.
Transportation Refund Credit Notice	A document issued by an airline or travel agent that indicates a Credit may need to be issued for a ticket. Transportation Refund Credit Notices are not acceptable Documentation of a Credit issued by an S/E nor of a Cardmember's right to a Credit.
Triple Data Encryption Algorithm (TDEA)	A block cipher which applies the Data Encryption Standard (DES) cipher algorithm three (3) times to each data block with at least two (2) different keys.
Two Factor Authentication	A two-step method of confirming a user's Authentication of a Transaction using two (2) Authentication methods (or factors).
U.S. Domestic	A situation in which a U.S. issued Card is used at a U.S. acquired Service Establishment.
U.S. Multi-Network Debit Cards	A Debit Card that is a "debit card" as defined in Federal Reserve Board Regulation II, 12 CFR Part 235.
U.S. Multi-Network Prepaid Cards	A Prepaid Card that is a "debit card" as defined in Federal Reserve Board Regulation II, 12 CFR Part 235.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Table 14-1. Definitions (continued)

Uniform Resource Locator (URL)	An address to an object, document, or page or other destination (for example, a newsgroup or a World Wide Web page) on the Internet or an intranet. A URL expresses the protocol (such as FTP or HTTP) to be accessed and where the destination is located. A URL may also specify an Internet email address.
United States or U.S.	The fifty (50) states of the United States of America and the District of Columbia.
United States Territories	AEGNS includes the following as United States Territories: American Samoa, Northern Mariana Islands, Guam, Puerto Rico, U.S. Virgin Islands, U.S. Minor Outlying Islands.
User Certification Contact	A Participant representative who is responsible for validating IDs and permissions against those IDs for their employees and contractors who have access to American Express systems.
Valid Billing Unit Code (VBU Code)	The Valid Billing Unit Code indicates the specific purpose for the fee being charged.
Valid Date Range	The period of time during which a Card is valid between and inclusive of the earliest effective date and latest effective date when both appear on the Card. If only an Expiration Date appears on the Card, then any date up to and including the Expiration Date.
Value-Added Tax (VAT)	An incremental excise that is levied on the additional value at each stage of the processing of a raw material or the production and distribution of a commodity and that typically has the impact of a sales tax on the ultimate consumer.
Virtual Currency	A financial currency unit not issued by a national monetary authority as the sole legal tender of an internationally recognized country or monetary union. Virtual Currencies may be accepted as a medium of exchange or monetary value transfer between two (2) or more individuals or entities but may not have all the attributes of a Real Currency.
Voice Authorization Request	The process by which an S/E telephones its Acquirer's Authorization center for Transaction Authorization, usually used by S/Es which lack access to or use of electronic Authorization POS terminals.
WINTER (WINdow To Early Referrals)	A FraudNet application that allows Issuers to view Eligible Transaction details including Fraud Probability Score and Recommendation Code.
Worldwide Fraud Information System (WFIS)	The American Express fraud reporting database used by Participants to manually enter S/E and Cardmember fraudulent Transaction data.

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Index

Numerics

3CSC 264, 265, 400, 470, 471, 517
  acronym 491
  optional host stand-in 258
4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented, see under *Chargeback(s), reasons*
4512 - Multiple Processing, see under *Chargeback(s), reasons*
4513 - Credit Not Presented, see under *Chargeback(s), reasons*
4515 - Paid Through Other Means, see under *Chargeback(s), reasons*
4516 - Request for Support Not Fulfilled, see under *Chargeback(s), reasons*
4517 - Request for Support Illegible/Incomplete, see under *Chargeback(s), reasons*
4521 - Invalid Authorization, see under *Chargeback(s), reasons*
4523 - Unassigned Cardmember Account Number, see under *Chargeback(s), reasons*
4527 - Missing Imprint, see under *Chargeback(s), reasons*
4530 - Currency Discrepancy, see under *Chargeback(s), reasons*
4534 - Multiple ROCs, see under *Chargeback(s), reasons*
4536 - Late Presentment, see under *Chargeback(s), reasons*
4540 - Card Not Present, see under *Chargeback(s), reasons*
4544 - Cancellation of Recurring Goods/Services, see under *Chargeback(s), reasons*
4553 - Not as Described or Defective Merchandise, see under *Chargeback(s), reasons*
4554 - Goods and Services Not Received, see under *Chargeback(s), reasons*
4750 - Car Rental Charge Non-Qualified or Unsubstantiated, see under *Chargeback(s), reasons*
4752 - Credit/Debit Presentment Error, see under *Chargeback(s), reasons*
4754 - Local Regulatory/Legal Dispute, see under *Chargeback(s), reasons*
4755 - No Valid Authorization, see under *Chargeback(s), reasons*
4763 - Fraud Full Recourse, see under *Chargeback(s), reasons*
4798 - Fraud Liability Shift - Counterfeit, see under *Chargeback(s), reasons*
4799 - Fraud Liability Shift - Lost/Stolen, see under *Chargeback(s), reasons*
4CSC 258, 265, 517
  acronym 491
  optional host stand-in 258
4DBC 265
  acronym 491
5CSC 264, 393
  acronym 491
  mandatory host stand-in 258

A

acceptance restrictions, Card 214
accommodations, alternate lodging 230
Account Data 38, 43
  definition 496, 505
Account setup, Issuer 206
Acquirer
  ATM Authorization 266–268
    systems 267
  Authorization standards 253
  CAPK Key Management Life Cycle 116
  CAPK Management Life Cycle 104
  Communication Platform 390
  compliance requirements 45
  Urgent Investigation Request (UIR) 389
Address
  Good Faith Submission 366
  Verification 250, 399
  Verification Automated 262
  Verification Services 261
  Zip Code Verification (ZCV) Program 357
Address Verification 250
Advance
  cash 210, 502
  emergency cash 196
Advance Deposit or Payment Program 231
  alternate accommodations 231
  cancellation policy disclosure 231
  definition 496
  reservation policy disclosure 231
AEGNS Security Risk Assessment 58
AEIPS
  Transactions and Retrieval Requests 288
AEIPS and Expresspay Cryptogram Validation Service 398
Affinity Card
  Agreements 203
  definition 497
  discriminatory treatment 215
  See also Co-Brand Card
Agreement
  access to Amex Shared ATM Network 408, 498
  AEGN Manuals 9
  arbitration rebuttal documentation accuracy 375
  between AEGN Acquirer and lodging S/Es 229–231
  between Card Issuer and American Express 448
  car rental 294, 296, 342

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Cardmember 207
Co-Brand and Affinity cards 203–205, 215
dispute deadline extension 24
Good Faith, between Acquirer and Issuer 365
Guaranty 449
Independent Operator
between GNS and Participant 435
Participant to ensure third-party confidentiality compliance 429
Lease/License, GLOBE
insurance fees 407
local Acquirer, Chip Card Fallback 247
Participant 22, 24–25, 28, 81–82, 108, 109, 117, 118, 120–122, 125, 251, 278, 408, 515, 521
one-year flat-fee servicing and pre-arranged work support 406
with AEGNS 269
with American Express, licensing agreement 431, 441
with GNS 429, 430, 439
S/E 86–93, 391
cancelled by Acquirer for derogatory reasons 388
Sponsored Merchant 520
termination due to non-compliance 35
third party 114
alternative dispute resolution 24, 26
American Express
relationship to AEGNS 1
American Express Enterprise Line Card, see under *Card*
AML, see *Anti-Money Laundering*
Annual EMV Attestation
definition 498
Anti-Corruption Laws 37
anti-corruption requirements 35
Anti-Money Laundering 84, 110
cash disbursements 33
general requirements 31
requirements
non-reloadable Prepaid (Gift) Cards 35
reloadable Prepaid Cards 35
Anti-Terrorist Financing 84, 110
general requirements 31
requirements
non-reloadable Prepaid (Gift) Cards 35
reloadable Prepaid Cards 35
Arbitration
Case 285
filing fees for 403
archival storage
ROC 103
assessments on fees 28
ATF, see *Anti-Terrorist Financing*
ATM
access 242
Acquirer Authorization Services
message content 267
systems 267
Authorization
end-to-end process 266
Requests 268
Responses 268
Card
acceptance 243
capture 243
cash access
provided by Issuer 210
via American Express Network 210
via shared network 210
Exception/First Presentment and Reversal form 476
Fulfillment data requirements for ATM Transactions 299
locations 244
Network, access to American Express 6
requirements 241
service
delivery 243
fees 408
Transaction
Authorization 247
Log archival storage 243
processing 242
routing 6
ATM optional services 211
ATM PIN Management 211
ATM security picture request 243
ATM Services 211
Attestation of Compliance 41
audit rights 26
Authorization
Acquirer standards
cancelled S/E 253
hours of operation 253
system outages 253
system standards 253
ATM
Requests 268
Responses 268
Chargeback types 304
Chip Card 254
Issuer requirements
hours of operation 251
message routing 252
Key Entered 254
log records 247
Magnetic Stripe 254
message routing
for Chip Cards 252
online request 245
online response 245
POS requests
Automated Address Verification 262
Card Not Present 254
Card Present 254
deferred payment plan 263

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

online 245
voice 255
processing 245
remote Stand-In 258
Request Responses
POS online 255
responses 255
services
activity logging 247
authorization log records 247
currency conversion 250
hours of operation 250
POS Transactions 247
reporting 251
Stand-In 251
System Outages 251
Stand-In 9
remote 258
Transaction routing 7
Authorization Adjustment 249
definition 499
Authorization Fraud Control Questionnaire
definition 499
Authorized Processors
compliance 82
use of 80, 81–82
Automated
Address Verification 262
Funds Exchange
AFE (Automated Funds Exchange) 273
Good Faith submission 367
good faith submission 367
Referral Handling 251
Automated Teller Machine, see *ATM*

B

bank holidays
Clearing 272
Settlement 275
Benefit Agreement 473
Benefit Description Form 473
Benefit Provider 473
benefits
American Express sourced 213
Benefits Participation 473
benefits, Cardmember additional 212
billing, Issuer provided 206
BIN Blocking 7, 250
services 7
blocking
BIN 7, 250
cancelled Recurring Billing Transactions 9
PIN 45
Blue Box Line, see under *Card*
Blue from American Express 126, 148
Books of Account 13
Brand Protection 97–100
Brand Protection Assessment 99
definition 500
correcting violations 99
data quality 100
definition 500
fees 413–414
Illegal or Brand Damaging Activity 97–98
definition 511
investigations 99
reporting violations 98
Supplemental Brand Protection Assessment 100
verification of legality 99

C

cameras, ATM security picture request 243
cancellation
of Recurring Goods/Services, ISO 4544 333
policy disclosure 231
Capital Damages to Rental Vehicles
Charge Submission Requirements 228
Documentation 228
capitalization in this manual 1
CAPK
Key Management Life Cycle 104
Acquirer 116
Expiry Date 104, 116
Issuer 104, 116
Management Life Cycle
Acquirer 104
capture
ATM Card 243
card 239
tax invoice 202
car rental
additional data required for 296
charge amounts for 227
Charge Non-Qualified or Unsubstantiated, ISO 4750 342
insurance 191
ISO charge non-qualified or unsubstantiated 342
Card
acceptance
procedures, S/E 214
restrictions (S/E) 214
S/E process 102
American Express Enterprise Line
advertising and marketing review requirements 18
definition 497
American Express Enterprise Line Card
Co-Brand program 203
commercial products 127, 152
consumer cards 126
corporate products 161
Issuer prerequisites 145
minimum features and benefits 145
travel agency service 192

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Blue Box Line
advertising and marketing review requirements 18
American Express Debit Card 126
Black American Express Card 126
Co-Brand program 203
commercial products 128
consumer cards 126
Max American Express Card 126
capture, ATM 243
Debit
BIN file 8
delivery
precautions against mail theft 379
preparation 379
return of undeliverable Cards 380
discriminatory treatment on acceptance 215
Personal 190
portfolio transfer 118
pricing, Issuer provided 207
production 376–379
production by Issuer 207
required features and benefits
Cardmember loyalty programs
rewards program 192
retail programs
theft and damage protection 201
warranty protection 201
Security 392
Cardmember Risk Management 393
suspect 238
validity period 207
Card Security Code (CSC) 258
acronym 492
definition 501
feature 264
key 258
validation 111
Version 2.0 algorithm 266
Cardholder Data Compromise (CDCRP) 49, 52
Cardholder Verification Method (CVM) 263
acronym 492
Cardmember
additional benefits 212
agreement provided by Issuer 207
customer service 192, 209
Dispute Chargeback types 305
information 89, 447
loyalty programs
cash rebate reward program 192
reward program 192
values program 192
monitoring ??–397
recurrent Fraud 396
remittance 408
suspect 239
Cardmembers
Eligible 473
cash
access
Issuer provided 210
advances, Issuer provided 210
awards 240
disbursements 210, 240, 251, 356
anti-money laundering requirements 33
issuer requirements 114
requirements for Acquirers 103
rebate rewards program 192
CATs (Customer Activated Terminals) 224
Central Rating and Underwriting Team (CRU) 11
definition 502
certification
Network infrastructure 14
change bars 1
changes to policy 1
charge amounts, estimated for
lodging 227
restaurants 228
charge ROCs, completing 236
Chargeback(s)
Compliance
Fees 403
counterfeit Card restriction 305
Final 284
definition 509
First 283
definition 509
format description 307
Fulfillment data requirements
airline industry 296
ATM Transactions 299
car rental industry 296
communication industry 298
lodging industry 297
regardless of industry 295
restaurant industry 298
Fulfillment Notification reason codes 293
Itemized Documentation Codes 294
overview 280
Policy rules 304
reasons
4507 - Incorrect Transaction Amount or Primary Account Number (PAN) Presented 309
4512 - Multiple Processing 312
4513 - Credit Not Presented 313
4515 - Paid Through Other Means 317
4516 - Request for Support Not Fulfilled 318
4517 - Request for Support Illegible/Incomplete 320
4521 - Invalid Authorization 322
4523 - Unassigned Cardmember Account Number 326

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

4527 - Missing Imprint 327
4530 - Currency Discrepancy 328
4534 - Multiple ROCs 329
4536 - Late Presentment 330
4540 - Card Not Present 331
4544 - Cancellation of Recurring Goods/Services 333
4553 - Not as Described or Defective Merchandise 335
4554 - Goods and Services Not Received 338
4750 - Car Rental Charge Non-Qualified or Unsubstantiated 342
4752 - Credit/Debit Presentment Error 344
4754 - Local Regulatory/Legal Dispute 345
4755 - No Valid Authorization 346
4763 - Fraud Full Recourse 349
4798 - Fraud Liability Shift - Counterfeit 351
4799 - Fraud Liability Shift - Lost/Stolen 353
Retrieval Request and Fulfillment, Notification Reasons 288
Retrieval types 304
routing and processing 7
Chip Card
acronyms associated with 493
AEIPS transactions and Retrieval Requests 288
AEIPS-Based Payments 132
Authorization 254
Authorization Request 281
Authorization Response 282
Chip Card special handling 355
definitions associated with 503, 505, 513, 515
Fallback 246
AEIPS fraud liability shift 361
Fallback floor limits 261
Final Chargeback 284
ISO 4507 - Incorrect Transaction Amount Presented 309
ISO 4521 - No Valid Authorization 322
ISO 4523 - Unassigned Cardmember Account Number 326
ISO 4527 - Missing Imprint 327
ISO 4755 - No Valid Authorization 346
process timeframes 303
requirements 104
Retrieval Request 282
Special Handling 355
classifications
S/E 102
Clearing and Settlement
clearing procedures
bank holidays for clearing 272
cancelled S/E submissions 271
cutoff schedules 271
financial life cycle 272
for Card Transactions 7
message inclearing 271
message order 270
message outclearing 271
message type 270
outages, scheduled 271
processing times 272
scheduled outages 271
submission process 270
overview 269
Transaction Life Cycle 269
Co-Brand Card
acceptance requirements 205
advertising standards and Card design 205
approval of Participants 204
definition 503
discounts on purchases 215
ownership and control 203
program 203
collections
Issuer provided 206
Commercial off-the-shelf (COTS) 38, 41, 503
compelling evidence
ISO 4540 - Card Not Present 301
ISO 4554 - Goods and Services Not Received 302
Compelling Evidence, Second Presentment Responsibility 301
Compliance
case 285
legal by Issuer 209
S/E validation requirements 42
compliance
for Authorized Processors 82
conducting business on Network
AEGNS assistance prior to 14
confidentiality 419
confidentiality obligations
for processors 82
connectivity to AEGNS 420
conversion rate, foreign exchange 274
Cost of Funds 277
definition 504
COTS, see *Commercial off-the-shelf (COTS)*
counterfeit Card Chargeback restriction 305
countries
prohibited 36
restricted 36
Credit ROC Not Presented, ISO 4513 313
Credit ROCs, completing 236
CRU, see *Central Rating and Underwriting Team (CRU)*
cruise lines
estimated charge amounts for 227
Cryptographic Key 44, 207
definition 504
Cryptoperiod
definition 504
CSC, see *Card Security Code (CSC)*
Cumulative Spend Protection Threshold 219, 323, 346, 349, 504

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

currency
  conversion services 7
  conversion, Authorization 250
  discrepancy, ISO 4530 328
  restrictions, Funds Exchange 278
Customer Activated Terminals (CATs) 224
customer screening program 32–33
  certification 33
  non-compliance 33
customer service, Issuer provided 209

D

Daily Activity process 273
Daily Settlement Advisement
  delay in 276
Data Compromise 39, 44, 46–49
Data Elements for Payment Facilitators 91
Data Elements for Sponsored Merchants 93
Data Security
  Cardholder Data Compromise (CDCRP) 49, 52
Data Security Policy 38, 412
Debit Card
  BIN file 8
  BIN range 131
Debit Cards
  Acquirer responsibilities 131
Decipher
  definition 505
Deferred Payment Plan 263
  (DPP) 250
De-tokenization 56
Digital Capabilities Enablement 52
  On-Behalf-Of Services 52
Digital Wallet
  Application-initiated Transactions 63
  Contactless-initiated Transactions 63
  MST Transactions 63
  Payment Cryptogram Validation 62
Digital Wallet Payments 63
Digital Wallet Programs 57–64
discounts on purchases at POS 215
display guidelines
  for website information 101
dispute(s)
  allowable codes for ATM dispute-related messages 355
  Cardmember Dispute Chargeback types 305
  fees 284, 402–403
  Funds Exchange dispute process 277
  Global Disputes Monitoring Program (GDMP) 29–30
  handling of disputed Transactions 281
  resolution
    alternative 24, 26
distribution of materials 2
Documentation
  Codes, Itemized 294
Domain Name System (DNS) 420
Double Byte Character (DBC) Support 279
Dynamic Data Validation 53
Dynamic Fraud Management (DFM) Network
    Services 394, 483
  definition 507
Dynamic Fraud Management Network Services
    (DFMNS) 400, 483
dynamic key exchange 45
Dynamic Tokens 54

E

ECR, see *Emergency Card Replacement (ECR)*
effective date of policies 1
Eligible Transaction 395, 483, 484
  definition 507
Emergency Assistance 196
Emergency Card Replacement (ECR) 196
EMV data
  processing 398
  validation 62
EMV-to-Magstripe Processing 62
Encipher
  definition 507
Encryption
  algorithm 432, 434, 442, 443
  data security requirements 44–46
  definition 507
end-to-end
  ATM Authorization process 266
  Chip Card Offline Authorization process 246
  Online Authorization process 245
English
  official language 2
Exception File
  batch file submission 8
  description 8
  uses 260
Exception, written request 124
exchange controls, Funds Exchange 278
expiration
  Participant agreement 121, 122
Expiry Date
  CAPK Key Management Life Cycle 104, 116
Expresspay 358
  acceptance 217
  Authorization 254
  Contactless Card 132
  cryptogram validation service 62
Expresspay Application 130, 254
  definition 508
Expresspay Mobile 104
  Beta Test 111
  Launch Date 111
  requirement 116

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Expresspay Mobile Transaction 254
  definition 508
Expresspay Transaction 104, 217–219, 323, 346, 349, 358
  allowable codes for 358
  valid Retrieval Request Notification Message Reason Codes for 290
Expresspay-enabled POS Device 105, 130, 217, 358
  definition 509

F

fees
  5CSC Program Non-Compliance 406
  additional Cardmember benefits and services 408
  Arbitration Filing 403
  ATM service 408
  Brand Protection 413–414
  Cardmember remittance 408
  Chargeback Arbitration filing 403
  Chargeback Compliance filing 403
  Data Security Policy 412
  dispute(s) 402–403
    Arbitration 403
    Compliance 403
    dispute Transaction 284, 403
    Good Faith 403
    Network Disputes Manager License 402
    pre-Arbitration and pre-Compliance processing 402
  Fee Schedule A
    violations 405
  FraudNet 406
  Funds Exchange reissue 409
  GLOBE 407
  GLOBE relocation 407
  Internet Virtual Private Network (VPN) 407
  late Settlement 409
  manual funds exchange processing 409
  Network Test Simulator 408
  non-compliance 412
  pre-Arbitration 402
  pre-Compliance 402
  Product Enhancement Service 408
  reporting 414
  security and fraud investigation service 406
  Settlement Advisement 409
  taxes on 28
filing fees
  Arbitration 403
  Compliance 403
financial
  safety and soundness of Participants 13
financial life cycle, Clearing and Settlement 272
Floor Limits
  alphabetical by country 486
  Chip Card Fallback 261
  S/E 102
foreign exchange
  conversion rate 274
foreign tax withholding
  requirements 28
Fraud
  5CSC Program Non-Compliance fees 406
  Chargeback
    types 285, 305, 404, 410
  communication platform 390, 397
  counterfeit Card Chargeback restriction 305
  data
    entry 384
    entry requirements 305
  investigation
    of S/Es, AEGNS 391
    service fees 406
  Liability Shift - Counterfeit, ISO 4798 351
  Liability Shift - Lost/Stolen - ISO 4799 353
  Penalty Fee Schedule A 404
  prevention 238
  prevention assistance 9
  Probability Score 395, 483
  recurrent, Cardmember 396
  risk
    monitoring, AEGNS 384
  suspect
    Cards 238
  to Gross Performance criteria 387
  to Gross Sales Volume ratio 385, 387
Fraud Full Recourse
  ISO 4763 349
Fraud Liability Shift (FLS) 360–363
Fraud Risk Services 397
Fraud Score
  definition 509
Fraud Scoring 250
FraudNet 395
  Issuer Override Request 395
  Participant Communication Platform 390, 397
FraudNet License Fees 406
Fulfillment 282
  data requirements
    airline industry 296
    all industries 295
    ATM Transactions 299
    car rental industry 296
    communication industry 298
    lodging industry 297
    restaurant industry 298
  description 282
  reason codes, notification 293
  Retrieval Request and 288
Funds Exchange
  delays 277
  dispute process 277
  Process 273
  process
    foreign exchange conversion rate 274
  Settlement and 9

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

G

GDMP, see *Global Disputes Monitoring Program (GDMP)*
general policies 11
general requirements
  AML 31
  ATF 31
Global Disputes Monitoring Program (GDMP) 29–30
  acronym 493
  definition 510
GLOBE
  fees 407
  general requirements 423
  insurance 422, 423
  relocation fees 407
  requirements 421
  returns 423
  risk of loss 422
  terms and conditions 421
Goods and Services Not Received, ISO 4554 338
Gross Fraud Rate 397, 483
  definition 510
Guaranty Agreement 449

H

HCE, see *Host Card Emulation (HCE)*
holidays
  bank 272
  Settlement bank 275
Host Card Emulation (HCE) 66–69
  certification of HCE products 69
  definition 511
Host Stand-In 257
hours of operation
  Acquirer Authorization standards 253
  Authorization services 250
  Issuer Authorizations 251

I

iCSC, see *Integrated Circuit Card Security Code (iCSC)*
identification, acceptable forms of 226
Incorrect
  Transaction Amount Presented, ISO 4507 309
IND, see *Issuer Notification Date (IND)*
Indirect Acceptors 74
in-person charges, S/E procedures for 216
installment sales, S/E 226
insurance
  car rental 191
  GLOBE 422, 423
Integrated Circuit Card Security Code (iCSC) 111, 115, 258, 264, 266, 501
  acronym 493
  program 393
    non-compliance fees 406
  validation 399
interface requirements 416
Internet Virtual Private Network (IVPN)
  fees 407
Internet Virtual Private Network (VPN)
  connections 424
investigations service fees 406
IOP, see
ISO Reason Codes, see *Chargeback(s)*
Issuer
  Authorization requirements
    hours of operation 251
    message routing 252
    system outages 252
  CAPK Key Management Life Cycle 104, 116
  Card Account services provided by
    Account setup and plastic issuance 206
    billing and collections 206
    Card production 207
    Card validity period 207
    Cardmember agreement 207
    collections 206
    legal compliance 209
    plastic issuance 206
    pricing 207
    risk assessment 209
  Communication Platform 397
  compliance requirements 45
  core Card services provided by
    cash access
      advances 210
      at Issuer's branch locations 210
      PIN issuance 210
      via American Express ATM Network 210
      via ATM network 210
      via shared ATM network 210
    customer service 209
    emergency assistance 196
  Urgent Investigation Request (UIR) 396, 405
Issuer Notification Date (IND) 50
  acronym 493
  definition 512
Issuer Originated Payment
  MPQR 72
Issuer Override Request
  fraud Liability 395
Issuer Override Request (IOR) 483
Issuers
  Network processing requirements for U.S. and Canadian Issuers 120
Itemized Documentation Codes 294
IVPN 416, 419

K

key contacts
  for Participants 22
key exchange 45
Key-Entered Authorization 254
Know Your Customer (KYC) 31

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

L

Late Presentment, ISO 4536 330
launch
  AEGNS assistance prior to 14
legal disclaimer
  Stand-In processing 261
Life Cycle Management (LCM) 52
Limited Use Payment Credentials (LUPC) 53
Local Regulatory/Legal Dispute, ISO 4754 345
lodging
  alternate accommodations 230
  cancellation 229
  estimated charge amounts for 227
  reservation 229
log records, Authorization 247
Loyalty Program 473

M

Magnetic Stripe Authorization 254
Mail/Telephone/Internet Charges and "Missing Imprint"
    Charges, S/E procedures 217
Management Information System (MIS)
  description 9
manuals, related AEGN 3
mapping services 62
Marketing Assistance 473
marketing, advertising, public relations 16, 108, 117
Merchant acquiring business
  requirements for conducting 83
Merchant-Presented QR Code 72
Merchant-Presented Quick Response
  Issuer Originated Payment 72
message
  content, ATM Acquirer Authorization 267
  inclearing 271
  order 270
  outclearing 271
  POS online response 255
  reason codes, Second Presentment 300
  routing
    Issuer Authorizations 252
  type, submission of 270
MIS (Management Information System) 9
Missing
  Imprint, ISO 4527 327
MNA, see *Multinational Account (MNA)*
Mobile Device 114, 282, 358, 376, 396
  Card Present Authorization 254
  Expresspay
    acceptance 217
    Authorization 254
Mobile Passcode
  definition 514
Mobile Proximity Payment Device
  Online Authorization process 245
Monthly Authorization Request Volume
  definition 514
MPQR, see *Merchant-Presented Quick Response (MPQR)*
Multinational Account (MNA) 88
Multiple Processing, ISO 4512 312
Multiple ROCs, ISO 4534 329

N

Name and Address Verification Program
  Issuer requirements 262
  NAV 262
  S/E requirements 262
NAV
  Name and Address Verification Program 262
Network
  acceptance, Service Establishment 9
Network Disputes Manager
  ATM security picture request 243
Network Fees, see *fees*
Network Floor Limits, see *Floor Limits*
Network infrastructure certification 14
Network Participant Updates 2
Network services
  ATM Network 6
  ATM Transaction routing 6
  Authorization Transaction routing 7
  BIN Blocking 7
  Chargeback routing and processing 7
  clearing 7
  currency conversion 7
  Exception file 8
  fraud prevention assistance 9
  Funds Exchange 9
  Management Information System 9
  policy and technical manuals 9
  Service Establishment Network acceptance 9
  Settlement and Funds Exchange 9
  Stand-In Authorization 9
Network Test Simulator, fees 408
No Show
  Reservations Program 229
No Signature/No PIN Program 232
No Valid Authorization
  ISO 4521 322
  ISO 4755 346
notification
  system outages 267

O

official language
  English 2
offline
  Chip Card Authorization process 246
One-Time Password (OTP) 266
  definition 515

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

ongoing eligibility requirements
for Participants 12
Online
Authorization end-to-end 245
online
Authorization Request 245
Authorization Response 245
Online PIN Certification and Enablement Program 234
OTP, see *One-Time Password (OTP)*
outages
notification of scheduled 252
notification of unscheduled 252
scheduled for Clearing and Settlement 271
System 251
outclearing message 271

P

paid placement 21
paid search 21
Paid Through Other Means, ISO 4515 317
PANDA, see *Pre-Authorization Network-based Dynamic Authentication*
parameter table
single charge Stand-In 465
velocity based Stand-In 468
Participant
Agreement 395
agreement
expiration/termination 121, 122
Communication Platform 390, 397
general eligibility requirements 11
minimum requirements 11
Participant Books of Account 13
Payment Account Reference 70
Acquirer Requirements 70
Payment Card Industry Data Security Standard 38, 39
Payment Card Industry Data Security Standard (PCI DSS) 39, 40, 41, 236, 237, 517
acronym 494
Payment Card Industry Payment Application Data Security Standard 38
Payment Card Industry PIN Security Requirements 38
Payment Card Industry PIN Security Standard Requirements 38
Payment Card Industry PIN Transaction Security 38
Payment Card Industry PIN Transaction Security, Point-of-Interaction 38
Payment Card Industry Secure Software Lifecycle 38
Payment Card Industry Secure Software Standard 38
Payment Tokens 54
PCI Assessment and Reporting Relief program 39
PCI DSS
Attestation of Compliance 41
PCI DSS, see *Payment Card Industry Data Security Standard (PCI DSS)*
PCI P2PE 39, 40, 41
PCI PA-DSS 39, 40
PCI PA-DSS, see *Payment Card Industry Payment Application Data Security Standard*
PCI PIN Security Standard Requirements 45
PCI Prioritized Approach Template 43
PCI PTS POI 38, 39, 40, 41
PCI PTS, see *Payment Card Industry PIN Transaction Security*
PCI Secure SLC 39, 41
PCI Secure SLC, see *Payment Card Industry Secure Software Lifecycle*
PCI SSS 39, 41
PCI SSS, see *Payment Card Industry Secure Software Standard*
PCP (Participant Communication Platform) 390, 397
Personal Identification Number (PIN)
Authorization process 268
issuance 210
Personally Identifiable Information (PII) 419, 437, 446, 516
PIN Entry on COTS 39, 40
PIN Management 211
PIN, see *Personal Identification Number (PIN)*
plastic issuance, Issuer 206
Platform 473
Point-to-Point Encryption 39
policy
effective date of 1
general 11
portfolio
transfer of 108
POS
online response messages 255
Transaction Authorization 247
POS Online PIN Certification and Enablement Program 234
pre-Arbitration
Fees 402
Pre-Authorization Network-based Dynamic Authentication (PANDA) 62
pre-Compliance 285
Fees 402
Prepaid Cards
AML/ATF Requirements 34
reloadable 35
Presentment 282
Second 283
press releases 22
Printed Card Security Code (PCSC) 103, 221, 240, 255, 331, 384, 388, 391, 501, 515
acronym 494
capturing at the POS 400
definition 517
validation 111–112, 215
validation of Bit 53 (Card Security Code) 398

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

process
Store and Forward 261
timeframes
Chip Card 303
processing
Authorization 245
Chargebacks 7
error Chargeback types 304
Offline PIN 234
Online PIN 234
Settlement Exception 274
processor's confidentiality obligations 82
product
Enhancement service fees 408
features 125
specifications 125
programs
customer screening 32
prohibited and restricted countries 36
provisioning services 62
publication schedule 2
publicity 22

Q

Qualified Security Assessor 43

R

Real Currency
definition 517
reason codes
Chargeback, see *Chargeback(s)*
Fulfillment Notification 293
Second Presentment message 300
Recommendation Code 483
Record of Charge (ROC)
completing Charge and Credit 236
records, Authorization log 247
Recurring Billing
Card Not Present Authorizations 254
Recurring Billing Cancellation Service 8, 9, 117, 260
Requirements 117
reference to other manuals 1
Referral Handling
Automated 251
related AEGN Manuals 3
reloadable Prepaid Cards
AML/ATF requirements for 35
Remote Stand-In 258
reporting
fees 414
Request for Support
Illegible/Incomplete, ISO 4517 320
Not Fulfilled, ISO 4516 318, 342
requirements
Issuer Authorization 251
ongoing for Participants 12
S/E compliance validation 42
reservations
lodging 229
No Show Reservations Program 229
policy disclosure 231
restaurant 232
restaurant
estimated charge amounts for 228
reservations 232
restricted and prohibited countries 36
Retrieval
Chargeback types 304
Request 282
Request and Fulfillment 288
revisions
procedures for 2
rewards program 192
risk
assessment provided by Issuer 209
score thresholds 62
Scoring 250
Risk-Mitigating Technologies 39
ROC
archival storage 103
routing
and processing, Chargeback 7
Chargebacks 7

S

S/E Actioning System (SEAS) 390
S/E cancellation, Acquirer Authorization standards 253
S/E classifications 102
S/E floor limits 102
scheduled
outages
notification of 252
Stand-In 259
SEAS, *see* S/E Actioning System (SEAS)
Second Presentment 283
Second Presentment message reason codes 300
Secure Remote Commerce 70
Chargeback Policies 71
Digital Card Facilitator 70
ecosystem 70
Requirements
Acquirers 71
Issuers 71
S/Es deploying SRC 71
Secure Report Commerce
Digital Payment Application 70

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

security
  Cardholder Data Compromise (CDCRP) 49, 52
  guidelines 380
  office 380
security requirements
  for Participants 13
service
  Deferred Payment Plan (DPP) 250
Service Code interrogation
  requirements 217
Service Establishment (S/E)
  acceptable forms of ID 226
  AEGNS investigation of 391
  cancelled S/E policy 253
  cancelled submissions 271
  Card acceptance procedures 214
  Card acceptance restrictions 214
  discounts on purchases 215
  discriminatory treatment on Card acceptance 215
  estimated charge amounts 227
  installment sales 226
  monitoring 389
  Network acceptance 9
  procedures for
    in-person charges 216
    mail charges 221
    telephone charges 221
  submissions, cancelled 271
Service Provider
  definition 519
services
  Fraud and Risk Scoring 250
  Fraud Risk 397
settle
  AEGNS failure to 275
  Participant failure to 275
Settlement
  Advisement 273
  and Funds Exchange 9
    procedures 272
  and funds exchange 272
  Clearing and 282–285
  Double Byte Character Support 279
  exception processes 274
    AEGNS failure to settle 275
    bank holidays, Settlement 275
    compensation computation 277
    compensation from Participant 277
    compensation to Participant 277
    currency restrictions 278
    Daily Settlement Advisements, delay in 276
    delays 277
    dispute process 277
    exchange controls 278
    Participant failure to settle 275
    Participant liability for net 276
    unjust enrichment 277
  process 272
special programs
  advance deposit or payment 231
  lodging reservation 229
  No Show Reservations Program 229
  No Signature/No PIN Program 232
  ZIP Code Verification 233
speed of pay 85, 88
Split Shipment Transaction 214
SRC, see *Secure Remote Commerce*
standards
  Acquirer Authorization 253
  ATM Acquirer Authorization 267
Stand-In 256
  Authorization 9
  Authorization Parameters 259
  Authorization services 251
  Parameter Table 260
  parameter table, single charge 465
  parameter table, velocity based 468
  processing
    legal disclaimer 261
  remote 258
  Scheduled 259
  unscheduled 259
Static Tokens 54
Store and Forward Process 261
submission process
  cancellations by S/E 271
  message order 270
  message outclearing 271
  message type 270
System Outages
  Acquirer Authorization standards 253
  description 251
  Notification 267
system standards, Acquirer Authorization 253
systems
  ATM Acquirer Authorization 267
systems development 14

T

TAT, see *Transit Access Terminal (TAT)*
tax
  taxes on fees and assessment 28
termination
  Participant agreement 121, 122
theft and damage protection 201
time format used in this manual 1
time usage 269
Token 53
  definition 521
Token BIN Allocation 53
Token Creation and Management 53
Token Service Provider (TSP) 54
  definition 521
Tokenization 57
  definition 522

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

Tokenization Services 53
Tokens
  Dynamic 54
  Payment 54
  Static 54
Transaction
  Acquirer processing 87
  activation for cash disbursement 34
  AEGNS Network Disputes Manager-Processed 355
  aggregated 224
  AML/ATF monitoring 32
  Authorization 247
  descriptor information, Internet 103
  Disputes Process Transaction Life Cycle 286
  handling of disputed 281
  Log archival storage 243
  processing, ATM 242
  routing, ATM 6
  routing, Authorization 7
  Transaction Life Cycle
    Authorization processing 281
    Clearing and Settlement 269
    Clearing and Settlement processing 282
    description 10
Transaction data use 24, 113
transfer
  Card portfolio 118
  of S/E portfolio 108
Transit Access Terminal (TAT) 105, 322, 323, 346
  definition 522
  Expresspay Transactions at 218–221
Transport Layer Security (TLS) 420
  definition 522

U

UIR, *see* Urgent Investigation Request (UIR)
Unassigned Cardmember Account Number, ISO 4523 326
United Kingdom Bribery Act of 2010 37
United States Foreign Corrupt Practices Act of 1977 37
unscheduled outages
  notification of 252
Unscheduled Stand-In 259
Urgent Investigation Request (UIR) 383, 389, 396, 405

V

values program 192
velocity based Stand-In parameter table 468
violations
  subject to Fee Schedule A 405
VIP status for Exception File 260
Virtual Currency
  definition 523
voice Authorizations 255
VPN, see *Internet Virtual Private Network (IVPN)* 407

W

warranty protection 201
website information
  display guidelines 101
WINTER 395, 483
  definition 523

Z

ZCV, see *ZIP Code Verification (ZCV) Program*
ZIP Code Verification (ZCV) Program 120, 233, 290, 357
  acronym 495

This document contains sensitive, confidential, and trade secret information, and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.