Merchant Guide: Stepping Up to EMV® Chip with PCI

This year is a big year of change for eight million merchants in the U.S. who must deploy capability to securely accept payment cards equipped with an EMV chip. An EMV chip payment card has a microprocessor chip embedded on the front side. Its role is to securely verify authenticity of a payment card offered in-person at the point-of-sale (POS). The PCI Security Standards Council plays a significant role in the EMV chip rollout in two ways. PCI Standards – particularly PIN Transaction Security – are vital for protecting cardholder data entered at the point-of-sale and onward through the payment system. PCI Standards also are an essential compliment to EMV chip technology for each addresses different aspects of payment security. Merchants should use PCI-approved point-of-sale devices that include EMV chip functionality.

Protection at the Point-of-Sale –
PIN Transaction Security with EMV Chip

PCI-listed POS devices provide:

- Strongest security protections
- EMV chip-capability
- A secure foundation to accept new payment technologies, such as mobile and contactless

This *At a Glance* describes EMV chip technology, lessons learned in using EMV, answers to frequently asked questions – and how merchants can start their transition to securely accepting EMV chip cards.

MIGRATION STEPS

- Consult your point-of-sale vendor to determine which EMV-capable devices are right for your business
- Check PCI Council website to ensure devices are PCI-approved
- Do same for payment software that runs in your payment environment
- Deploy the EMV solutions for stronger authentication at point-of-sale

What Is EMV?

EMV technology comes from EMVCo, a standards organization created to facilitate worldwide interoperability and acceptance of secure payment transactions. Today there are EMV Specifications based on contact chip, contactless chip, common payment application, card personalization, and tokenization. This work is overseen by EMVCo's six member organizations and supported by dozens of banks, merchants, processors, vendors and other industry stakeholders who participate as EMVCo Associates.

How EMV Chip Helps Merchants to Reduce Fraud

Three elements are required for use of EMV: a payment card with an embedded EMV chip; an EMV-enabled payment terminal at the physical point-of-sale; and EMV-enabled payment software for the point-of-sale terminal, and throughout the payment system to the processor or acquiring bank. When physically presented for acceptance by a merchant, an EMV chip card exchanges data with an EMV chip-activated terminal to verify that the card is genuine. The cardholder identity is verified by entering a personal identification number or signature (hence the terms, Chip-and-PIN or Chip-and-Signature). Electronic information exchange between the microchip and terminal assess the transaction details – including generation of a one-time code required for transaction approval.

EMV technology provides issuers and merchants with enhanced ability to control risk in face-to-face purchases. Merchants may accept EMV cards with non-EMV-enabled terminals and software, but will be unable to electronically authenticate those cards using the EMV chip.

EMV RESOURCES

Merchants are encouraged to consult the resources below to plan their rollout of EMV-enabled terminals and software.

- **EMV Migration Forum**
  www.emv-connection.com
- **EMVCo**
  www.emvco.com
- **American Express**
  www209.americanexpress.com/merchant/services/en_US/payment-EMV?intlink=US:Amex:NewSiteSearch:RecomLink1
- **MasterCard**
  www.mastercard.us/mchip-emv.html
- **Visa**
  www.visachip.com

PCI Security Standards Council
www.pcisecuritystandards.org

- PCI DSS Applicability in an EMV Environment
- PCI Approved PIN Transaction Security (PTS) Devices listing
- PCI Validated Point-to-Point Encryption (P2PE) Solutions listing
- And others

Preparing for EMV Chip with PCI

Tighten security at the POS – Upgrade your terminals and devices for the best security and to take the advantage of the latest technology options to enable your business.

Talk to your POS vendor to understand how they can support you

Consider any future Point-to-Point Encryption (P2PE) and tokenization plans and what additional layers of security you may want to make the best investment

Replace any version that has expired – choose a 3.1 version device or higher from the PCI Approved PIN Transaction Security (PTS) Devices listing

Check out the PCI Approved PIN Transaction Security (PTS) Devices listing and PCI Validated Point-to-Point Encryption Solutions listing on the PCI SSC website: http://www.pcisecuritystandards.org

Lessons Learned from Global EMV Chip Deployments

Based on global experience after deploying EMV chip, merchants in the U.S. will experience a drop in face-to-face card fraud. For example, in the UK and France, after deploying EMV chip technology rates of face-to-face fraud dropped more than 75% and have stayed consistently low ever since. However, as merchants strengthen security at the point-of-sale with EMV, fraudsters will shift their efforts to more vulnerable payment channels. In the UK, card-not-present fraud rose 79% in the first three years[1] after merchants switched to EMV chip cards, and card-not-present fraud has more than doubled in Australia and Canada. As they deploy EMV, U.S. merchants thus should be constantly vigilant in applying controls as specified in PCI Standards to protect cardholder data in all payment channels.

Frequently Asked Questions

Who must use EMV chip and where? American Express, Discover, MasterCard, and Visa have announced plans for moving to a chip-based payments infrastructure in the U.S., which requires merchants who accept payment cards in face-to-face transactions to use EMV-capable terminals and software at points of sale. Eighty countries are in various stages of EMV chip migration, according to the EMV Migration Forum.

When must merchants complete the transition to EMV chip? Card brands expect merchants' POS terminals and software to be EMV-capable by October 1, 2015.

Will the EMV chip solve all security problems? No. EMV primarily focuses on improving authentication of face-to-face transactions. Other payment channels such as telephone, mail, and online require different security measures to protect cardholder data, which are covered by the PCI Data Security Standard.

What about card-not-present fraud? The spike in card-not-present fraud we've seen in in other countries that have deployed EMV chip highlights the need for multi-channel protections. Combined with EMV chip at the POS, the PCI DSS provides merchants with comprehensive controls to secure card data in all environments.

Does EMV chip adoption mean PCI is no longer needed? Both are essential and address different aspects of payment security. EMV focuses on authentication of face-to-face transactions. PCI Standards focus on securing cardholder data and apply to all payment channels.

How should merchants start the EMV chip transition? Consult your POS vendor to choose devices for your payment environment. Your payment processor, acquiring bank, or card brand can provide authoritative guidance. Consult the PCI Council's PIN Transaction Security Approved Devices listing to ensure EMV devices are PCI-approved to protect cardholder data.

[1] Aite Group, cited in CreditCards.com (http://www.creditcards.com/credit-card-news/online-fraud-surge-emv-1273.php)

The intent of this document is to provide supplemental information, which does not replace or supersede PCI SSC Security Standards or their supporting documents.
EMV is a trademark of EMVCo. The EMV trademark is registered in the U.S. and other countries.