Europay, MasterCard®, Visa® (EMV)
Frequently Asked Questions

The Next Generation of Payments
Payment technology is changing, and transforming the merchant and consumer experience worldwide. Safe, simple and smart ways to pay have led to the new Europay, MasterCard, Visa (EMV) product. EMV chip cards contain embedded microprocessors that provide strong transaction security features.

What is EMV?
EMV is a global standard for secure payments between chip-embedded credit and debit cards (referred to as chip cards or smart cards) and point-of-sale (POS) devices. The standard was developed by Europay, MasterCard, and Visa (EMV) in the mid-1990s. Europay has since merged with MasterCard.

What is an EMV chip card?
EMV chip cards, also known as chip cards, are the new wave of credit and debit cards developed around the EMV standards. The chip cards are embedded with a microprocessor chip, which stores and protects cardholder information, like the card account number, and securely transmits data during a transaction. Currently, all transaction data is stored on the magnetic stripe on the back of credit and debit cards.

Why is the United States transitioning to EMV?
Card issuers have been including chips in bank cards in over 80 other countries around the world since the mid-1990s. The magnetic stripe technology that is currently used on credit and debit cards in the U.S. dates back to 1960. While cards with a magnetic stripe are relatively inexpensive to produce, they tend to be more susceptible to fraud through "skimming."

Skimming is a criminal act where a small, hard-to-detect device is used to scan credit and debit cards, to steal and store information from the magnetic stripe of the cards. Information stolen can then be programmed to another magnetic stripe card (counterfeit card) to make fraudulent purchases.

With more than a billion EMV cards issued in the rest of the world and projections for continued growth in EMV card issuance outside of the United States, criminals are expected to aggressively move magnetic stripe card counterfeiting activities to the United States1. The U.S. is now actively implementing the adoption of EMV chip cards and EMV-compliant terminals to increase security and reduce fraud.

What are the benefits of EMV?
The biggest benefit of EMV to businesses is the reduction in card fraud resulting from counterfeit, lost and stolen cards. EMV also provides businesses with the ability to accept and process chip cards for their customers on any EMV-capable payment terminal in the world. EMV technology supports enhanced cardholder verification methods and, unlike magnetic stripe cards, EMV payment cards can also be used to secure online payment transactions.

Why are EMV transactions secure and effective in preventing fraud?
First, EMV cards have a microprocessor chip that can execute cryptographic (special code similar to encryption) processing and store data securely. The chip card microprocessor carries security credentials that are encoded by the card issuer, which help prevent card skimming and counterfeiting.

Second, when an EMV transaction occurs, the card is authenticated as genuine. The cardholder is verified, and the transaction includes "dynamic data." Dynamic data is ever-changing, which means no transaction will have the exact same data, unlike in a magnetic strip transaction.

Third, 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 environment, since every EMV transaction carries dynamic data.

Is new equipment required?
For most merchants, the answer is yes. Most terminals used by merchants are not set up with EMV capabilities. U.S. processors are required to upgrade their processing systems to recognize and transmit EMV transaction data by April 2013. Please contact our Merchant Customer Service Center at (888) 849-6012 if you need more information about your terminal capabilities.

What is required of the merchant?
There are no requirements for merchants at this time. However, the shift to EMV chip cards and the adoption of EMV processing has several implications for merchant businesses. It is highly recommended that merchants update to an EMV-capable terminal to benefit from the emergence of EMV processing and technology in the U.S.
What are the implications of EMV to my business?
First, consumers will have debit or credit cards that may not work at merchant stores that do not update to an EMV terminal, possibly resulting in a loss of sales.

Second, the added security of EMV processing is available to businesses beginning April 2013 with an EMV-capable POS device.

Third, card brands have set timeframes for the liability of fraudulent purchases to shift from card issuers to card-present merchants that do not accept purchases via an EMV terminal. This liability shift is planned to be instituted in the U.S. effective October 1, 2015.

Fourth, the adoption of EMV will require processors to create updated POS terminal applications. Updated applications replace older applications and over time result in older units no longer being supported for processing.

Last, PCI requirements may be minimized if certain criteria are met.

Again, please contact our Merchant Customer Service Center at (888) 849-6012 if you need more information about your terminal capabilities.

Will there be non-compliance fees for merchants that do not upgrade to an EMV-capable POS terminal?
Today, there are no non-compliance fees associated with not upgrading to an EMV terminal. However, merchants who do not switch over may lose out on business due to non-acceptance of the new EMV chip cards. In addition, merchants without EMV-capable POS terminals will bear more liability on fraudulent charges.

What if I don’t upgrade to an EMV-capable POS terminal (the 2015 liability shift from card issuers to merchants)?
Effective October 1, 2015, Visa’s global POS counterfeit liability shift will be instituted in the U.S. This means that if a merchant does not have a POS that accepts EMV cards, then the merchant will be held liable for all fraudulent transactions from that date forward. In addition, all card issuers who haven’t transferred cards over to EMV chip cards will be held liable for fraudulent charges.

How will I process card-not-present transactions and who will be liable for the fraud?
For now, EMV cards will not change how you process card-not-transactions (CNP) or shift its fraud liability. U.S. merchants will continue to be financially responsible for fraudulent CNP transactions.

You may have heard EMV technology does allow for multi-factor authentication on e-commerce transactions or online accounts, enabling cardholders to insert their chip cards in a handheld reader and enter their PIN. However, this feature has not been adopted in the U.S. at this time.

To help detect a potential fraudulent CNP transaction, you may use the Address Verification Service (AVS) and verify the card’s three-digit security code. Please contact our Merchant Customer Service Center at (888) 849-6012 if you need more information on how to use these fraud detection tools.

Does the liability shift apply to small ticket and/or No Signature Required transactions?
Yes, it applies to all transaction types regardless of cardholder verification method. The liability shift pertains only to counterfeit fraud. Today, the U.S is not instituting a lost and stolen fraud liability shift.

Where can I learn more about EMV?
EMVCo provides many resources on its website. The Smart Card Alliance also provides an EMV resources web page. Website links are below:

- www.EMV-connection.com
- www.EMVCO.com
- www.smartcardalliance.org/