EMV: 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, MasterCard, JCB, 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?

EMV has been implemented in more than 80 countries around the world, with approximately 1.5 billion EMV cards issued globally and 21.9 million POS terminals accepting EMV cards at the end of 2011. The U.S. payments infrastructure is now moving to EMV with incentives and requirements for issuers, acquirers/processors and merchants to adopt EMV over the next three years.

The United States is one of the last countries to migrate to EMV. In 2011 and 2012, American Express, Discover, MasterCard and Visa all announced their plans for moving to an EMV-based payments infrastructure in the U.S.

- In August 2011**,** Visa announced plans to accelerate chip migration and adoption of mobile payments in the United States, through retailer incentives, processing infrastructure acceptance requirements and counterfeit card liability shift.
- In January 2012, MasterCard announced their U.S. roadmap to enable the next generation of electronic payments, with EMV the foundational technology**.**
- In March 2012, Discover announced implementation of a 2013 mandate for acquirers and direct-connect merchants in the U.S., Canada and Mexico, to support EMV.
- In June 2012, American Express announced its U.S. EMV roadmap to advance contact, contactless and mobile payments and plans to begin issuing EMV-compliant cards in the U.S. in the latter half of 2012.

3. Why are countries migrating to EMV?

Issuers around the world are including chips in bank cards and merchants are moving to EMV-compliant terminals to increase security and reduce 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 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 supports enhanced cardholder verification methods and, unlike magnetic stripe cards, EMV payment cards can also be used to secure online payment transactions.

5. Why are EMV credit and debit cards and EMV payment transactions secure?

First, 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 cardholder verification method (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.

Third, 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 a EMV payment transaction successfully.

6. Is EMV going to be implemented in the United States? Are there any U.S. banks issuing EMV cards?

In August 2011, Visa announced plans to accelerate chip migration and adoption of mobile payments in the United States, through retailer incentives, processing infrastructure acceptance requirements and counterfeit card liability shift.

In January 2012, MasterCard announced their U.S. roadmap to enable the next generation of electronic payments, with EMV the foundational technology.

In March 2012, Discover announced implementation of a 2013 mandate for acquirers and direct-connect merchants in the U.S., Canada and Mexico, to support EMV.

In June 2012, American Express announced its U.S. EMV roadmap to advance contact, contactless and mobile payments and plans to begin issuing EMV-compliant cards in the U.S. in the latter half of 2012.

U.S. banks have already started issuing and some intend to issue payment cards with EMV technology to their customers. Announcements as of July 2012 include the following:

- American Express
- Andrews Federal Credit Union
- Bank of America
- Chase
  - JPMorgan Palladium Card
  - JP Morgan Select Visa Signature card
  - Chase Hyatt Visa Signature Credit Card

    - Chase British Airways Visa Signature Credit Card
- Citi
    - Citi Commercial Cards
    - Citi ExecutiveSM / AAdvantage® Card
- Jack Henry & Associates Payment Processing Solutions
- PSCU Financial Services
- Silicon Valley Bank
- Star One Credit Union
- State Employees Credit Union
- Travelex Cash Passport
- United Nations Federal Credit Union
- U.S. Bank
- Wells Fargo

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

U.S. travelers are reporting troubles using their magnetic stripe cards while traveling. Aite Group has estimated that 9.7 million U.S. cardholders experienced magnetic stripe card acceptance issues when they traveled internationally in 2008, costing banks $447 million in lost revenue. 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 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 card includes a secure microprocessor chip that can store information securely and perform cryptographic processing during a payment transaction. EMV 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 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 or magnetic stripe environment, since every EMV transaction carries dynamic data.

And lastly, EMV can also address card-not-present (CNP) fraud, with cardholders using their EMV cards and individual readers to authenticate Internet transactions.

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

Countries implementing EMV 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."

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. For example, The U.K. group, Financial Fraud Action UK, reported that in 2009, CNP fraud "showed a year-on-year decrease for the first time. The reasons behind the decrease include the increasing use of sophisticated fraud screening detection tools by retailers and banks, as well as the continuing growth in the use of cardholder authentication processes such as MasterCard SecureCode and Verified by Visa by both online retailers and cardholders."

EMV can also address CNP fraud, as described in the next question.

11. Can EMV address card-not-present fraud – for example, with Internet merchants?

Yes. For example, MasterCard Chip Authentication Program (CAP) and Visa Dynamic Passcode Authentication (DPA) allow EMV smart cards to be used to authenticate the user for online transactions (where no card is present). For an online transaction, the user would insert the EMV credit or debit card into a handheld reader. Once the user enters the PIN, the reader will display a one-time password which can be used to validate the user's identity. The user enters the password in the appropriate field on the merchant's checkout page (or online banking site) and the password is passed back to the issuer for authentication using the MasterCard® SecureCode™, Verified by Visa, or online banking infrastructure.

According to Toni Merschen, the former group head of chip for MasterCard International and now principal of his own consulting firm, 30 million Europeans already use EMV cards and readers for Internet transactions. These programs prevent CNP fraud on the Internet and removes the value to cyber criminals of stealing payment card numbers.

12. 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 brand 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.

13. 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 brand 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."

14. 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.

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

15. 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 brands. EMV has also published specifications for contactless POS readers that work with the payment brands' contactless applications.

The EMV specifications provide a basis for contactless EMV payments, but do not specify all payment application functionality. Payment brands 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.

16. How does NFC mobile payments relate to EMV?

With the anticipated growth in the use of Near Field Communication (NFC)-enabled mobile devices for mobile contactless payments and other mobile applications (such as coupons and loyalty), EMVCo has been active in defining the architecture, specifications, requirements and type approval processes for supporting EMV mobile contactless payments. This effort has been critical in supporting the launch of NFC mobile contactless payment in Europe, which uses an EMV-based payments infrastructure.

17. How difficult or easy would it be for the United States to migrate to EMV?

With the maturity and wide availability of EMV technology and products, U.S. migration will be less complicated now than it would have been a decade ago. Since the U.S. payments infrastructure is already an always-online environment, domestic implementation could be significantly simplified vs. previous implementations in other countries. The Smart Card Alliance provides the various options available for the United States to migrate to EMV in its white paper, "Card Payments Roadmap in the U.S."

18. Where I can learn more about EMV?

The Smart Card Alliance provides an EMV Resources web page that provides Alliance resources, industry resources, and recent articles and news on the topic. EMVCo also provides many resources on its website.

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

A good first start is to read the Smart Card Alliance white paper "Card Payments Roadmap in the U.S.," which explores roadmap options for issuers, acquirers/processors, merchants and ATM owners to move to EMV. It is an education tool for the U.S. payments industry stakeholders on the actions each stakeholder needs to consider to issue, accept and process EMV transactions.

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.