TSYS Merchant Solutions℠

EMV®, Tokenization, & Encryption:

The Path to Securing your Small Business

Time is growing short for merchants in the United States making the move to EMV. Anyone accepting credit cards for payment in the U.S. should be ready to accept EMV chip cards by October 1, 2015. For most merchants, this requires the updating of point-of-sale (POS) devices and systems.

Fraud is Fueling the Transition

In the U.S., the majority of consumers use less secure magnetic stripe cards to pay for goods in person. When swiped, information contained on the card's stripe – including the account holder's name, card number, and expiration date – can be intercepted or hacked from the retailer's data system.

EMV cards fight fraud by storing cardholder information within an embedded, secure computer chip. Since much of the world began moving to EMV in 1994, millions of cards and POS terminals have been issued, making EMV chip the standard for in-person payments around the globe. The transition has also helped nations like the U.K. achieve all-time lows for credit card fraud.

Upgrading to EMV

In addition to the fraud-fighting advantages of EMV cards and systems, there will be consequences for merchants and others who fail to update their systems by the October 2015 deadline.

Right now, when an in-store transaction is made using a counterfeit, stolen, or compromised card, losses from the transaction, depending on the card's terms and conditions, tend to fall on the merchant or issuing bank.

After October 1, 2015, losses will be the responsibility of whichever party is the least EMV-compliant in a fraudulent transaction. And that is before any additional fines and penalties.

What Is EMV?

EMV stands for Europay®, MasterCard®, and Visa®, although it's now grown to include partners like American Express®, Discover®, JCB®, and UnionPay®.

The primary technology for EMV cards is a small computer chip, which offers better protection against fraud. Cardholder data on magnetic stripe cards is extremely vulnerable to theft as it is transmitted from card readers to a POS server or a merchant's server. Since all purchasing data used on magnetic stripe cards is static and doesn't change when someone gains access to this information, it's easy to use.

Conversely, each time an EMV-compliant card – sometimes referred to as a chip-and-PIN card (because it may require a PIN), a smart card, a chip card, or a chipped card – is used for a transaction, it creates a unique, dynamic authentication code for that specific purchase which cannot be used again. So even if the data is intercepted or acquired by thieves, it is very difficult to use.

The move to EMV is great news for retailers in the United States, who lost an estimated $5.4 billion to credit card fraud in 2012. It's important to note that EMV technology focuses on fighting fraud during card-present or in-person purchases. For now, it does not prevent fraudulent transactions made online or over the phone.

Setting Up Your Business for EMV

While putting a strategy in place for accepting EMV chip cards might sound overwhelming, there is no need to panic. The experts at TSYS Merchant Solutions are standing by to help plan and implement the conversion.

It's important to note that EMV compliance only affects merchants accepting in-person or card-present transactions. Online retailers, mail order, and telephone order businesses are currently not affected. Although, as EMV chip cards help to fight in-person fraud, thieves are expected to turn their attention to other merchants, such as those accepting card-not-present transactions, where fraud is easier to commit. Card-not-present merchants are encouraged to follow best practices from the card brands and the PCI Security Standards Council to discourage fraudulent activity.

The conversion process may require merchants accepting in-person payments to upgrade POS devices and software to accept transactions initiated with EMV chip cards and NFC (near field communication) devices. Once updated, employees may need training on handling the new cards and NFC devices. While information may differ from system to system, overall payment processes for chip cards and NFC should remain the same.

Aside from meeting the EMV standard, a new POS system is a great investment. For starters, chip cards and NFC-enabled devices will be the dominant payment methods of the future. Second, it could help to save money.

As noted earlier, when EMV compliance takes effect in October 2015, counterfeit fraud liability will shift to those who are less EMV compliant in any given situation. So if someone makes a fraudulent purchase at a business after October, and the merchant has not switched to an EMV POS system, chances are the merchant will be on the hook for damages.

Upgrading to EMV-enabled POS devices and systems might also increase customer satisfaction. Consider how much faster the checkout/payment process will be when customers use NFC payments, which simply require a tap or wave of a card or mobile device near the POS device to complete a transaction.

For many merchants, the smartest approach to purchasing an EMV-ready POS system may be to find one that incorporates both EMV and NFC. This one-and-done approach allows them to offer customers both types of payments.

Why the Delay to Adopt EMV in the U.S.?

Why is the U.S. lagging in EMV chip card adoption? With millions of magnetic stripe cards still in use by consumers around the country, upgrading to EMV chip cards is an expensive proposition. There are also costs associated with updating millions of merchant POS card readers and systems.

But cost is not the only reason. U.S. card issuers are very good at detecting and preventing fraudulent activity, unlike their counterparts in other countries. Without the level of fraud-fighting sophistication found in the U.S., the switch to EMV cards was a necessity for issuers in other countries. Additionally, credit card companies in Europe were always liable for costs associated with fraud, while in the U.S., some fraud is covered by retailers and consumers.

Now, retailers are leading the charge for EMV reform in the U.S. Companies like Whole Foods Market®, Home Depot®, Target®, Walgreens® and Walmart® have already made the switch to chip card readers. In October 2014, President Barack Obama signed an executive order requiring the federal government to adopt EMV technology for all government payment cards, and to update all POS terminals at federal facilities, such as post offices and national parks.

The Fundamentals of EMV Payments

Instead of swiping an EMV card, as consumers would with a magnetic stripe card, the card is inserted into a POS device. The card stays there during the entire transaction, while the consumer types a PIN or signs a receipt. When the transaction is finished, the card is removed from the reader.

Dual-interface cards – those with both a chip and NFC-enabled contactless antenna – can also be "tapped" or "waved" to complete a transaction. This method is generally seen as being much faster than standard transactions, but as of now, much like EMV, the process in America is still not widespread.

Magnetic stripes will not vanish completely. They will still be found on chip cards in the event of a purchase initiated via a traditional terminal.

EMV, Encryption, and Tokenization

In addition to EMV, merchants should consider adding encryption and tokenization to their fraud-fighting arsenal to protect and secure transactions.

Encryption

Encryption is a process that begins at a POS terminal and protects a transaction throughout its short lifecycle. Encryption works by converting a transaction's plain text information, or primary account number (PAN), into an unreadable format called "ciphertext." Once the plain text has been converted to ciphertext, a code key is needed to decipher the information and return it to its original format.

With encryption, whenever a transaction is initiated – whether via the swipe of a card, the insertion of an EMV card, or the wave of an NFC device – data is scrambled and useless to any thief who intercepts it without the key. This can seriously reduce the pilfering of valuable transaction data.

Tokenization

Tokenization is a method for protecting card data by substituting a card's Primary Account Number (PAN) with a unique, randomly generated sequence of numbers. This "token" can be reversed to its true associated PAN value at any time with the right decryption keys. Tokens can be either single- or multi-use.

The number is the same length and format as the original PAN; it is no different from a standard payment card number in the virtual eyes of back-end transaction processing systems, applications and storage tools. The random token sequence acts as a substitute value for the actual PAN while the data is at rest inside an issuer's or retailer's systems. Tokenization eliminates the need for merchants, e-commerce sites and operators of mobile wallets to store sensitive payment card data on their networks.

Payment tokenization allows a consumer to register a payment card with a mobile wallet or online store and replace the actual card number with a payment token number used for that merchant or wallet vendor.

Ensuring PCI Compliance

The PCI Security Standards Council recommends merchants install or enable encryption and/or tokenization to ensure transaction security, and advises all merchants to ensure they are meeting PCI standards.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of data security requirements governed by major card brands to protect cardholder account information. PCI DSS includes best practices to identify vulnerabilities in processes, procedures, and website configurations. These practices help businesses protect themselves against security breaches, safeguard customer data, and secure payments.

Retaining PCI compliance is an ongoing maintenance process that allows merchants to offer secure payment options, protect their business, and instill customer confidence.

Benefits of PCI compliance help mitigate the risks of non-compliance, which may include fines, penalties, lawsuits, insurance claims and a loss of reputation.

PCI DSS Best Practices to Protect Customer Information:

1	Install and maintain a firewall configuration to protect data.
2	Do not use vendor-supplied defaults for system passwords and other security parameters.
3	Protect stored cardholder data.
4	Encrypt transmission of cardholder data across open, public networks.
5	Protect all systems against malware and regularly update anti-virus software or programs.
6	Develop and maintain secure systems and applications.
7	Restrict access to data by business need-to-know.
8	Identify and authenticate access to system components.
9	Restrict physical access to cardholder data.
10	Track and monitor all access to network resources and cardholder data.
11	Regularly test security systems and processes.
12	Maintain a policy that addresses information security for all personnel.

References

- **"EMV and Encryption + Tokenization: A Layered Approach to Security,"** a First Data White Paper, 2012: http://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF
- **"Cutting Through EMV Hype and Confusion In The U.S.: Where We Are, Where We Should Be, and How to Become EMV Compliant,"** Jeremy Gumbley, Creditcall, 2014: http://www.pymnts.com/creditcall-emv-ebook/#.VUqSK_lVhBc
- **"A Brand New Checkout Experience: EMV Transformation"** by Gelmalto and Verifone, 2013: http://global.verifone.com/media/3710276/gemalto_emv_transformation.pdf
- **"EMV: The Next Twelve Months,"** by PYMNTS.com, Gemalto, Oberthur, Datacard, Creditcall, and Moneris, 2014: http://www.pymnts.com/emv-ebook/#.VUqTUflVhBc
- **"Preparing Your Small Business for EMV,"** PaySimple.com, 2015: http://paysimple.com/blog/2015/02/10/preparing-your-small-business-for-emv/
- **"Lack of EMV Means US Leads The World in Card Fraud,"** Bankingtech.com: http://www.bankingtech.com/173772/lack-of-emv-means-us-leads-the-world-in-card-fraud/
- **"8 FAQs About EMV Credit Cards,"** CreditCards.com, 2015: http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php
- **"Credit Card Fraud Falls to a 10-Year Low,"** Telgraph, UK, 2012: http://www.telegraph.co.uk/finance/personalfinance/borrowing/creditcards/9127605/Credit-card-fraud-falls-to-a-10-year-low.html
- **"PCI DSS Tokenization Guidelines",** Scoping SIG, Tokenization Taskforce, PCI Security Standards Council, 2011 https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

TSYS®

GET TO KNOW US

at **merchantsales@tsys.com**, or contact us at **800.354.3988** to learn more about how we can work together to put people at the center of payments.

1601 Dodge Street • Omaha, NE 68102 • 800.354.3988

ABOUT TSYS MERCHANT SOLUTIONS

TSYS Merchant Solutions is a leading payment processor with more than 30 years of experience providing first-rate service and comprehensive end-to-end payment solutions to businesses accepting payments across North America. Our dedicated, experienced team of industry professionals provides innovative card-acceptance solutions and unparalleled customer service every day to meet the long-term needs of our customers.

TSYS Merchant Solutions is a wholly owned subsidiary of TSYS® (NYSE: TSS). TSYS delivers advanced technology and enhanced value to many of the world's leading companies, making it possible for hundreds of millions of consumers to use their credit, debit, commercial, private-label, prepaid and chip cards safely and securely.

www.facebook.com/tsysmerchant

www.twitter.com/tsysmerchant

www.youtube.com/tsysmerchant

www.plusgoogle.com/+tsysmerchantsolutions

www.linkedin.com/company/tsysmerchantsolutions

GET TO KNOW TSYS

AFRICA	ASIA-PACIFIC	COMMONWEALTH OF INDEPENDENT STATES	EUROPE	INDIA & SOUTHEAST ASIA	MIDDLE EAST	NORTH & CENTRAL AMERICA, MEXICO & THE CARIBBEAN	SOUTH AMERICA
+27 21 5566392	+603 2173 6800	+7 495 287 3800	+44 (0) 1904 562000	+911204191000	+971 (4) 391 2823	+1.706.644.3819	+1.706.644.3819