An Introduction to EMV

Summary

EMV will significantly alter the U.S. payments industry, bringing a global standard and advanced security to the point of sale, while paving the way for innovation through mobile acceptance. Every physical point-of-payment that accepts a mag-stripe card today will be updated to include the ability to accept contact and contactless EMV chip cards and related devices (smart phone, key fob, watch, etc.).

Over the next few years, EMV will act as a springboard for the implementation of a wide-range of innovative value-added smart card and mobile commerce applications. These applications will, in turn, provide a world of exciting possibilities for consumers, merchants and financial institutions.

EMV adoption will dramatically alter the way payments are made, similar to major shifts that occurred with the migration from paper to electronic processing, and again with the introduction of e-commerce and online shopping.

Smart Cards and EMV Defined

A “smart card” (also known as a “chip card”) is a device that was invented in 1977 by Honeywell Bull and contains a secure embedded circuit chip. The chip has the ability to read and write information and performs functions that validate, store and encrypt data. Cardholder data is more secure on a chip-embedded card that utilizes dynamic authentication, than on a static mag-stripe card. Unlike a mag-stripe card that can be copied (“skimmed”), chip technology combats counterfeiting by assigning a dynamic value for each transaction.

EMV is a global standard developed in 1994 for payment cards based on chip technology. Today, the EMV standard is managed by EMVCo, which is a joint venture of MasterCard, Visa, American Express and JCB. There are more than 1 billion EMV cards in circulation globally, along with nearly 20 million EMV terminals. EMV is for card-present transactions and has four main functions:

- Card authentication to protect against counterfeit cards
- Cardholder verification to protect against lost/stolen cards
- Terminal authentication to prevent hacking
- Transaction authorization to manage issuer-defined rules

There are 2 primary ways to authenticate an EMV card: signature (“Chip and Sign”) and PIN verification (“Chip and PIN”). Visa mandates global interoperability, meaning that the solutions must be capable of processing both Chip and PIN and Chip and Signature cards when presented.
Form Factors

EMV chips can be on a physical card, or can be embedded on key fobs/tags, stickers, and even in mobile phones containing the NFC (Near Field Communication) radio-based protocol. EMV-enabled payment terminals and peripherals are able to read and process the information in either by direct contact with the chip, or by close proximity through contactless (“tap and go”) technology.

**Contact:**
- Chip is embedded in the card
- The card is inserted into an EMV-enabled device

**Contactless:**
- The chip is embedded in card or other form factor
- The card/phone/key fob is held close to the reader
- Both the chip and the reader have an antenna and communicate via radio frequency
- Mobile wallets will become secure and convenient alternatives for physical wallets

EMV Benefits

The advanced security and global interoperability standards associated with EMV will benefit all parties involved in processing payments: consumers, merchants, card issuers and payment processors.

- Consumers will experience peace of mind knowing that their card information is secure. They will also be able to use cards anywhere in the world.
- Merchants will realize fewer fraud-related chargebacks due to stolen cards and skimming. They will also increase customer satisfaction with their international patrons. And they will be ready for the future of mobile wallets and other innovations.
- Card issuers and payment processors will benefit from a reduction in counterfeit card fraud. They will also be able to take advantage of innovations in mobile commerce.

The U.S. Timeline for EMV

The card schemes —Visa, MasterCard, American Express and Discover—have released EMV strategies and are all aligned on timelines and requirements. They have put both “carrots” and “sticks” in place to motivate U.S. merchants to adopt EMV within the next few years. These incentives center on the requirement for merchants to adopt dual-interface terminals, defined as those that have the ability to actually process EMV contact/contactless cards and Mobile NFC contactless payments. This will not only spur adoption of a more secure transaction, but will also fuel the innovation and growth of mobile
payment solutions. The card schemes have communicated the following timeline:

- **April 2013: Acquirer Chip Processing Mandate**
  Acquirers and processors must support the ability to process EMV transactions and NFC contactless payments.

- **October 2015: Liability Shift from Issuer to Merchant**
  Merchants of any size), will be liable for domestic and cross-border counterfeit fraud committed at the point of sale if they are not using a compliant EMV & NFC POS solution (Merchants with Automated Fuel Dispensers (“pay at the pump”) have until October 2017).
  - A *non-compliant merchant* is liable for fraud that occurs on any chip card used on a magnetic swipe terminal.
  - A *non-compliant issuer* is liable for fraud that occurs on any magnetic stripe card used on a chip card-enabled terminal.

Reaching critical mass at the point of sale is expected to take 2 – 5 years. Every payment application, point-of-sale solution, payment terminal/peripheral, and processor network must be replaced/updated, certified, and installed.

Merchants are encouraged to make the investment now in advance of the liability shift. Elavon offers a variety of EMV-enabled countertop and wireless solutions to meet the needs of a variety of merchant environments.

For more information concerning EMV and the NAEDA endorsed credit card processing program, contact Morna Kennedy at (800) 226-9332, ext. 5395 or morna.kennedy@elavon.com.