EMV

Answers to Your Questions about EMV

EMV (Europay®, MasterCard® and Visa®) is a global, open-standard set of specifications for smart cards and compatible acceptance devices (ATMs, merchant terminals, etc.). Originally developed by Europay, MasterCard and Visa, the EMV specifications define requirements to ensure interoperability between chip-based payment cards and terminals that authenticate credit and debit card transactions. EMV chip cards contain embedded microprocessors that offer greater transaction security (and other capabilities) than the magnetic stripe card technology used in the U.S.

EMVCo, owned by American Express, MasterCard, JCB and Visa, manages, maintains and enhances EMV specifications. EMV is the predominant payment technology in Europe, Asia and Canada. The U.S. is the last market in the industrialized world to adopt the standard.

Here are answers to the common questions U.S.-based financial institutions have about adopting the EMV card technology.

Q&A

Q: Does the EMV card still have a magnetic stripe like the cards we already use?

A: Yes, the EMV card will have a magnetic stripe with all the same encoded data it has today, but the magnetic stripe is used as a back-up technology in case the EMV chip fails. EMV card transactions are protected through: 1) card authentication; 2) cardholder verification to protect against lost/stolen cards; and 3) transaction authorization (online or offline) using issuer-defined rules. Online transaction authorizations proceed as they do today with magnetic stripe cards, but they include a transaction-specific cryptogram. 4) EMV cards store payment information in a secure chip rather than on a magnetic stripe and personalization of EMV cards is accomplished using issuer-specific keys. It is virtually impossible to create a counterfeit EMV card.

Q: Why is there discussion about a shift of liability from companies adopting the EMV card to those that do not deploy the new technology?

A: The card associations are trying to protect against fraud from lost, stolen and counterfeit cards. The key benefit of using the EMV card technology is it significantly reduces the risk of fraud. Adopting the technology would shift fraud liability.

Here's how the liability shift works. If an institution issues EMV-compliant cards and its cardholder uses an EMV card at a merchant that does not process via an EMV terminal (either because it doesn't use EMV terminals or it didn't process the transaction that way), the merchant would be liable for any fraud that occurs on the transaction. The converse is also true.
If a financial institution does not issue EMV cards and its customer transacts business with an EMV-compliant merchant and the merchant tries to process the transaction as an EMV transaction, the merchant is protected. Liability shifts to the financial institution.

Q: What are the dates associated with the liability shift?

A: For 2013, processors must support American Express EMV transactions; for Discover, processors and merchants must be EMV certified. For 2014, MasterCard merchant acquirers and processors must be EMV certified. By October 2015, all financial brands (MasterCard, Visa, American Express and Discover) will enforce a liability shift date to issuers. In October 2017, the liability shift will be enforced for automated fuel dispensers (AFD).

Q: What is the final deadline to comply with EMV?

A: There is no mandate to move to EMV, however, the liability shift that pertains to issuers takes place in October 2015. Harland Clarke encourages financial institutions to issue EMV cards before that date to ease the transition.

Q: Some financial institutions have been advised not to issue EMV cards until EMV standards are firmly established. What does Harland Clarke recommend?

A: EMV is a well-established, interoperable, global standard, and the card specifications are publicly released and available today. A financial institution should engage its card association, its EFT processor and its card issuers to understand how they work together on existing card programs, and discuss platform and chip options, personalization options and costs related to EMV card issuance. A financial institution needs to consider its fraud risk and the liability shift that is coming.

Q: How is a PIN used in the Chip and PIN EMV environment?

A: In the EMV environment, a PIN replaces the customer signature at the point of sale. The customer enters a PIN to verify the transaction. A PIN enables different card verification methods (CVM), including: 1) card authentication; 2) cardholder verification to protect against lost/stolen cards; and 3) transaction authorization

(online or offline) using issuer-defined rules. Online transaction authorizations proceed as they do today with magnetic stripe cards, but they include a transaction-specific cryptogram.

Q: Will financial institutions be able to establish different card verification methods (CVM)?

A: Yes, there are a number of different card verification methods that can be tied to a card program. A financial institution needs to be proactive and discuss program parameters with its card association and EFT processor. Completing the card association's questionnaire is the first step a financial institution should take.

Q: How will the EMV card affect the mobile market?

A: Already, some of today's mobile transactions are tied to EMV-certified chips used in mobile handsets. A greater number of today's mobile transactions are tied to contactless or radio frequency identification (RFID) technology. If a financial institution's EMV infrastructure is designed to handle contactless cards, it will be positioned to offer mobile payments.

Q: Isn't it possible that mobile payments technology will bypass EMV card technology?

A: It's possible, but there is no timetable for the advancement of mobile payments technology. It's difficult to anticipate what will happen. On the other hand, there *is* a timetable for implementation of EMV card technology. An institution must evaluate the financial impact of the liability shift to determine whether it's prudent to implement EMV technology now. In many instances, the financial impact of the liability shift warrants a move to EMV.

Q: Does Harland Clarke have an instant issuance solution for EMV?

A: Yes, it's called Card@Once. It is a unique, very affordable software solution that has been on the market for more than three years. Harland Clarke recently announced an upgrade to the Card@Once printer to generate EMV cards. So, a financial institution can distribute EMV cards with knowledge that Harland Clarke's instant issuance solution is ready to go.

For more information on how Harland Clarke can assist with your card services needs, including expertise on making a smooth transition to EMV, please contact **Greg Kuyava** at **651.683.6364**.