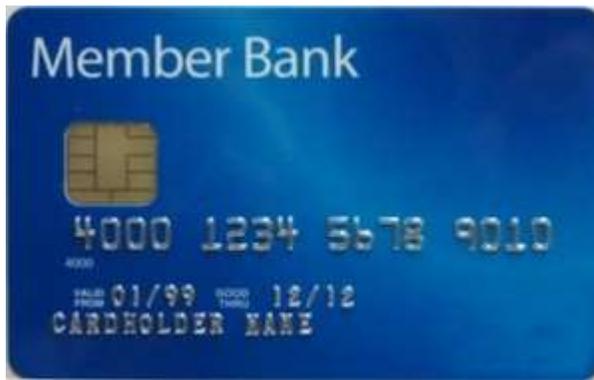# EMV Chip Payment Technology
Frequently Asked Questions

This FAQ was developed by the Smart Card Alliance to answer questions about EMV chip payment technology

- Permalink
- Share on Twitter
- Share on LinkedIn

In this FAQ:

1. What is EMV?
2. Where has EMV been adopted?
3. Why are countries migrating to EMV?
4. What are the benefits of EMV?
5. Why are EMV credit and debit cards and EMV payment transactions secure?
6. Is EMV going to be implemented in the United States? Are there any U.S. banks issuing EMV cards?
7. What are the payment brand milestones for U.S. migration to EMV?
8. What is the current status of the U.S. migration to EMV chip cards?
9. Should U.S. travelers with magnetic stripe only payment cards expect issues when traveling to countries that have implemented EMV?
10. Will travelers with EMV cards visiting the U.S. have issues paying for purchases?
11. How does EMV address payments fraud?
12. What is the proven impact of EMV adoption on payment card fraud?
13. How does card authentication work with EMV?
14. How are cardholders verified with EMV?
15. How are transactions authorized with EMV?
16. How does contactless technology relate to EMV?
17. How does NFC mobile payment relate to EMV?
18. How do EMV chip and PCI DSS work together?
19. Where I can learn more about EMV?
20. Where can I learn more about issuing EMV cards to my financial services customers?

Answers:

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, 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?** Eighty countries globally are in various stages of EMV chip migration, including Canada and countries in Europe, Latin America and Asia. According to EMVCo, as of December 2013:
   - 2.37 billion chip payment cards are in use
   - 99.9% of terminals in Europe are chip-enabled
   - 84.7% of terminals in Canada, Latin America, and the Caribbean are chip-enabled
   - 86.3% of terminals in Africa and the Middle East are chip-enabled
   - 71.7% of terminals in Asia Pacific are chip-enabled

   The United States is one of the last countries to migrate to EMV chip technology. American Express, Discover, MasterCard and Visa have all announced their plans for moving to a chip-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.
   Within the U.S., the contactless credit and debit cards that are being issued already include some EMV security features.

   U.S. issuers are already issuing EMV chip cards (see question 6 below). According to the EMV Migration Forum, 120 million EMV chip cards were issued in 2014.

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 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 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. **Is EMV going to be implemented in the United States? Are there any U.S. banks issuing EMV cards?** American Express, Discover, MasterCard and Visa have all announced their roadmaps for moving to EMV in the U.S. (See question 2)

   U.S. banks have already started issuing payment cards with EMV technology to their customers. See Figure 1. for a list of U.S. credit and debit card issuers who are issuing or who have announced plans to issue EMV payment cards.

Figure 1.   **EMV Issuers / Available EMV Cards in U.S.**

AAA Member Rewards Visa

American Express

     American Express Platinum

     Asiana Airlines American Express

     Business Platinum

     Delta Reserve

     EveryDay

     EveryDay Preferred

     Premium Corporate

     Virgin Atlantic American Express

Andrews Federal Credit Union

Bank of America

     AAA Member Rewards Signature Visa

     Alaska Airlines Visa

     BankAmericard Cash Rewards Visa

     BankAmericard Power Rewards Visa

     BankAmericard Privileges Cash Rewards

Barclaycard

     Apple Rewards card

     Barclaycard Arrival

     Carnival World MasterCard

     Diamond Resorts International

MasterCard

     Hawaiian Airlines World Elite

MasterCard

     Plus™ World Elite Signature

     BankAmericard Privileges Travel

Rewards Visa

BankAmericard Travel Rewards Visa

BankAmericard Visa

Community Bank business

Corporate One business

Corporate Travel business

Executive One business

Hawaiian Airlines Visa

Norwegian Cruise Line MasterCard

Royal Caribbean Visa

Travel Rewards Visa

BMO Diners Club Card

Chase

     British Airways Visa

     Chase British Airways Visa Signature

     Chase Freedom

     Chase Hyatt Visa Signature Credit Card

     Chase Slate

     JPMorgan Palladium Card

     JPMorgan Select Visa Signature card

     Marriott Rewards Premier

     Ritz-Carlton Rewards

     Sapphire Preferred

     Southwest Rapid Rewards Premier

     United Mileage Plus Club Visa

Citi

     AAdvantage Platinum Visa

     Chairman MasterCard

Diamond Preferred MasterCard

Hilton Honors Reserve Visa

Thank You MasterCard

Citi Commercial Cards

Citi Executive AAdvantage® Card

Citi® Hilton HHonors Reserve Card

Citi® Platinum Select® / AAdvantage®

Visa Signature Card

AAdvantage Executive World

MasterCard

AAdvantage Gold MasterCard

Citibank Platinum Select MasterCard

Citibank Dividend MasterCard

ThankYou Premier MasterCard

Citi ThankYou® Preferred Rewards Card

Citi® Diamond Preferred® Card

Citi Prestige

Citi Expedia+

First South Financial Credit Union

HSBC

Jack Henry & Associates Payment Processing

Solutions

North Carolina State Employees' Credit Union

PSCU Financial Services

Sam's Club & WalMart MasterCard

Silicon Valley Bank

World Elite MasterCard for Business

Star One Credit Union

State Department Federal Credit Union

EMV Visa Platinum

State Employees Credit Union

SunTrust

Travelex Cash Passport

United MileagePlus

United Nations Federal Credit Union

Visa Elite with EMV Chip and PIN

USAA

Preferred Cash Rewards World

MasterCard

Cash Rewards World MasterCard

Cashback Reward Plus American Express

US Bank

FlexPerks Travel Rewards Visa

Korean Air SkyPass Classic Visa

Korean Air SkyPass Secured Visa

Korean Air SkyPass Visa Signature

SKYPASS Visa Signature

Wells Fargo

Cash Back Visa and Visa Signature

Propel World American Express

Propel 365 American Express

Platinum Visa

Wells Fargo Visa Signature

Rewards Visa

Cash Back College card

7. **What are the payment brand milestones for U.S. migration to EMV?**

   Visa Milestones

   - **October 1, 2012 – PCI Audit Relief**: If more than 75 percent of merchant Visa transactions originate from EMV-compliant POS terminals that support both contact and contactless transactions, the merchant may apply for relief from the audit requirement for PCI compliance (but is still mandated to be PCI compliant).
   - **April 1, 2013 – Acquirer Compliance**. Acquirers and sub-processors must be enabled to handle full EMV chip data in transactions.
   - **October 1, 2015 – Counterfeit Card Liability Shift**. The party that has made investment in EMV deployment is protected from financial liability for card-present counterfeit fraud losses on this date. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today. This date excludes automated fuel dispensers.
   - **October 1, 2017 – Counterfeit Card Liability Shift, Automated Fuel Dispensers**. This extends the card-present counterfeit card liability shift to transactions from automated fuel dispensers.

   MasterCard Milestones

   - **October, 2012 – PCI Audit Relief**: If more than 75 percent of merchant MasterCard transactions originate from EMV-compliant POS terminals that support both contact and contactless transactions, the merchant is relieved of audit requirement for PCI compliance (but is still mandated to be PCI compliant).
   - **April, 2013 – Acquirer Compliance**. Acquirers and sub-processors must be enabled to handle full EMV chip data in transactions.
   - **April, 2013 – Cross-Border ATM Liability Shift.** At this milestone, MasterCard will extend its existing EMV liability shift program for inter-regional/cross-border Maestro ATM transactions taking place in the United States.
   - **October, 2013 – Account Data Compromise (ADC) Relief**: MasterCard has announced ADC relief for merchants. On this date, if at least 75 percent of MasterCard transactions originate from EMV-compliant contact and contactless POS terminals, the merchant is relieved of 50 percent of account data compromise penalties.
   - **October, 2015 – Fraud Liability Shift**. MasterCard liability hierarchy takes effect. The party that has made investment in the most secure EMV options is protected from financial liability for card-present fraud losses for both counterfeit and lost, stolen and non-receipt fraud on this date.
   - **October, 2015 – Account Data Compromise Relief**: On this date, if at least 95 percent of MasterCard transactions originate from EMV-compliant POS terminals, the merchant is relieved of 100 percent of account data compromise penalties.
   - **October, 2017 – Fraud Liability Shift, Automated Fuel Dispensers**. MasterCard liability hierarchy takes effect for automated fuel dispensers.

   Discover Milestones

   - **March 15, 2012.** Discover announced implementation of a 2013 mandate for acquirers and direct-connect merchants in the U.S., Canada and Mexico, to support EMV. Discover's approach will support all card authentication channels (online and offline), all cardholder verification methods (including both chip and PIN or chip and signature transactions), and all commerce channels (contact and contactless, including mobile).

   American Express

   - **April, 2013 – Acquirer/Processor Compliance**. Processors must be able to support American Express EMV chip-based contact, contactless and mobile transactions.

- **October, 2013 – PCI DSS Reporting Relief**. Merchants will be eligible to receive relief from PCI Data Security Standard (DSS) reporting requirements if the merchants' POS acceptance locations, where 75 percent of their transactions occur, are enabled to process American Express EMV chip-based contact and contactless transactions.
- **October, 2015 – Fraud Liability Shift**. American Express will institute a fraud liability shift policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology.
- **October, 2017 – Fraud Liability Shift, Automated Fuel Dispensers**. American Express fraud liability shift takes effect for transactions generated from automated fuel dispensers.

8. **What is the current status of the U.S. migration to EMV chip cards?** According to the EMV Migration Forum, by the end of 2014, an estimated 120 million chip cards had been issued to U.S. consumers and this number is expected to jump by 600 million or more cards by the end of 2015. In addition, millions of EMV-capable terminals and ATMs have been installed, some of which are accepting chip cards today.

9. **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[i].

10. **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.

11. **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.

12. **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 percent since 2004; lost and stolen card fraud fell by 58 percent between 2004 and 2009; and mail non-receipt fraud has fallen by 91 percent 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[ii]. Interac debit card fraud losses as a result of skimming hit a record low in 2013, decreasing to $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.

13. **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.

14. **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."

15. **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.

16. **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.

17. **How does NFC mobile payment 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.

18. **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 PCI 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 eco-system, 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.

19. **Where I can learn more about EMV?** The EMV Connection website (http://www.emv-connection.com) provides Alliance resources, industry resources, and recent articles and news on the topic. EMVCo also provides many resources on its website (https://www.emvco.com).

20. **Where can I learn more about issuing EMV chip 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. The EMV Connection website (http://www.emv-connection.com) also provides a number of resources for card issuers.

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.

[i]Aite Group, "The Broken Promise of Anytime, Anywhere Card Payments: The Experience of the U.S. Cardholder Abroad," October 2009. http://www.aitegroup.com/Reports/ReportDetail.aspx?recordItemID=603

[ii]Interac Association, "Chip technology helping in the fight against Interac debit card fraud," March 2012, http://www.interac.ca/en/press-releases/interac-chip-fraud-reduction.