EMV® Chip Cards

FREQUENTLY ASKED QUESTIONS

What is EMV® Chip Cards?

American Express chip cards follow EMV® specifications, enabling seamless and secure in-store payments and helps prevent fraud at the Point-of-Sale. The American Express network was an early adopter of EMV technology. In 1996, the company invested in EMV contact deployment (e.g., Chip & PIN). Today, the American Express network is EMV-enabled globally and processes millions of EMV transactions annually.

1. General FAQ

Q1.1 What is EMV?

EMV is a global industry standard for integrated-circuit, chip-based payment and acceptance devices, including Point of Sales (POS) 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. EMVCo maintains and enhances the EMV specifications and provides product approval for terminals and chip product security on behalf of the payments industry.

Q1.2 Who is EMVCo, LLC?

EMVCo, LLC, a company owned by American Express, Discover, JCB, MasterCard, Visa and UnionPay, 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 POS terminals/payment accepting devices and payment cards for both the Common Core Definitions (CCD) and Common Payment Application (CPA) specifications.

Security and interoperability are the overarching goals of the EMV specifications and EMVCo. American Express, Discover, JCB, MasterCard, Visa and UnionPay have representatives in the EMVCo organization at both management and working group levels.

Q1.3 How do EMV contact chip cards work?

Chip Card technology was designed to reduce counterfeit, lost/stolen and Card-not-received fraud. Chip Cards can either be contact or contactless. Contact EMV® chip Cards utilize microprocessor chips which securely store Card data. The Card is inserted into a terminal reader designed for smart Cards. Depending if the Card is “Chip and PIN” or “Chip and Signature,” it will require the Card Member to either enter a PIN for authorization at the point of sale or the Card Member may be asked to sign.

1. General FAQ

Q1.4 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 cards that have invalid numbers within its digital signature. SDA cannot identify counterfeit cards that have copied all the original card data.
- **Dynamic Data Authentication (DDA):** Verifies the EMV card's contents and detects if the card has been copied or counterfeited. DDA improves upon SDA by making use of dynamic card and terminal data elements to validate a unique cryptogram generated for each transaction by the card. This authentication method is more secure than SDA. American Express released a network mandate by which all new EMV card Issuers must use DDA technology.
- **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.

Q1.5 Will contact EMV chip-based payments help reduce fraud and chargebacks?

Contact EMV chip-based payments have been proven to reduce fraud from counterfeit, lost or stolen cards and potentially the number of chargebacks. The cryptogram data generated by the EMV chip in both contact and contactless transactions enhances payment security by authenticating each transaction uniquely, providing cardholders and merchants with stronger protection against counterfeit and fraud 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. 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 that protect Merchants who have implemented EMV technology.

1. General FAQ

Q1.6 What types of Cardholder Verification Methods (CVMs) does American Express support?

The American Express Global Network specifications support all EMV recognized methods of cardholder verification, including Offline PIN, Online PIN, Signature (if applicable), Consumer Device CVM, and No CVM for low dollar amounts. The cardholder verification method that is used at the point-of-sale will depend on the card product, terminal capabilities and transaction value.

Q1.7 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 Card Member 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 chip 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. Capturing signature is optional, meaning a Merchant may process a transaction without Card Member signature.

Q1.8 What is the difference between EMV contact and contactless cards?

Contact EMV cards refer to either “Chip & PIN” or “Chip” cards. Both payment cards utilize microprocessor chips, which securely store card data. The card is inserted into a terminal reader designed for chip cards. Depending on the Card, the terminal reader will require the Card Member to either enter a PIN for authorization at the point of sale or the Card Member may be asked to sign.

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, mobile device with a payment wallet enabled, or another form factor, such as a smart watch. Payment information is then sent securely using radio frequency for Card or Near Field Communication (NFC), which allows a mobile device to send the required data to the reader (payment terminal). Both contactless cards and contactless readers contain tiny antennae that allow data communication to take place. The payment device never leaves the possession of the customer, which means there is enhanced security as the card is not taken away from the Card Member and speeds up the electronic transaction process.

Q1.9 How do I find out more about EMV Chip Cards?

For more information about EMV Chip Cards, visit our web page or reach out to your American Express Representative.

2. Merchant FAQ

Q2.1 Do Merchants or banks need to capture signature?

Capturing Card Member signature on Card Present Transactions is optional to complete a receipt and at the discretion of the Merchant, unless required by applicable law. Please contact your local American Express representative for more information.

Q2.2 What are the benefits of EMV chip technology for Merchants?

Deploying EMV contact chip technology for payments can help Merchants optimize their business operations by delivering:

- A more secure payment option by heightening the level of card authentication
- Deterring counterfeit and lost/stolen card fraud at the point of sale
- Increased confidence for consumers who feel more secure with their transactions
- Deploying the industry standard for secure payments and a foundation for emerging payment technologies around the world

Q2.3 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. It is strongly recommended that Merchants include American Express EMV compliant software or terminals within their point-of-sale upgrade plans.

Q2.4 What is the certification process and requirements to move to EMV?

There are varying degrees of testing that could be required as part of certification, including EMVCo testing for payment accepting devices or American Express end-to-end certification. This testing is similar to the approach of other card brands. For more information about 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.

2. Merchant FAQ

Q2.5 If terminals can accept EMV contact chip transactions, are they also able to accept mobile or contactless transactions?

EMV terminals can accept mobile or contactless transactions depending on 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.

Q2.6 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 chip card technology. 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.

3. Processor/ATM Processor FAQ

Q3.1 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.

Q3.2 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.

Q3.3 What does an ATM owner need to do to support EMV?

To support EMV, ATM owners may need to upgrade their ATM hardware and/or software, including the deployment of contact and contactless reader hardware. The ATM owners will need to coordinate the ATM hardware and/or software upgrade with their processors to ensure EMV certification has been completed.

4. Issuer FAQ

Q4.1 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.

Q4.2 How long does it generally take for card-issuing partners to complete an EMV migration?

Migrating to EMV is a complex project that depend on a number of factors that may include:

- Product development and certification Card platforms.
- Updating Card production and personalization processes.
- Updating host and downstream systems to process Expresspay transactions.
- Product-launch Card Member communication.

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.

Q4.3 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.