EMV:
Preparing for the shift

The impending shift in liability for card-present fraud is driving a transition to EMV, which comes replete with new retail IT requirements and consumer-facing changes to the payment experience. Are you ready?

By Raymond Moorman, Director of Product, Element Payment Services
and Brendan Miller, Sr. Product Marketing Manager, Mercury

MERCURY®

Overview

On October 1, 2015, the first major push by the card brands for retailers' adoption of EMV (Europay®, Mastercard® and Visa®) technology goes into effect. It's a big one. On that not-so-distant date, merchants and acquirers—as opposed to card issuers—will assume the financial burden associated with the fraudulent use of counterfeit, lost and stolen cards. The retailers' only means of eliminating that risk is by demonstrating and documenting compliance with EMV chip card standards.

Lest you hastily react with disdain at the thought of yet more payment card security measures, we've put together a primer on what EMV is, a pragmatic analysis of its pros and cons, and a handful of helpful pointers on what to expect—and what to be doing now.

What is EMV?

The EMV standard was developed by EMVCo, a joint venture of American Express®, JCB®, MasterCard®, Visa®, and China Union Pay®. Its intent is to minimize credit card counterfeiting and improve cardholder security.

The EMV standard is based on smart card technology. While EMV chip cards look just like standard magnetic stripe cards, they contain a microprocessor, or chip, which enables every transaction they initiate to carry a unique cryptogram. That cryptogram is validated by the issuer, and it's very difficult for criminals to break it and steal card information for counterfeit use. Hence the dramatic declines in card present fraud where chip cards have been adopted. Here in the U.S., Aite Group® predicts that about 70 percent of cards in the U.S. will have EMV chips by 2015, with most card issuers delivering them in the fourth quarter of 2014 or first quarter of 2015.[1]

Why EMV? Why Now?

Since virtually every major commercial market in the world converted to the EMV standard for secure payments, the U.S. has been under siege by fraudsters. Consider that payment card fraud losses in the U.K. have dropped 36 percent from their peak since the country adopted EMV in 2001.[2] In Europe, fraud rates are falling despite increased card usage and transaction volume. The same can't be said of the U.S. In 2011, 59 percent of the more than 37 billion debit card transactions that were made were verified by signature, 85 percent of all fraudulent debit card transactions involved signature verification, and $1.15 billion of the total $1.35 billion in debt card fraud losses (85 percent) stemmed from signature debit card transactions[3]. Credit card and debit card fraud resulted in losses amounting to $11.27 billion during 2012, with card issuers and merchants incurring 63 percent and 37 percent of those losses, respectively.[3] Nilson reports that those card issuer losses occur mainly at the POS from counterfeit cards.[4] Card present fraud has migrated here to the point of rampancy, creating urgency on the part of card issuers to catch the U.S. up with the rest of the EMV-enabled world.

This urgency prompted Visa to announce the first major U.S. initiative toward EMV adoption back in 2011, in an effort to prep the retail community on the high-level requirements for EMV card deployment and acceptance. In January 2012, MasterCard also endorsed EMV and announced its own incentives for merchants who adopt the technology, including breach and lost/stolen card protection for EMV-enabled merchants. The push by the card-brands was on.

Credit card and debit card fraud resulted in losses amounting to $11.27 billion during 2012, with card issuers and merchants incurring 63 percent and 37 percent of those losses, respectively.[3]

Effective October 1, 2015, Visa will institute a liability shift for counterfeit card-present POS transactions.

Where Are We Now On The EMV Timeline?

On October 1, 2012, Visa expanded its Technology Innovation Program (TIP) to the U.S. TIP eliminates the requirement for eligible merchants to annually validate their compliance with the PCI Data Security Standard for any year in which at least 75 percent of merchants' Visa transactions originate from EMV chip-enabled terminals. While we are some ways out from that milestone here in the states, this marked the first major incentive for merchants to transition to EMV-compatible POS and peripheral systems. To qualify for the PCI validation exemption, terminals must support both contact and contactless chip acceptance, including mobile contactless payments based on near field communication (NFC) technology.

While those who implement EMV-enabled POS devices may be excused from some PCI audits and the costs associated with them, qualifying merchants must continue to protect sensitive data in their care by ensuring their systems continue to adhere to the PCI-DSS standards as applicable.

As of April 1, 2013, Visa required U.S. acquirer processors and sub-processor service providers to be able to support merchant acceptance of chip transactions. Chip acceptance requires service providers to carry and process the additional data included in chip transactions that makes each transaction unique.

We're now preparing for the most significant benchmark on the timeline. Effective October 1, 2015, Visa will institute a liability shift for counterfeit card-present POS transactions. Effectively, this means that if an EMV card is presented to a merchant that has not adopted EMV terminals, liability for counterfeit fraud may shift to the merchant's acquirer, that may then pass that liability on to the merchant. Currently, card issuers absorb the liability for counterfeit fraud. This liability shift is the most overt incentive to date to encourage merchant adoption of EMV.

Still, while the timeline has been readied for some time, we'll see in the next section that the same can't necessarily be said of the U.S. merchant community.

How Do Merchants Prepare?

For some, primarily big box retailers, in-store preparation for EMV has already begun. For many others, the acronym remains a foreign concept. Aite Group data indicates that the number of active EMV terminals will rise from 1.5 million in 2013 to 12.4 million by 2017, improving EMV's penetration at U.S. POS systems from 14 percent in 2014 to 87 percent by 2017.[5] While encouraging, these figures still

indicate a laggard approach to the October, 2015, liability shift. At the current pace of adoption, Aite Group anticipates that fewer than 60 percent of merchants will have made the migration by the end of 2015. Some industry insiders peg that figure far lower.

Merchants have understandably taken pause, given the giant investments made in networks, devices, software, and fees required to run merchant payment applications. Many have balked at the notion that an upgrade to these investments is necessary. Indeed, for some retailers, EMV might not be the right solution. In some merchant environments, the potential liability is so small that it might not be worth the retailer's time, money, and effort to implement EMV. Merchants are advised to discuss all their payment security options, including encryption, tokenization, contactless and mobile payment acceptance, with their ISVs and resellers.

While implementing payment terminals that feature EMV card slots is the foundation for EMV acceptance, doing so doesn't mark the end of the retailer's responsibility. There are also interface and integration considerations that precede device functionality and compliance—such as configuration of the POS with the requisite information to identify and engage EMV-enabled cards, and support of response codes for proper prompts and application displays at the POS (i.e. transaction process prompts, loyalty standing/point display, etc.). This is work best done in partnership with your POS provider, when working in conjunction with Mercury® can help you achieve step-by-step EMV compliance, from terminal selection through network and POS configuration.

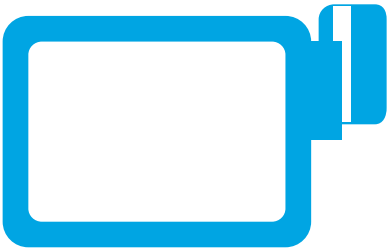
When And How Are Merchants Deemed EMV Ready?

Standard EMVCo Level 1 testing will verify that the merchant's mechanical and network requirements (including physical, electrical, and transport-level interfaces) are met. Effectively, Level 1 testing assures that the network, POS, and EMV terminal are operational per EMVCo standards. EMV Level 2 covers payment application selection and financial transaction processing, spelling out what's necessary of the software applications associated with debit and credit transactions. Level 2 considerations include the data elements that comprise the transaction interchange, software commands, and security.

What Change Will EMV Bring To The Transaction?

Many retailers are concerned about maintaining a fluid transaction experience for consumers in the context of EMV. Indeed, POS and support associates on the front lines of retail customer interaction

Standard EMVCo Level 1 testing will verify that the merchant's mechanical and network requirements are met.



U.S. merchants that have **prioritized the transition to EMV** should be working closely with their processors, acquirers and POS software providers

will play a pivotal role in the transition. Current consumer habits, such as swiping the card before the transaction, will not be an option in the EMV environment, where the transaction must be totaled before card swipe. When a consumer swipes an EMV card at an EMV-enabled terminal, the terminal will prompt the consumer to insert the card into a slot—where the chip in the card will initiate data communication with the reader—and leave it there until prompted for removal. A seemingly small change in process, yet it brings with it major throughput implications in high-volume environments. These changes in customer behavior at the POS will require training of associates, who will then bear the brunt of customer training and reinforcement responsibility. Merchants should expect an impact to their line speed due to increased transaction times and as unfamiliar consumers begin to familiarize themselves with the new transaction. Training should also be extended to help-desk, customer service, and store management staff. Additionally, the more device prompts and POS signage presented to the customer, the less likely the need for efficiency-disabling associate intervention.

Will EMV Help Or Hinder Mobile Payments?

The payment brands are certainly cognizant of the fact that nearly all adult consumers in the U.S. use smartphones. They are placing their bets on payments going mobile. Because it works well with NFC contactless technology—whether in card format or on an electronic device, EMV is inherently promising to merchants with strategic NFC-based mobile POS initiatives. Further, Visa calls for the EMV terminal's facilitation of contact-based smart card readers, contactless readers, and NFC capabilities, which will assuredly drive wider adoption of NFC-based mobile payments.

Conclusion

EMV acceptance is not a standalone payment security panacea. Rushing an EMV acceptance solution to market without encryption and tokenization in place is counterproductive. Collectively, EMV, encryption, and tokenization constitute the three pillars of a holistic merchant payment security solution. With that said, U.S. merchants that have prioritized the transition to EMV should be working closely with their processors, acquirers and POS software providers in the days leading up to the October 1, 2015, liability shift to ensure minimal disruption to the payment process as a result of deployment. EMV adoption and rollout won't be turnkey; the technology introduces a significant change to transaction protocol and speed. But the tradeoff between those concerns and the payment functionality and security enabled by EMV is measurable, with the potential to benefit cardholders and merchants alike.

For more information on Mercury Payments and your transition to EMV, go to www.mercurypay.com.

About Mercury Payment Systems

Mercury works with thousands of resellers and developers to offer small and medium size businesses a comprehensive portfolio of integrated payment products and services that help control costs and increase revenue.

Founded in 2001, Mercury's mission is to provide tech-enabled services that help small-to-medium-sized merchants compete and thrive. We are dedicated to providing our merchant and partners with the best customer service and technical expertise in the industry, 24/7.

Mercury's mission is to provide tech-enabled services that help small-to-medium-sized merchants **compete and thrive.**

Contact

Mercury - Durango, CO
150 Mercury Village Dr.
Durango, CO 81301

Mercury - Denver, CO
4610 South Ulster St.
Suite #600
Denver, CO 80237

800.846.4472
salessupport@mercurypay.com
ics@mercurypay.com

1 EMV: Lessons Learned and the U.S. Outlook, Aite Group, June 10, 2014, http://www.aitegroup.com/report/emv-lessons-learned-and-us-outlook
2 Craig Jones, UK Card Association, BBC Radio Wake Up To Money, May 20, 2013
3 PaymentsJournal, February 2012
4 Nilson Report, August 2013
5 EMV: A Roadmap and Guidebook for the U.S. Market, Aite Group, June 27, 2013 http://www.aitegroup.com/report/emv-roadmap-and-guidebook-us-market

MERCURY®