# EMV Chip Payment Technology: Frequently Asked Questions

## 1. What is EMV?

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, China Unionpay, 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.

## 2. Where has EMV been adopted?

Financial institutions in Europe, Latin America, Asia/Pacific, Canada and the United States are issuing contact or dual-interface EMV chip cards for credit and debit payment (commonly referred to as “chip and PIN”) or migrating to EMV issuance and acceptance. EMVCo publishes global statistics on EMV issuance and acceptance. EMVCo reported that over 3.4 billion EMV cards were in circulation globally at the end of 2014. EMVCo also reports the status of “chip-on-chip” transactions; one in three of all card-present transactions undertaken globally between June 2014 and June 2015 used EMV chip technology.

The U.S. is now migrating to EMV chip cards. The EMV Migration Forum is the cross-industry organization focused to address issues that require broad cooperation and coordination across many constituents in the payments space in order to successfully introduce secure EMV contact and contactless technology in the United States. As of the end of 2015, the Forum estimates that approximately 400 million EMV chip cards have been issued in the U.S., with 675,000 merchant locations accepting EMV chip transactions.

The Forum has published a variety of resources to assist payments industry stakeholders with EMV migration; resources are available on the EMV Connection web site.

## 3. Why are countries migrating to EMV?

Issuers around the world are including chips in bank cards and merchants are moving to EMV-compliant point-of-sale (POS) terminals to increase security and reduce card-present fraud resulting from counterfeit, lost and stolen cards.

## 4. What are the benefits of EMV?

The biggest benefit of EMV is the reduction in card-present fraud resulting from counterfeit, lost and stolen cards. 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. EMV technology also supports enhanced cardholder verification methods.

## 5. Why are EMV credit and debit cards and EMV 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 and 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.

## *6. What is the status of EMV migration in the United States?*

The U.S. is in the process of migration to EMV, with the initial fraud liability shift milestone complete in October 2015.

According to the EMV Migration Forum, as of the end of 2015, approximately 400 million EMV chip cards have been issued in the U.S., with 675,000 merchant locations accepting EMV chip transactions.

Additional information on U.S. EMV migration can be found on the EMV Connection web site.

## *7. Should U.S. travelers with magnetic stripe only payment cards expect issues when traveling to countries that have implemented EMV?*

Some U.S. travelers have been reporting troubles using their magnetic stripe cards while traveling. The most common areas where travelers may face issues are at unmanned kiosks for tickets, gasoline, tolls and/or parking, and in rural areas where shop owners do not know how to accept magnetic stripe cards.

## *8. Will travelers with EMV cards visiting the U.S. have issues paying for purchases?*

Currently, all EMV chip cards also have a magnetic stripe, so that those cards can be used in regions and countries that have not deployed EMV. There has been some discussion by the European Payment Council (EPC) to allow European financial institutions the option to issue chip-only cards. However, European cardholders who travel internationally would be able to enable magnetic stripe acceptance as needed.

## *9. 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.

## *10. What is the proven impact of EMV adoption on payment card fraud?*

Countries implementing EMV chip payments have reported a decrease in card fraud. As an example of the impact of EMV, the UK Cards Association has reported a dramatic reduction in fraud since the introduction of EMV cards.

> "Fraud on lost and stolen cards is now at its lowest level for two decades and counterfeit card fraud losses have also fallen and are at their lowest level since 1999. Losses at U.K. retailers have fallen by 67 per cent since 2004; lost and stolen card fraud fell by 58 per cent between 2004 and 2009; and mail non-receipt fraud has fallen by 91 per cent since 2004."

Similarly, the national roll-out of EMV in Canada in 2008 had a dramatic impact on fraud. Losses from debit card skimming in Canada fell from CAD$142 million in 2009 to CAD$38.5 million in 2012, according to the Interac Association. Interac debit card fraud losses as a result of skimming hit a record low in 2013, decreasing to CAD$29.5 million.

The experiences of the U.K. and other countries that have adopted chip have shown a reduction of domestic card-present fraud. But their experiences have also shown a migration to other types of fraud, namely card-not-present (CNP) fraud and cross-border counterfeit fraud (particularly ATM fraud). Fraud migration offsets some of the savings from the decrease in domestic card-present fraud. This reality reinforces the need for a layered approach to security, even with EMV deployment, to address fraud migration and other security vulnerabilities.

## *11. How does card authentication work with EMV?*

Card authentication protects the payment system against counterfeit cards. Card authentication methods are defined in the EMV specifications and the associated payment network chip specifications. Card authentication can take place online with the issuer authenticating the transaction using a dynamic cryptogram, offline with the card and terminal performing static or dynamic data authentication, or both.

## *12. How are cardholders verified with EMV?*

Cardholder verification authenticates the cardholder. EMV supports four CVMs:

- Online PIN, where the PIN is encrypted and verified online by the card issuer
- Offline PIN, where the PIN is verified offline by the EMV card
- Signature verification, where the cardholder signature on the receipt is compared to the signature on the back of the card
- No CVM, where none is used (typically for low value transactions or for transactions at unattended POS locations)

Depending on payment network rules and issuer preference, chip cards are personalized with one or more CVMs in order to be accepted in as wide a variety of locations as possible. Different terminal types support different CVMs. For example, attended POS devices, in addition to supporting signature, may support online or offline PINs (or both), while some unattended card-activated terminals may support “no CVM."

## 13. How are transactions authorized with EMV?

EMV transactions can be authorized online or offline. For an online authorization, transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction in real time.

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.

Chip cards can be configured to allow both online and offline authorization, depending on the circumstances. Due to improvements in telecommunications infrastructure worldwide, most EMV chip transactions are now authorized online.

## 14. How does contactless technology relate to EMV?

Issuers are now issuing EMV cards that support contact and/or contactless EMV transactions. Contactless EMV transactions use the ISO/IEC 14443 protocol for communication, with EMVCo defining the EMV Contactless Communication Protocol Specification that is common for all payment networks. EMVCo has also published specifications for contactless POS readers that work with the payment networks’ contactless applications.

The EMV specifications provide a basis for contactless EMV payments, but do not specify all payment application functionality. Payment networks can implement contactless payment for EMV transactions to function in both offline and online transaction environments and to leverage the EMV cryptogram security function to validate the authenticity of the card and the transaction.

## 15. How does NFC-enabled mobile payment relate to EMV?

Contactless payment transactions between an NFC-enabled mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by EMV contactless credit and debit cards. This means that consumers can use their NFC-enabled mobile phones for payment at the existing installed base of contactless credit and debit terminals that are based on this standard. Additional information can be found in the Smart Card Alliance white paper, EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments.

## 16. How do EMV chip and PCI DSS work together?

EMV chip has strong security features that have been proven to reduce counterfeit card fraud at card-present retail environments. The Payment Card Industry Data Security Standard (PCI DSS) provides other complementary levels of security necessary when the cardholder information reaches the merchant’s system. The PCI DSS contains 12 key technical and operational requirements. Rather than focusing on a specific category of fraud, the PCI DSS seeks to protect cardholder and sensitive authentication data anywhere this data is present within the payment ecosystem, thus limiting the availability of this data to fraudsters. When used together, EMV chip and PCI DSS can reduce fraud and enhance the security of the payments ecosystem.

## 17. Where I can learn more about EMV?

The EMV Connection website (http://www.emv-connection.com) provides Smart Card Alliance and EMV Migration Forum resources, industry resources, and recent articles and news on the topic. EMVCo also provides many resources on its website (https://www.emvco.com).

### *18. Where can I learn more about issuing EMV cards to my financial services customers?*

The EMV Connection website is a good place to start. A section of the web site is focused on information relevant to card issuers, including technical guidance and other best practices for EMV chip migration.

## *About the Smart Card Alliance*

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.