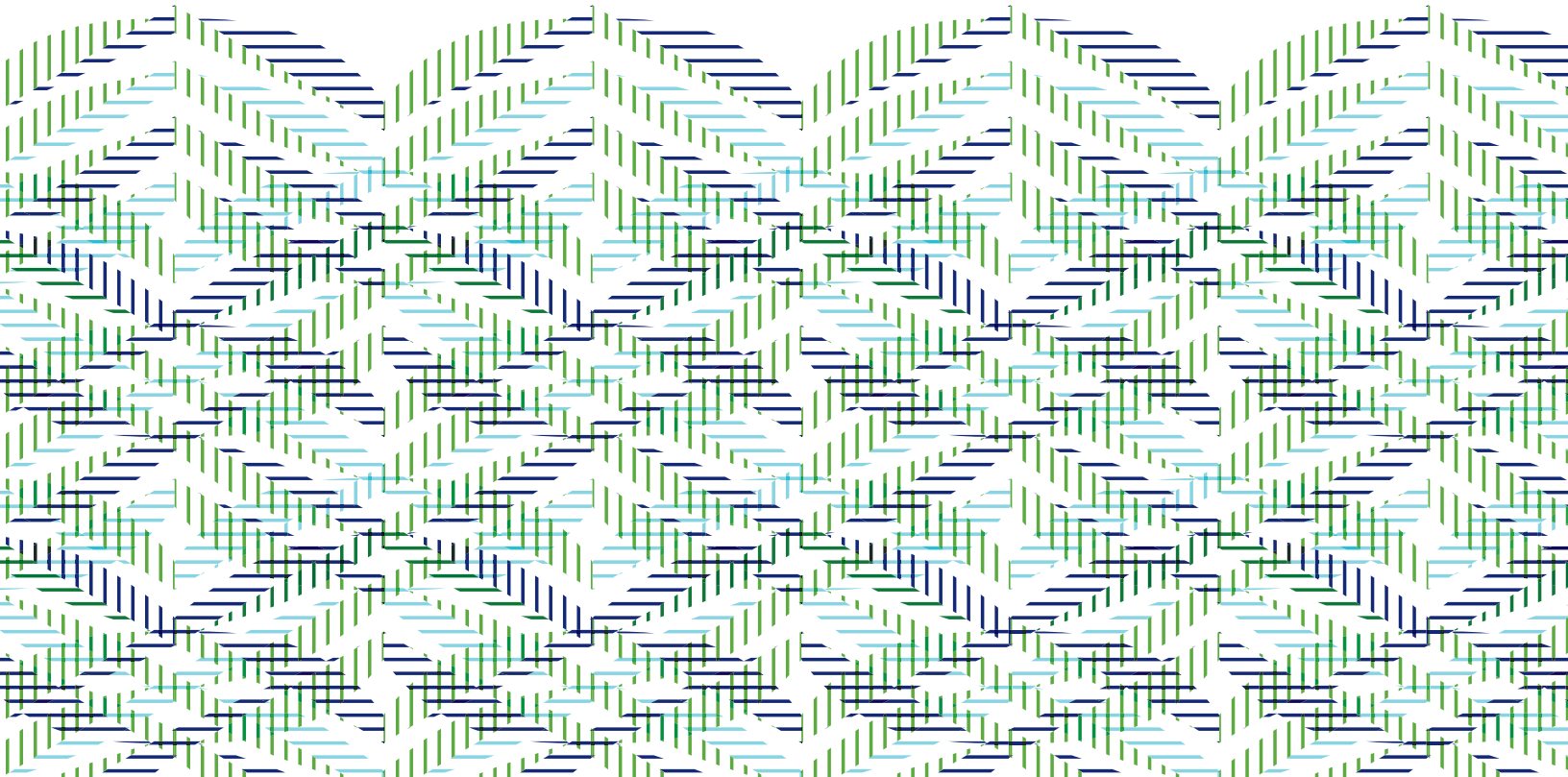
# AMERICAN EXPRESS SAFEKEY®

# FREQUENTLY ASKED QUESTIONS

JANUARY 2017



## WHAT IS AMERICAN EXPRESS SAFEKEY®?

The American Express SafeKey program ("SafeKey") is an authentication tool that adds an extra layer of security when a participating Card Member shops online. SafeKey can help reduce unauthorized online use before it happens by validating the Card Member's identity through various authentication methods including risk-based authentication and dynamic one-time passcodes.

### WHERE IS SAFEKEY AVAILABLE?

Effective April 15, 2016, American Express SafeKey is available globally.

### WHAT IS 3-D SECURE®?

3-D Secure is an e-commerce fraud prevention protocol that is accepted as an industry standard for globally interoperable payment authentication. American Express has licensed the 3-D Secure protocol and launched a branded solution called SafeKey.

### WHAT KIND OF AUTHENTICATION METHODS DOES SAFEKEY SUPPORT?

SafeKey is based on the 3-D Secure protocol supporting multiple authentication methods including risk-based authentication and dynamic one-time passcodes.

### IS SAFEKEY ALIGNED WITH INDUSTRY STANDARDS?

**Yes.**
To facilitate ease in certification of SafeKey and minimize development costs as much as possible, SafeKey has aligned with industry standards. Issuers, Acquirers and Vendors should find the American Express 3-D Secure solution to be virtually the same as others in the payment industry.

### WHAT OTHER ONLINE FRAUD PREVENTION TOOLS ARE AVAILABLE?

SafeKey compliments other American Express fraud prevention solutions and tools such as Automated Address Verification (AAV) and Enhanced Authorization (EA). SafeKey is intended to be used in conjunction with other fraud prevention solutions as an additional layer of security.

### WHAT IS SAFEKEY FRAUD LIABILITY SHIFT (FLS)?

For qualifying SafeKey transactions, SafeKey FLS transfers fraud exposure from the Merchant/Acquirer to the Issuer when an enrolled SafeKey Merchant authenticates a Card-Not-Present transaction with an Issuer. If the Merchant attempts a SafeKey transaction or an Issuer is able to authenticate a SafeKey transaction, the Issuer may not raise a fraud chargeback to an eligible Merchant.

### CAN SAFEKEY BE UTILIZED FOR ONLINE TRANSACTIONS ON ALL CARD PRODUCTS?

SafeKey cannot be enabled for or used to authenticate Card products that are anonymous, like some Prepaid Cards where the user's identity is not registered. This includes Card products that may have multiple users like Purchasing Cards.

# MERCHANT FAQ

### HOW CAN A MERCHANT ENROLL IN SAFEKEY

Merchants will be able to enroll in the SafeKey program by visiting the SafeKey enrollment portal at amexsafekey.com. Alternatively, Merchants can contact their Merchant Plug-In (MPI) or Payment Service Provider.

### WHAT IS THE ESTIMATED DEVELOPMENT EFFORT FOR A MERCHANT CHOOSING TO IMPLEMENT SAFEKEY?

Depending on the processing model, varying levels of technical development may be required to support the integration of SafeKey. Merchants should consider costs incurred from internal technical development and external linkages with third parties.

### CAN SAFEKEY BE TURNED OFF BY THE MERCHANT AFTER IMPLEMENTATION?

Technically, SafeKey can be switched off by the Merchant. However, the intention of SafeKey is to reduce instances of Card-Not-Present fraud. As such, American Express does not recommend turning off SafeKey at any time in accordance with SafeKey Implementation Guidelines.

### HOW IS A CARD AUTHENTICATED AND AUTHORIZED WHEN BOTH THE MERCHANT AND CARD MEMBER ARE ENROLLED IN SAFEKEY?

- ☐ During checkout, the Card Member inputs his/her payment method as American Express and provides the Card number.
- ☐ The MPI component integrated with the Merchant website will communicate with the SafeKey Directory Server to determine if the American Express Card is enrolled in SafeKey.
- ☐ The SafeKey Directory Server will communicate with the Card Issuer to determine if the Card is eligible for the service.
- ☐ The Issuer will respond with a status of "Y" if the Card is eligible, along with a URL where the Card Member needs to be sent for authentication (the Authentication Site).
- ☐ The Merchant application will automatically redirect the Card Member to the Authentication Site.
- ☐ At the Authentication Site, the Issuer will display the authentication dialogue page where the Card Member will attempt to authenticate. The Issuer will send a response to the Merchant with the authentication result. For security, the message will be digitally signed.
- ☐ The MPI will validate the signature and advise the Merchant of the authentication result.
- ☐ The Merchant can approve or decline the transaction based on the authentication result.

### WILL MERCHANT TERMS AND CONDITIONS REQUIRE CHANGES TO SUPPORT THE SAFEKEY PROGRAM?

**Yes.**
The Terms and Conditions for American Express Card Acceptance may be amended or re-issued to enable SafeKey FLS.

### WHAT IS THE DEFINITION OF AN ATTEMPTED TRANSACTION?

A SafeKey authentication attempt occurs when a Merchant requests to authenticate the Card Member but the Card Member or Issuer has not been enrolled in the SafeKey program. In this scenario, valid authentication data [e.g., American Express Verification Value ("AEVV") and Electronic Commerce Indicator ("ECI")] will be required in the Authorization and Submission messages as evidence of the attempt.

### WILL A PARTICIPATING MERCHANT OBTAIN SAFEKEY FLS ON ALL CARD-NOT-PRESENT TRANSACTIONS?

**No.**
Merchants can only obtain SafeKey FLS on fully-authenticated and attempted SafeKey transactions. For standard e-commerce charges, the standard Card-Not-Present Card acceptance policy applies and the Merchant is liable if the Card Member later disputes the charge.

### WHERE CAN A MERCHANT OBTAIN AUTHORIZATION AND SUBMISSION SPECIFICATIONS FOR SAFEKEY?

The most up-to-date global Merchant technical specifications can be found at americanexpress.com/merchantspecs. For additional information on which market-standard specifications currently support SafeKey, Merchants may contact their American Express Client Manager or their Payment Service Provider (PSP).

### WHAT CRITERIA MUST BE SATISFIED FOR A MERCHANT TO QUALIFY FOR SAFEKEY FLS?

**In order to be eligible for SafeKey FLS, a Merchant must:**

- ☐ Utilize SafeKey.
- ☐ In markets outside the U.S., use all other American Express online fraud prevention tools available in their market.
- ☐ Maintain a Fraud-to-Gross (FTG) level of 1% or less for all SafeKey transactions. In the U.S. market, maintain data completeness and quality thresholds above 85%.

In the UK, for example, this would mean the Merchant would need to participate in AVS and collect/send the Printed Card Security Code (PCSC) in addition to utilizing SafeKey and maintaining the appropriate FTG level.

# ISSUER FAQ

### WHAT IF AN ISSUER DECIDES NOT TO PARTICIPATE IN SAFEKEY?

Though SafeKey is an optional service for Issuers, Issuers that do not participate may be liable for transactions where SafeKey authentication was attempted by the Merchant. Please refer to the Business and Operational Policies manual Section 7.9 located at GNSweb.

### WHAT COSTS ARE INVOLVED TO SUPPORT SAFEKEY?

In addition to the costs of obtaining an ACS service, costs for Network certification and certificates can be confirmed by contacting your American Express Representative.

### HOW CAN AN ISSUER FIND OUT WHICH ACS VENDORS ARE CERTIFIED FOR SAFEKEY?

For specific information on SafeKey-certified ACS providers, please contact your local AEGNS representative. If you are already participating in 3-D Secure programs from other associations and would like to utilize the same ACS vendor for SafeKey, please request your ACS vendor to visit the SafeKey Enrollment website in order to complete certification for SafeKey.