BOOSTING CREDIT SECURITY

The U.S. is more than three years into its migration to Europay MasterCard Visa (EMV) chip payments, and 2015 is expected to be a year of great progress. Last year, there were approximately 120 million chip cards in the market, and this number is expected to leap dramatically to 600 million cards (or half the total cards in the market) by the end of 2015. Merchants are preparing too, with some estimates that as many as 50 percent of all payment acceptance terminals in the U.S. will be fully enabled to accept EMV chip cards by the end of the year.

What parking professionals need to know about EMV chip migration.

By Randy Vanderhoof

The U.S. parking industry, which generates more than $25–30 billion in gross revenues from its many thousands of parking garages, lots, and on-street parking meters, is one of the larger merchant segments taking on chip implementation projects. Upgrading all of the payment terminals throughout the industry to accept chip cards is not a simple or inexpensive task, but it is one that can help better secure the parking payment infrastructure and prevent fraud losses from counterfeit card fraud and skimming. Read on to learn why 2015 will be the "year of the chip."

Why Chip and Why Now?

More than 80 countries have already implemented EMV chip payments based on the EMV global standard. The EMV standard defines a set of requirements to ensure interoperability between chip-based payment cards and terminals. Chip cards contain embedded microprocessors (the "chip") that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards.

The U.S. is one of the last major economies to adopt chip technology. Chip implementation was initiated in the U.S. market in 2011 and 2012 when American Express, Discover, MasterCard, and Visa announced their roadmaps for supporting an EMV-based payment infrastructure. One of the drivers for this decision is for the U.S. to implement a payment system that is interoperable with the rest of the world. The other major driver? Fraud reduction and prevention.

Deciding to Implement Chip

Making the decision to implement chip acceptance sooner rather than later will benefit parking organizations in two ways: It will protect their payment systems from hackers and skimmers, and it will prevent them from assuming potentially higher fraud losses after Oct. 1, 2015, when the liability for fraudulent card transactions shifts to the party with the least secure technology. Implementing chip is a decision for each individual merchant and card issuer, and while it is not a mandate, those who don't migrate to chip will absorb resulting losses in the event of fraud.

Chip Security Features

While 2015 is poised to be the "year of the chip," 2014 was, unfortunately for many, the "year of the data breach." There were many instances of overseas hackers infiltrating retailer systems and stealing consumers' payment account data. Why are overseas hackers so interested in U.S. payment card data? It's because the magnetic stripe payment card data in retailer systems is extremely valuable to hackers; criminals will pay high prices for it because it's easy to use to create functioning counterfeit payment cards. Magnetic stripe cards are also extremely easy to skim, which has been a problem in the parking industry, particularly for those with unattended payment terminals.

Its reliance on magnetic stripe cards is one of the reasons why the U.S. has increasingly become a target for fraud. The U.S. loses approximately $5 billion a year to fraud, which accounts for about half of global card fraud despite our only generating about a quarter of the total volume of purchases and cash.

EMV chip card data can help combat some of this fraud because it cannot be used to make functioning counterfeit cards. There are three major chip card transaction security features that work to prevent fraudulent transactions:

- **Microprocessor chip**. Each chip card contains a secure microprocessor chip that stores payment card data placed by the issuer during the personalization process that can perform cryptographic processing during a payment transaction. This payment data is stored securely in the card's chip and is protected with advanced chip hardware and software security. This helps prevent card skimming and card cloning, which are the most common ways magnetic stripe cards are compromised and used for fraudulent activity.
- **Authentication**. In a chip card transaction, the card is authenticated as being genuine by the issuer or the terminal, and the chip's processor generates a dynamic data element that is unique for each transaction.
- **One-time-use cryptogram**. Unlike the static code in a magnetic stripe transaction, the chip card uses a one-time-use cryptogram for each transaction. Even if fraudsters are able to steal account data from a chip transaction, the stolen code will have already been used and is therefore invalid. In addition, chip cards do not include other data needed for magnetic stripe transactions, so criminals cannot use the stolen data to make counterfeit magnetic stripe or counterfeit chip transactions.

What this means for the parking industry: For organizations that start accepting chip payments, the data in their systems will become a lot less valuable to hackers. It has been seen in other countries that have migrated to chip technology that hackers will focus their attacks on organizations that still use magnetic stripe data. Skimming operations, too, will become fruitless as consumers increasingly use their chip cards.

Chip cards, already deployed in more than 80 countries, have been proven to dramatically reduce counterfeit card fraud and strengthen the payments ecosystem for all stakeholders.

October 1 Fraud Liability Shift

The other major factor in the decision to implement chip technology is the upcoming Oct. 1, 2015, fraud liability shift date set by the major payment brands. After Oct. 1, the payment brands will shift the responsibility for counterfeit card transactions to the party with the least secure technology. If neither or both parties involved in the transaction have implemented chip technology, the liability stays with the issuer, as it is today. An example of how this works: If a magnetic stripe off a chip card is copied, made into a counterfeit magnetic stripe card, and used at a parking facility that has not upgraded to accept chip payments, that facility may be responsible for the fraudulent transaction. The goal of the liability shift is to encourage both issuers and merchants to move to chip technology at the same time so that fraud is removed from the system, not shifted from one party to another.

In making the decision on when and if to implement chip technology, parking professionals should strongly weigh implementation costs versus the fraud risks that come with not implementing. Bear in mind that the cost to implement occurs only once, while the fraud losses from not migrating can multiply in years to come.

Change and Choice with Chip

Implementing chip technology within parking facilities will involve replacing hardware and software with EMV-certified offerings, integrating them with existing systems, and undergoing end-to-end testing and certification with each of the payment brands. It also provides many choices that can help them optimize revenues and customers' payment experience. Two of the key decisions to make include:

- **Interfaces.** The EMV standard supports both contact and contactless chip payments, so a parking facility can choose to accept only contact chip card payments, or both contact and contactless payments. Today, most EMV-certified terminal hardware suppliers sell readers that are equipped to handle contact, contactless, and mobile payments but will require software configured to enable acceptance of the payments. Contactless payments require less maintenance in outdoor environments so may be a good choice for unattended terminals. Contactless chip readers are also compatible with mobile near field communication (NFC) payments, so if a parking facility wants to accept Apple Pay, for example, it can be enabled during the chip implementation project. To future-proof investments, parking facilities should consider purchasing hardware that accepts contact, contactless, and mobile payments, even if they do not immediately enable contactless capabilities with software.
- **Card Verification Methods (CVMs).** The EMV standards support the use of PINs, signatures, or no CVMs to verify the cardholder in a payment transaction. Unattended machines can be enabled to accept PINs but are required to accept chip transactions with no CVM if the chip card does not support a PIN.

Parking professionals should work with their vendors and payment solution providers to determine what choices make the best sense for their businesses.

Conclusion

The U.S. is rapidly moving toward a more secure payment infrastructure with EMV chip card payments. Chip cards, already deployed in more than 80 countries, have been proven to dramatically reduce counterfeit card fraud and strengthen the payment ecosystem for all stakeholders. For all merchants, including parking professionals, implementing chip is a decision that each organization should make carefully; however not migrating can result in increased susceptibility to hackers and fraud. While moving to chip will introduce fundamental change to the parking payment infrastructure, it also can provide an opportunity for parking professionals to provide more innovative and fast payments to their customers, such as contactless and mobile NFC payments.

Parking professionals are not alone in this migration. There are terminal vendors, payment solutions providers, and industry groups ready and willing to help with migrating systems to chip in the most efficient manner possible. The Smart Card Alliance's sister organization, the EMV Migration Forum, provides a platform for industry stakeholders to come together and engage with their peers about the most pressing issues facing their migrations. For more information and/or to attend a meeting, visit emv-connection.com.

RANDY VANDERHOOF is executive director of the Smart Card Alliance. He can be reached at rvanderhoof@smartcardalliance.org.