EMV FREQUENTLY ASKED QUESTIONS

What is EMV?

EMV is an abbreviation for Europay, Mastercard and Visa, the three organizations that developed the initial specifications. EMV is an open-standard set of specifications for smart card payments and acceptance devices. The EMV specifications were developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards. Today, EMVCo manages, maintains and enhances the specifications. EMVCo is owned by American Express, Discover, JCB, MasterCard, UnionPay, and Visa, and includes other organizations from the payments industry participating as technical and business associates. Information on the specifications and organization is available at http://www.emvco.com.

What are the benefits of EMV?

The biggest benefit of EMV is the reduction in card-present card fraud resulting from counterfeit, lost and stolen cards.

- **Improved security over cards that solely use a magnetic stripe.** Whereas a magnetic stripe card delivers the same static cardholder data to the terminal for every transaction, an EMV chip card and an EMV-capable terminal exchange unique data for each transaction using sophisticated cryptographic authentication technology. As a result, any transaction data that is stolen cannot be used to produce counterfeit cards(s). Also, every EMV transaction authorization request includes additional data that allows the issuer to verify that the card used is genuine and that the transaction data has not been modified.
- **EMV also provides interoperability with the global payments infrastructure – consumers with EMV chip payment cards can use their card on any EMV-compatible payment terminal.**

How does an EMV transaction work?

There is a fundamental difference between magnetic stripe and EMV chip transaction. With a magnetic stripe card, the stripe stores data that is read by a terminal. The terminal reads the magnetic stripe and initiates an online credit, debit, or prepaid transaction. Subsequently, the transaction is routed to/through branded payment networks and/or various payment processors for authorization. The physical card and stripe no longer play a role in the transaction once the initial data is read.

An EMV chip and an EMV-capable terminal interact dynamically in real time using more sophisticated cryptographic authentication technology. During an EMV transaction, the chip is capable of processing information and actually determines some of the rules for the payment. The terminal helps enforce the rules set by the issuer. These rules can include defining the cardholder verification method, including PIN or signature, requiring online authorization or even authorizing a low-dollar transaction offline. It's up to the issuing bank, in collaboration with their payment processor, to define which of these services is required for the current transaction via the rules placed on the chip.

Why are EMV credit and debit cards and EMV chip payment transactions secure?

EMV secures the payment transaction with enhanced functionality in three areas:

- **Card authentication** - **protecting against counterfeit cards**. The card is authenticated during the payment transaction, protecting against counterfeit cards. Transactions require an authentic card validated 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**, authenticating the cardholder and protecting against lost and stolen cards. Cardholder verification ensures that the person attempting to make the transaction is the person to whom the card belongs. EMV supports four cardholder verification methods (CVM): offline PIN, online PIN, signature, or no CVM. The issuer prioritizes CVMs based on the associated risk of the transaction (for example, no CVM is used for unattended devices where transaction amounts are typically quite low).

- **Transaction authorization**, using issuer-defined rules to authorize transactions. The transaction is authorized either online or offline. For an online authorization, transactions proceed as they do today in the U.S. with magnetic stripe cards. The transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction. In an offline EMV transaction, the card and terminal communicate and use issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized. Offline transactions are used when terminals do not have online connectivity (e.g., at a ticket kiosk) or in countries where telecommunications costs are high.

EMV cards store payment information in a secure chip rather than on a magnetic stripe and the personalization of EMV cards is done using issuer-specific keys. Unlike a magnetic stripe card, it is virtually impossible to create a counterfeit EMV card that can be used to conduct an EMV payment transaction successfully.

How does EMV address payments fraud?

First, the EMV chip card includes a secure microprocessor chip that can store information securely and perform cryptographic processing during a payment transaction. Chip cards carry security credentials that are encoded by the card issuer at personalization. These credentials, or keys, are stored securely in the EMV card's chip and are impervious to access by unauthorized parties. These credentials therefore help to prevent card skimming and card cloning, one of the common ways magnetic stripe cards are compromised and used for fraudulent activity.

Second, in an EMV chip transaction, the card is authenticated as being genuine, the cardholder is verified, and the transaction includes dynamic data and is authorized online or offline, according to issuer-determined risk parameters. As described above, each of these transaction security features helps to prevent fraudulent transactions.

Third, even if fraudsters are able to steal account data from chip transactions, this data cannot be used to create a fraudulent transaction in an EMV chip or magnetic stripe environment, since every EMV transaction carries dynamic data.

And lastly, EMV may also help to address card-not-present fraud with cardholders using their EMV cards and individual readers to authenticate internet transactions.