FREQUENTLY ASKED QUESTIONS

EMV **Global and US**

APRIL 2013

TABLE OF CONTENTS

General Background 1
General FAQ ..... 1 - 2
Merchant FAQ 3
Processor/ATM FAQ 4
Issuer FAQ 4
US Specific FAQ ..... 4 - 5

AMERICAN EXPRESS

GENERAL BACKGROUND

The American Express network was an early adopter of EMV technology. In 1996, the company invested in EMV contact deployment (e.g., Chip & PIN and Chip & Signature). Today, the American Express network is EMV-enabled globally and processes millions of EMV transactions annually.

American Express, one of four major payment organizations that are equity members in EMVCo, is committed to helping secure and interoperable payments globally for chip card transactions. American Express is aligning its EMV specifications alongside other industry participants to deliver process efficiencies for all merchants, processors and issuers of American Express-branded cards.

GENERAL FAQ

Q1: What is EMV?
EMV® is an open-standard set of payment industry specifications for integrated-circuit, chip-based payment and acceptance devices, including terminals and ATMs. The EMV specifications were developed to define a set of requirements to ensure interoperability between chip-based payment products and terminals.

EMV chip products contain embedded microprocessors that provide strong transaction security features and other application capabilities that are not possible with traditional magnetic stripe cards. Today, EMVCo manages, maintains and enhances the EMV specifications and provides product approval for terminals and chip product security on behalf of the payments industry. "EMV" is a trademark of EMVCo.

Q2: What is EMVCo, LLC?
EMVCo, LLC, a company owned by American Express, JCB, MasterCard and Visa, manages, maintains and enhances the EMV Integrated Circuit Card Specifications to ensure global interoperability of chip-based payment cards and acceptance devices, including point-of-sale terminals and ATMs.

EMVCo also administers a testing and approval process and oversees the procedures for confirming compliance with EMV specifications. These activities include compliance testing for both chip-based payment accepting devices and payment cards for both the Common Core Definitions (CCD) and Common Payment Application (CPA) specifications. The testing process and procedures help ensure cross-payment system Inter-operability, which is the over-arching goal of the EMV specifications and EMVCo. American Express, JCB, MasterCard, and Visa have representatives in the EMVCo organization at both management and working group levels.

Q3: What is the status of EMV globally? According to the Nilson Report (January 2012), over 80 countries are in various stages of EMV chip migration. According to EMVCo.'s May 2012 release, 1.5 billion EMV cards have been issued globally and almost 22 million POS terminals accept EMV cards as of Q4 2011. This represents more than 44.7% of the total payment cards in circulation globally and more than 76.4% of the POS terminals installed globally at the time.

Q4: How does EMV work?
EMV cards store payment information on a secure chip rather than on a magnetic stripe. In a contact EMV transaction, the card remains in the EMV terminal throughout the transaction and exchanges information with the terminal. There are three areas of exchange that secure the transaction:

- Card authentication: Cards are authenticated during the payment transaction, helping protect against counterfeit cards. Transactions require card validation either online by the issuer using a dynamic cryptogram or offline with the terminal using Static Data Authentication (SDA), Dynamic Data Authentication (DDA) or Combined DDA with application cryptogram generation (CDA). EMV transactions also create unique transaction data so that any captured data cannot be used to execute new transactions.

- Cardholder verification: Cardholder verification helps ensure that the person attempting to make the transaction is the person to whom the card belongs. Cardholder verification methods (CVM) include Offline PIN, Online PIN, Signature and No Cardholder Verification Method for low dollar amounts.
- Transaction authorization: The transaction is authorized either online or offline. For online authorization, transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction. For offline transactions, the card and terminal communicate and use issuer-defined risk parameters that are sent in the card to determine whether the transaction can be authorized.

Q5: What are DDA, CDA and SDA and how is American Express using them?

The flow of data from an EMV card is encrypted to prevent it from being intercepted or manipulated in transit by unauthorized parties. There are three data authentication methods currently employed, each with differing levels of security.

- Static Data Authentication (SDA): Verifies that the EMV card's contents match its digital signature. SDA will identify fraudulent EMV cards that have invalid numbers within its digital signature. SDA cannot identify counterfeit cards that have copied all of the original card data.
- Dynamic Data Authentication (DDA): Verifies the EMV card's contents and detects if the card has been copied or counterfeited by forcing the card to correctly respond to a card-specific test. This authentication is believed to be more secure than SDA. American Express released a network mandate by which all new EMV card issuers must use DDA technology and authentication.
- Combined Dynamic Data Authentication (CDA): Similar to DDA, except that the terminal performs offline data authentication while producing the application cryptogram. This combines the two processes and therefore delivers a higher level of security than is required of most applications.

Q6: Will contact EMV help reduce fraud and chargebacks?

Contact EMV chip-based payments are believed to reduce fraud from counterfeit, lost or stolen cards and potentially the number of chargebacks.

Similar to other chip-based payments, the dynamic chip data generated by EMV chip-based contact and contactless transactions provide both cardholders and merchants with enhanced security at the point-of-sale.

Secure EMV cards that perform dynamic data authentication have proven effective in combating counterfeit fraud that occurs on magnetic stripe cards in markets like the U.K.[1] EMV cards that have been enabled with a PIN provide added cardholder verification protection against fraud resulting from a lost or stolen card.

The American Express network is EMV-enabled globally and processes millions of EMV transactions annually. Internationally, American Express has fraud liability shift rules and other chargeback-related policies. These policies will be expanded to the U.S. once the U.S. fraud liability shift policies are implemented.

Q7: If EMV cards are more secure, why don't all cards have chips in them?

The move to EMV cards has evolved at a different pace throughout the world and requires investment in technology by both the issuer and merchant. While magnetic stripe cards are secure, EMV is a global standard that introduces more security features and will enable the future evolution of the global payment industry.

Q8: What is the difference between Chip & PIN and Chip & Signature?

Chip & Signature and Chip & PIN are based on the same EMV chip-based technology. The difference is in the Cardholder Verification Method (CVM). For Chip & Signature, the Cardmember signature is the verification method. For Chip & PIN, a PIN is the verification method, Chip & PIN and Chip & Signature both offer enhanced security against counterfeiting compared to traditional magnetic strip-only Cards.

The issuer decides whether to issue the Card as Chip & Signature or Chip & PIN. The American Express network supports both. The merchant terminal will indicate whether it is Chip & Signature or Chip & PIN and the steps that should follow as a result.

Q9: What is the difference between EMV contact and contactless cards?

Contact EMV cards refer to either "Chip & PIN" or "Chip & Signature" cards. Both payment cards utilize microprocessor chips, which securely store card data. The card is inserted into a terminal reader designed for chip cards.

Contactless –enabled cards allow transactions to be initiated by tapping or waving the card in front of a contactless reader at the point-of-sale. The contactless payment device can be a card, bracelet, key fob or smart phone. Card account and security information is then sent wirelessly, using radio frequency, from the contactless device to the reader. Both contactless cards and contactless readers contain tiny antennae that allow data communication to take place. The device never leaves the possession of the customer which enhances security and speeds up the electronic transaction process.

1 First Data, EMV in the U.S.: Putting it into Perspective for Merchants and Financial Institutions, 2011

Q10: What is the difference between magnetic stripe and EMV?

Item	Magnetic Stripe Card	EMV Card
Data Storage	Holds basic cardholder information	Holds cardholder information and additional data securely
Cardholder Verification	Can be vulnerable to counterfeit, lost or stolen or card-not-present fraud as magnetic stripe can be copied	More secure for card present fraud as an EMV card is difficult to copy and transaction is interactive between chip and terminal EMV cards enabled with PIN offer additional protection against fraud resulting from lost or stolen cards
Utility	Facilitates standard payment transactions	In the future, may also facilitate additional payment and non-payment applications (e.g., loyalty programs)

MERCHANT FAQ

Q11: What are the benefits of EMV for merchants?
Deploying EMV contact chip technology for payments can help you optimize your business operations by delivering:

- Potential reduction in fraud-related expenses due to fewer disputed transactions made with American Express-branded cards
- Expanded interoperability as you will be able to accept EMV cards from around the globe and from other payment brands
- Increased confidence for consumers who feel more secure with their transactions

Q12: What is the cost to migrate to EMV?
Costs associated with migration to EMV vary greatly by merchant. Some of the variables influencing the costs include which terminals are chosen; the level of external support required; and the tasks that have to be completed to integrate EMV into the merchant network and POS.
We strongly recommend that you include American Express EMV compliant software within your point of sale upgrade plans.

Q13: What is the certification process and requirements to move to EMV?
Per EMVCo., each card brand requires end to end certification. To get more information about how American Express and EMV in your region, contact your American Express representative. If you are using a third-party processor to authorize and submit card transactions, you will need to work with your processor to get more details about the certification process. If you authorize or submit card transactions directly to American Express, please contact your American Express representative.

Q14: If terminals can accept EMV transactions, are they also able to accept mobile or contactless transactions?
EMV terminals can accept mobile or contactless transactions subject to the POS hardware and software being used. It is the merchant's decision whether to accept contactless and mobile transactions as part of the EMV terminal upgrade. If you do, you will need to make sure the EMV terminal upgrade includes the mobile and/or contactless capabilities and is able to support the latest American Express specifications..

Q15: What is Fraud Liability Shift and how does it apply to EMV?
Fraud Liability Shift (FLS) is used to encourage the adoption of fraud mitigation technologies, such as EMV.

For EMV, FLS transfers liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. The decision to implement FLS is made by each payment brand individually, on a country-by-country basis.

FREQUENTLY ASKED QUESTIONS

EMV **Global and US**

APRIL 2013

PROCESSOR/ATM PROCESSOR FAQ

Q16: What are processors and ATM processors required to do to support EMV?
All processors are required to certify their infrastructure to support American Express EMV chip-based contact, contactless and mobile transactions.

Q17: What are the American Express certification requirements for EMV?
American Express requires EMV host certification and end to end certification for every terminal/reader model and/or unique configuration. For further details, please contact your American Express Representative.

Q18: What does an ATM owner need to do to support EMV?
To support EMV, an ATM owner may need to upgrade their ATM hardware and/or software, including the deployment of contact and contactless reader hardware. The ATM owner will need to coordinate the ATM hardware and/or software upgrade with their processor to ensure EMV certification has been completed.

Q21: Does American Express offer non-financial support to issuers to expedite the migration to EMV cards?
Yes, American Express provides an "On Behalf Of" cryptogram validation service for EMV card transactions. This enables participants to take advantage of EMV without the costs associated with building cryptogram validation logic on the issuer's authorization host system. For issuers using this capability, American Express will validate the cryptogram on the issuer's behalf and forward an incoming authorization message to the issuer for decisioning with a flag indicating whether the cryptogram was successfully validated.

ISSUER FAQ

Q19: Do issuers need to complete any certification on the American Express card issuance infrastructure to support EMV issuance?
Yes. Issuers should contact their American Express representative to review the engagement process and certification requirements for the issuer's chip products.

Q20: How long does it generally take for card-issuing partners to complete an EMV migration?
Migrating to EMV is a complex project that will impact issuing and acquiring infrastructures as well as back-end authorization systems. As the scope of each issuer implementation could vary, an exact estimate is difficult to provide; however, for planning purposes, an issuer should plan for an approximate 6-9 month timeframe to complete an EMV migration.

U.S.-SPECIFIC FAQ

Q22: What is American Express' position on EMV in the U.S.?
The U.S. remains in the early stages of adoption, and we believe that American Express is entering at the right time to contribute to industry plans and advance EMV adoption.

The American Express network was an early adopter of EMV technology and is committed to helping secure and interoperable payments globally for EMV card transactions. Today, the American Express network is EMV-enabled globally and processes millions of EMV transactions annually.

Q23: What does American Express' EMV roadmap in the U.S. look like?
American Express will work alongside other industry participants to encourage interoperability across the U.S. and other countries and support chip-based technology for chip & PIN, chip & Signature, contactless and mobile transactions. The company's key policy requirements and dates for the U.S. are:

- By April 2013, processors must be able to support American Express EMV chip-based contact, contactless and mobile transactions.
- Beginning October 2013, merchants will be eligible to receive reduced PCI Data Security Standard (DSS) reporting requirements if the merchants' point-of-sale (POS) are certified to process American Express EMV chip-based contact and contactless transactions.
- Effective October 2015, American Express will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. U.S. fuel merchants will have an additional two years, until October 2017, before the FLS takes effect for transactions generated from automated fuel dispensers.

Q24: Will American Express support all types of Cardholder Verification Methods (CVMs)?
Yes, the American Express network specifications support all EMV recognized methods of cardholder verification, including Offline PIN, Online PIN, Signature and No CVM for low dollar amounts, regardless of the issuer's EMV product presented by the Cardmember at the point-of-sale. The cardholder verification method that is used at the point-of-sale will depend on the card product, terminal capabilities and transaction value.

Q25: What is the merchant demand for EMV-enabled terminals in the U.S.?
In the past year, American Express has seen an increase in merchant requests for EMV-enabled terminals in the U.S. EMV technology offers enhanced security and the potential for reduced applicable card fraud. Merchant terminals typically require both hardware (to read the EMV contact and contactless chips) and American Express compliant? EMV software to read and interact with the chip and process incremental chip data generated. Once merchants load their terminals with American Express compliant software, merchants will be required to certify their devices with American Express, if their processor has not already done so, to confirm conformance with our requirements.

Q26: What does it mean for merchants to get relief from PCI DSS reporting requirements in the U.S.? Does that mean financial relief?
Beginning October 2013, merchants will be eligible to receive reduced PCI Data Security Standard (DSS) validation reporting requirements if a minimum75% of American Express in-person transactions are processed on Point of Sale (POS) devices certified to accept American Express EMV chip-based contact and contactless transactions

PCI DSS reporting relief refers to the reduction in PCI validation documentation required by merchants to be in compliance with the American Express Data Security Operating Policy (DSOP). EMV merchants may be eligible to submit an Annual EMV Attestation (AEA) which may replace the Annual Attestation of Compliance (AOC) or Self Assessment Questionnaire (SAQ) and Quarterly Network scans currently required for American Express DSOP validation documentation. The PCI DSS reporting relief may reduce the time spent on reporting and other associated administrative efforts.

Q27: What is your fraud liability shift policy in the U.S.? Is this a financial incentive for merchants?
Effective October 2015, American Express will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. Following the rollout of EMV in other countries, merchants have seen a reduction in certain types of fraud and fraud chargebacks. It is expected that merchants will experience similar reductions the U.S. This reduction of fraud and chargebacks can result in a beneficial return on EMV-related investments by merchants and issuers.

U.S. fuel merchants will have an additional two years, until October 2017, before the FLS takes effect for transactions generated from automated fuel dispensers.

Q28: What are the consequences for U.S. merchants for non-compliance for EMV transactions?
Effective October 2015, American Express will institute a Fraud Liability Shift (FLS) policy to transfer liability for certain types of fraudulent transactions away from the party that has the most secure EMV technology. A merchant could be subjected to increased fraud exposure for failing to adopt EMV technology. American Express is dedicated to ensuring all parties embrace a policy that supports secure processing of Cardmember data

Q29: When will changes be made to American Express' U.S. Merchant Regulations?
The American Express Merchant Regulations – U.S. will be updated prior to the October 2015 Fraud Liability Shift (FLS) effective dates.

Q30: What is the time table for processors to convert to EMV in the U.S.?
U.S. processors must be enabled to support American Express EMV chip-based contact, contactless and mobile transactions by April 2013.

Q31: When did American Express issue EMV chip-based cards in the U.S.?
American Express began issuing EMV-compliant cards in the U.S. in the latter half of 2012.

Q32: Will ATMs in the U.S. that accept American Express Cards also accept EMV chip-based cards?
American Express expects that over time ATM owners in the U.S. will deploy ATMs that accept contact and contactless EMV cards. American Express will be working with ATM owners and their processors to ensure ATMS are enabled to process transactions made with American Express-branded EMV cards as EMV transactions.