Frequently Asked Questions
What You Should Know About EMV

You may swipe hundreds of them every day, but have you ever stopped to consider the sensitive account information contained in the nondescript strips of credit and debit cards? Consequently, stealing information from those strips has become big business in the realm of card fraud. Fast-forward to what the industry is doing to combat this trend—chip instead of strip.

The chip-based payment card contains an embedded microprocessor, a type of small computer that provides strong security features and other capabilities not possible with traditional magnetic stripe cards. There are “contact” cards—a square on the front of the card connects the chip to the reader in a terminal, and “contactless” cards—radio frequency allows the nearby card reader to accept the data while the physical card remains in the physical possession of the consumer.

Chip-based payments, with a global standard for cards, was created by Europay, MasterCard®, and Visa® (thus EMV) and is now maintained by EMVCo, LLC. According to EMVCo LLC, there are already more than 1 billion chip-based payment cards in use worldwide though the chip’s presence in the United States is only recently gaining momentum. Acquirers, issuers and technology providers across the U.S. industry, including Bank of America Merchant Services, are busy upgrading terminals and certifying acceptance of EMV. The card migration strategy enacted by issuers must align with EMV’s series of testing procedures and global specifications to achieve the ultimate goal of fraud prevention worldwide.

**EMV IN GENERAL**

**Q. What does EMV stand for?**

**A. Europay, MasterCard, and Visa.** 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, China Union Pay®, JCB®, and Visa, and includes other organizations from the payments industry participating as technical and business associates.

**Q. Who is EMVCo, LLC?**

**A. EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, MasterCard, Visa, China Union Pay, Discover and JCB, a Japan-based company.**

© 2013 Banc of America Merchant Services, LLC. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.

Merchant Services are provided by Bank of America, N.A. and its representative Banc of America Merchant Services, LLC. Banc of America Merchant Services, LLC is not a bank, does not offer bank deposits, and its services are not guaranteed or insured by the FDIC or any other governmental agency.
Q. What is the difference between a chip-based payment and that processed with a magnetic stripe on the payment card?

A. The most important difference between a magnetic strip and an embedded microprocessor, or chip, within a payment card, is that the traditional payment card with a magnetic strip can be more susceptible to counterfeit fraud through *skimming*. Skimming occurs when a card is swiped through a reader recording all necessary payment information. Later, this recorded data is used to manufacture a duplicate card. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim’s credit card out of their immediate view. Other instances of skimming have been accomplished at ATMs or fuel pumps using a device placed over the card slot that reads the magnetic strip as the user unknowingly passes their card through it.

Q. What is meant by the term “dual-interface” terminal?

A. Dual-interface refers to the ability of the terminal to accept both contact and contactless EMV chip cards or payment devices such as mobile phones. Dual-interface terminals are able to process transactions from various payment products including EMV chip contact cards, contactless cards, mobile devices, and magnetic-stripe cards.

Q. Is Visa mandating PIN implementation along with chip?

A. No. Visa continues to support a range of cardholder verification methods (CVMs) including signature, online PIN, and no-signature for low-value, low-risk transactions. Visa will maintain interoperability across those methods with technical standards, business rules, and compliance programs.

Q. Do new chip cards have a magnetic-stripe?

A. Yes. Chip cards include a magnetic-stripe to ensure that Visa-branded cards may be used everywhere they are accepted, including in environments where migration to chip technology is not complete.

Q. Is there a plan to eliminate the magnetic-stripe in the long run?

A. There are no specific plans to eliminate magnetic-stripe. Global chip migration will continue to be gradual, and until we reach ubiquity, the magnetic-stripe on the back of the card will continue to provide global acceptance interoperability.

Q. What happens if a merchant has a chip terminal and the card’s chip cannot be read?

A. The merchant will process a “fallback” transaction using the card’s magnetic-stripe. The liability shift will not apply to the merchant as long as the transaction is properly flagged as a “fallback” transaction.

Q. How will chip acceptance affect the speed of processing a transaction at the point of sale compared to what I experience today?

A. In general an online contact or contactless chip transaction should have a negligible difference in speed compared to a magnetic stripe transaction that you process today.
Q. Are all merchants expected to comply?

A. U.S. merchants are not *required* to support chip processing. However, there are many disadvantages of not staying current with the technology and commerce that the rest of the payments world embraces. The cost of fraud, which persists in unique and often elusive ways, can be much greater than what will be required in cost, time and training for the migration to EMV, whether the merchant is a small business or a multinational enterprise. Merchants in the U.S. are beginning to see international travelers coming to the U.S. to use those cards, so it’s important that the U.S. start to gain adoption of this payment type. As consumers travel here more frequently with these cards, merchants will be expected to be able to process the transactions.

Q. What changes in the checkout process can I expect for chip cards versus magnetic stripe cards?

A. For contact chip cards, your customers must insert the chip card into the payment terminal reader instead of swiping the card as they do with a magnetic stripe card. Also, your customers must leave the chip card in the payment terminal reader until the total transaction amount is known. Therefore it is recommended that the chip card only be inserted in the payment terminal reader once the total amount is available. It is also recommended that the customer-facing display prompt the cardholder when it is time to insert and remove the card, so as to train the cardholder both in leaving the card in the reader, and in inserting/removing it at the proper time. For contactless cards and mobile devices, your customers will simply hold the contactless chip card or mobile device up to the payment terminal for a few seconds, until the 4 lights flash on and a beep is heard signifying the contactless chip card or mobile device has been successfully read.

Q. What are the advantages for merchants?

A. EMV is a payment application that resides in a secure computer chip embedded into a payment device with the purpose of securely securing cardholder data, protecting data on the chip against unauthorized modification and reducing the number of fraudulent transactions from counterfeit and lost/stolen cards. In addition, EMV will prime the U.S. payments market for the acceptance of mobile and contactless transactions. The utilization of Mobile and contactless technologies will assist with speeding up checkout lanes and help drive loyalty by providing merchants with the ability to provide cardholders with electronic offers and coupons.

Q. Why has the United States been slow to adopt EMV?

A. While EMV technology is far superior to the magnetic strip; most merchants in the United States have not adopted the technology yet. It has been used successfully in Europe for many years to reduce fraud resulting from counterfeit and lost stolen transactions. The ability to allow credit card acceptance to areas of the country that do not have a stable network infrastructure using EMV’s “offline” capabilities was also a driving factor in the global acceptance of EMV. However, it has been slow to be adopted in the United States.

There are a few reasons why the United States has been slow to adopt EMV. First, the U.S. has a robust network telecommunications and payment infrastructure that did not make EMV a necessity as most areas of the country have access to a network connection and are able to process an electronic payment transaction. Another reason that it has been slow to make a change is due to the costs it would take to implement EMV from a merchant, acquirer and issuer standpoint. Supporting EMV would require most merchants to make an investment in hardware and software capable of supporting EMV. Issuers would also need to re-issue all magnetic stripe cards with EMV cards that are considerably more expensive to create than a magnetic stripe card.
Q. What is the cost to merchants?

A. Merchants should plan on the following expenses: hardware and system upgrades, training, implementation and certification.

CARD BRAND MANDATES

Q. What is the timing of EMV migration here in the United States?

A. Visa, MasterCard, American Express and Discover including Diner’s Club International, and their respective PIN debit networks of Interlink, Maestro and Pulse have mandated that all acquirers will be ready to support, at the host level, EMV transactions by April of 2013. Bank of America Merchant Services and our equity partner First Data currently support EMV for all Payment Brands.

Visa, MasterCard, American Express and Discover is providing counterfeit liability protection to merchants (excluding automated fuel dispensers) supporting EMV starting October 2015. The party that has made investment in EMV deployment is protected from financial liability for card-present counterfeit fraud losses. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today.

Visa, MasterCard, American Express and Discover is providing counterfeit liability protection to Petroleum merchants using automated fuel dispensers supporting EMV starting October 2017. The party that has made investment in EMV deployment is protected from financial liability for card-present counterfeit fraud losses. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today.

Q. What about American Express?

A. By April 2013, processors must be able to support American Express EMV chip-based contact, contactless and mobile transactions.

Beginning October 2013, merchants will be eligible to receive relief from PCI Data Security Standard (DSS) reporting requirements if the merchants’ point-of-sale (POS) acceptance locations, where 75% of their transactions occur, are enabled to process American Express EMV chip-based contact and contactless transactions.

October 2015, American Express will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. U.S. fuel merchants will have an additional two years, until October 2017, before the FLS takes effect for transactions generated from automated fuel dispensers.

Q. What are the key dates that Bank of America Merchant Services is following?

A. Effective April 1, 2013, acquirer processors and sub-processors must ensure their systems support merchant EMV chip acceptance by certifying their ability to carry and process the additional data in EMV chip transactions, including the cryptographic message that makes each transaction unique.

Effective October 1, 2015 (October 1, 2017 for Automated Fuel Dispensers), Visa’s global POS counterfeit liability shift will be instituted in the U.S. With this liability shift, liability for counterfeit fraud will shift to the party that has not made the investment in EMV chip cards (issuers) or terminals (merchants’ acquirers).
MasterCard, unlike Visa above, has two components of their announced liability shift, one for Chip and one for Chip and PIN.

Chip: Effective October 1, 2015 (October 1, 2017 for Automated Fuel Dispensers), MasterCard’s chip liability shift will be instituted in the U.S. With this liability shift, liability for counterfeit fraud will shift to the party that has not made the investment in EMV chip cards (issuers) or terminals (merchants’ acquirers).

Chip & PIN: Effective October 1, 2015 (October 1, 2017 for Automated Fuel Dispensers), MasterCard’s chip & PIN liability shift will be instituted in the U.S. With this liability shift, liability for lost, stolen, or NRI (not received as issued fraud) will shift to the party that has not made the investment in EMV PIN-prefering chip cards (issuers) or PIN-prefering terminals (merchants’ acquirers).

American Express: By April 2013, processors must be able to support American Express EMV chip-based contact, contactless and mobile transactions.

Beginning October 2013, merchants will be eligible to receive relief from PCI Data Security Standard (DSS) reporting requirements if the merchants’ point-of-sale (POS) acceptance locations, where 75% of their transactions occur, are enabled to process American Express EMV chip-based contact and contactless transactions.

October 2015, American Express will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. U.S. fuel merchants will have an additional two years, until October 2017, before the FLS takes effect for transactions generated from automated fuel dispensers.

Discover: In alignment with U.S. EMV migration timelines, Discover is introducing Fraud Liability Shift for Discover Network (in the U.S., Canada and Mexico) and PULSE (in the U.S.), effective October 1, 2015 at point-of-sale terminals and Oct. 1, 2017 at automated fuel dispensers. This Fraud Liability Shift policy will be a risk-based payments hierarchy that benefits the entity that leverages the highest level of available payments security. As Fraud Liability Shift is already in place for Diners Club International (effective December 31, 2012 for mandated participants), Discover will have one standard liability shift policy in place across all networks by October 1, 2015.

Starting October 2013, Discover will also grant annual PCI audit waivers for merchants that process 75% of Discover Network transactions via terminals supporting both contact and contactless payments.

**EQUIPMENT**

**Q. What POS terminal equipment is needed for a merchant to become EMV capable?**

**A.** On February 19, 2013, the FD35 enabled with EMV/NFC was released in production supporting the following POS devices:

- FD50Ti with the FD35 EMV/NFC peripheral
- FD100 and FD100Ti with the FD35 EMV/NFC peripheral
- FD200 and FD200Ti with the FD35 EMV/NFC peripheral

Merchants using an Integrated POS system, Multi-Lane POS devices and/or Unattended Cardholder Activated Terminals (UCAT) will need to insure their terminals are EMV capable and Level 1 and Level 2 certified.
Q. Will a merchant be able to start taking EMV cards once they have the FD35 EMV and NFC capable peripheral?

A. The hardware release of the FD35 peripheral is EMV/NFC capable and can be enabled for EMV/NFC acceptance through a merchant application download effort. Bank of America Merchant Services updated the processing system in November 2012 with the required host changes to support full EMV/NFC transaction processing.

Q. What POS terminal software will be enhanced to support EMV and NFC?

A. On February 19, 2013, the FD35 enabled with EMV/NFC was released in production supporting the following POS devices: (Nashville Only)

- FD50Ti with the FD35 EMV/NFC peripheral
- FD100 and FD100Ti with the FD35 EMV/NFC peripheral
- FD200 and FD200Ti with the FD35 EMV/NFC peripheral

FDACS is in the process of rolling out the following hardware and software applications that will be enabled to support EMV/NFC on the Buypass and Nashville frontend platforms. Production release dates are TBD.

<table>
<thead>
<tr>
<th>Terminal</th>
<th>Peripheral Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD130</td>
<td>Integrated EMV/NFC</td>
</tr>
<tr>
<td>FD130Duo</td>
<td>FD35 EMV/NFC</td>
</tr>
<tr>
<td>FD55</td>
<td>VeriFone Vx805 EMV/NFC</td>
</tr>
<tr>
<td>FD300 and FD300Ti</td>
<td>FD35 EMV/NFC</td>
</tr>
<tr>
<td>FD400GT</td>
<td>Integrated EMV/NFC</td>
</tr>
<tr>
<td>VeriFone Vx520</td>
<td>VeriFone Vx805 EMV/NFC</td>
</tr>
<tr>
<td>VeriFone Vx520</td>
<td>Integrated EMV/NFC</td>
</tr>
<tr>
<td>VeriFone Vx570</td>
<td>VeriFone Vx805 EMV/NFC</td>
</tr>
<tr>
<td>VeriFone Vx510 DC</td>
<td>VeriFone Vx805 EMV/NFC</td>
</tr>
<tr>
<td>VeriFone Vx680 wireless</td>
<td>Integrated EMV/NFC</td>
</tr>
<tr>
<td>Equinox T4205</td>
<td>Apollo CFD EMV/NFC</td>
</tr>
<tr>
<td>Equinox T4210</td>
<td>Apollo CFD EMV/NFC</td>
</tr>
<tr>
<td>Equinox T4220</td>
<td>Apollo CFD EMV/NFC</td>
</tr>
<tr>
<td>Equinox Apollo AIO (All-in-One)</td>
<td>integrated EMV/NFC</td>
</tr>
<tr>
<td>FD Advanced POS Restaurant Solution</td>
<td>VeriFone Vx805 EMV/NFC</td>
</tr>
</tbody>
</table>

CERTIFICATION AND TESTING

Q. What is the certification process for EMV?

A. The certification process a merchant follows to support EMV is going to be dependent on the type of POS system that is being used and the EMV requirements that will be supported (i.e. Online and Offline Card Authentication, Cardholder Verification Methods, support for Contact and Contactless transactions). Types of POS systems include Stand-Alone Terminals, Integrated POS systems, Multi-Lane POS devices and Unattended Cardholder Activated Terminals (UCAT).

© 2013 Banc of America Merchant Services, LLC. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.

Merchant Services are provided by Bank of America, N.A. and its representative Banc of America Merchant Services, LLC. Banc of America Merchant Services, LLC is not a bank, does not offer bank deposits, and its services are not guaranteed or insured by the FDIC or any other governmental agency.
Stand-Alone Terminals typically provide the ability to authorize and clear a transaction directly to the processor. A Stand-alone Terminal usually is not connected to a merchant’s Electronic Cash Register; rather it connects directly to the host processor. When using this type of terminal you will want to ensure your equipment is capable of supporting EMV for both Contact and Contactless transactions. Bank of America Merchant Services offers multiple types Stand-Alone Terminals that support EMV and will work with you to identify the POS equipment that best meets your processing needs.

Merchants using an Integrated POS system, Multi-Lane POS devices and/or Unattended Cardholder Activated Terminals (UCAT) will need to insure their terminals are EMV capable and Level 1 and Level 2 certified. A Letter of Approval required to be provided from your terminal manufacturer prior to beginning certification with the acquirer. Utilization of testing tools (test cards and simulators) provided by an accredited testing facility will be required. Merchants should anticipate a lengthy certification process that will take approximately 12 months depending on the POS environment, EMV requirements being supported and level of EMV expertise from the merchant and/or POS vendor’s development teams. A typical EMV certification will require hardware and software modifications to a merchants POS environment and it is expected that merchant and their POS vendors will be required to support unit testing, regression testing, user acceptance testing and Association testing for each Payment Brand being supported. As a part of the implementation process, Bank of America Merchant Services will work with you to ensure you understand the options available to support EMV and will assist with creating the project requirements and developing the implementation strategy.

IMPLEMENTATION OPTIONS

Q. Is EMV the same thing as “Chip and PIN?”

A. No. EMV commonly referred to as “chip technology.” 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.

Chip and PIN is an implementation option for EMV processing. That is, Chip and PIN may be used or Chip and Signature or Chip and no card verification method for some cases, e.g., low-value transactions.

Q. Is PIN more secure than signature?

A. There is information available that states that signature is a weaker card holder verification method than PIN. While Visa does not distinguish between PIN and signature, MasterCard does state that using PIN is a less risky option than signature.

Q. What are a merchants implementation options?

A. If a merchant and/or vendor is certifying to FDCS, the go forward solution is Rapid Connect. Rapid Connect was created by First Data to allow for easier/faster certifications into the FDCS platforms by providing a tailored message specification that will eventually interface to all FDCS platforms. Merchants and/or vendors may also request to use the standard industry specifications (ISO8583, ATL105, etc). Granting the use of these specifications will require approval from FDCS Global Partner Management.

Q. What is Rapid Connect?

© 2013 Banc of America Merchant Services, LLC. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.

Merchant Services are provided by Bank of America, N.A. and its representative Banc of America Merchant Services, LLC. Banc of America Merchant Services, LLC is not a bank, does not offer bank deposits, and its services are not guaranteed or insured by the FDIC or any other governmental agency.
A. Rapid Connect was created by First Data to allow for easier/faster certifications into the FD platforms. Rapid Connect provides for a global one-message specification using XML messaging that will eventually interface to all FD platforms. It provides a web portal for developers, third parties and merchants to access the tool and create/manage their own certification projects and allows the developers to manage their own testing through a test sandbox. Only the final certification requires the intervention of the FD Support team. By speeding up the certification process, more third parties and merchants will be able to access all FD products, thereby increasing Bank of America Merchant Services cross-sales opportunities.

Q. Who determines if PIN or signature is required?

A. While the card organizations can determine what they require, the decision is ultimately made by the card issuer. Upon card creation and personalization, the issuer will determine which card holder verification methods they will accept for a specific transaction. For example, if the issuer will only accept PIN, if the merchant POS does not allow PIN, e.g., no PIN pad, then the merchant cannot accept the card.

Q. How will EMV affect a merchant’s HSM and PIN encryption?

A. Online PIN processing does not change with EMV. A merchant can continue using their HSM to manage their PIN-pad devices as they do today.

Methods of implementation:

- Authorization through Bank of America Merchant Services/First Data front end—Merchant POS can encrypt the PIN and send Bank of America Merchant Services the PIN block just like magnetic stripe; Bank of America Merchant Services/First Data HSMs will handle the decryption process.
- Authorization through DEX—Merchants can use the same HSM they use for PIN debit today for EMV.

Q. What is “online” vs. “offline” card authentication?

A. 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.

Online card authentication requires the transaction to be sent online for the issuer to authenticate and authorize in the same way magnetic stripe transactions are sent online today in the U.S. The important difference is the chip card’s use of symmetric key technology to generate an application cryptogram which is validated by the issuer during the online authorization request.

Offline card authentication involves the EMV card and EMV terminal without connection to the issuer host. Three methods of offline card authentication are static data authentication (SDA), dynamic data authentication (DDA) and combined DDA with application cryptogram (CDA). The principle of offline card authentication is to establish a chain of trust without the need for an online connection.

Q. If a card is processed “offline” for card authorization must it also be processed “offline” for the transaction authorization?

A. No. If a card is authenticated “offline”, the transaction may be authorized “offline” as well as “online”. If the card is authentication is “online”, the transaction will be required to be authorized “online” as “offline” will not be supported. Due to the U.S. having a robust network structure
compared to other parts of the world, it is expected that transactions will be authorized “online” with the exception of a few industries where “offline” may make sense.

**Q. Will Bank of America Merchant Services support online PIN for credit EMV transactions?**

**A.** At this time, Bank of America Merchant Services cannot commit to supporting online PIN for credit EMV. Supporting Online PIN for credit in the U.S. will require a substantial investment for acquirers to support (larger than EMV initiative), and an equally substantial investment will be required by merchants, POS providers, networks and issuers. The entire payment ecosystem as a whole must agree that this is a legitimate path forward before taking necessary steps for implementation. We will continue to receive guidance and monitor steps merchant, POS providers, networks and issuers are taking that would signal adoption of this CVM for credit.

**DATA SECURITY**

**Q.** Will TransArmor® (encryption and tokenization) be needed if implementing EMV?

**A.** We recommend it. TransArmor is a complementary solution to be used with EMV. The purpose of EMV is to provide fraud protection against counterfeit, lost and stolen cards at the point of sale. When using EMV, cardholder data is still provided to the acquirer in the clear unless an encryption product such as TransArmor is used. The purpose of TransArmor is to protect sensitive card data against theft or exposure from the point of swipe through storage in back-end systems – in transit, in use and at rest.

**CONTACTLESS**

**Q.** Will implementing EMV include EMV contactless?

**A.** Not necessarily. EMV Contact and Contactless are considered separate requirements; however the Payment Brands are encouraging both to be implemented at the same time. Visa and MasterCard are also providing PCI DSS Audit Relief if both Contact and Contactless are supported.

**Q.** Will PayPass and Paywave still be accepted?

**A.** Yes. Both Visa and MasterCard have updated their specifications to include EMV versions of their current contactless payment methods.

**Q.** What will be required for my POS to support coupon programs?

**A.** While upgrading POS machines and terminals to accept EMV and EMV contactless, this would be a good opportunity to incorporate new payment acceptance methods like coupon, loyalty and marketing programs. Merchants should also use EMV as an opportunity support additional products such as TransArmor and Dynamic Currency Conversion and incorporate the development of these products into their roadmap plans to support EMV.

**ECOMMERCE**

**Q.** Will EMV lower eCommerce fraud as well?
A. No. In fact, eCommerce fraud may increase as EMV gains critical mass in the U.S. being shifted from the more secure face-to-face chip option to the weaker link.

However, we will provide fraud tools to help mitigate this shift to eCommerce.

Q. What approach does Bank of America Merchant Services recommend?

A. Merchants should determine timing for their EMV implementation based on the impact of the card brand liability shifts and a holistic assessment of existing and new payment technologies including:

- Mobile payments / NFC
- TransArmor (encryption and tokenization)
- eWallets
- Deals and offers
- Loyalty applications
- Others influencing the way we shop

The EMV POS upgrade is an opportunity to incorporate additional security, new payment acceptance methods and customer retention applications to keep up with the changing world of how customers around the world pay – and shop.