CDW PEOPLE WHO GET IT

ARE YOU READY FOR EMV?

A new payment technology is arriving in the U.S. with a promise to **improve security** and **reduce fraud**.

Paying with a credit card at retail stores in the United States has become almost as natural for consumers as handing over cash. Customers simply swipe a card, scribble out a signature and head out with their merchandise. However, that system is inherently insecure, as evidenced by a Nilson Report in 2013 showing that the U.S. accounted for 47.3 percent of worldwide payment card fraud while making up only 23.5 percent of the total volume of transactions.

To combat fraud, retailers in Europe implemented the EMV (EuroPay, MasterCard, VISA) system, which replaced the magnetic strips on most payment cards with a computer chip. Cardholders no longer have to sign their names for verification and instead enter a personal identification number.

"The United States is the last bastion of sign-and-swipe cards," says Paula Rosenblum, a managing partner for Retail Systems Research. "They are much less secure and easier to forge. In the United Kingdom, where EMV was implemented, fraud is virtually zero."

The new cards enhance security in two main ways. First, the magnetic strip on the old cards contained static data that was easy to capture and replicate. Once someone stole that data, it could be applied to an unlimited number of fake cards and used anywhere. By contrast, the chips embedded on EMV cards generate a new code for every transaction. If someone steals the data on the chip during a transaction, it can't be used again because it would have all changed the next time someone tried to use the stolen information.

In the United States, rules are changing in October 2015 to include a "liability shift." After October, liability for fraud that occurs when a chip-enabled card is used will shift to the party — either the card issuer or the retailer — that is the least compliant with EMV. For example, if a retailer uses a point-of-sale (POS) system that supports only swipe and pay, and a customer uses an EMV chip-enabled payment card, the retailer is liable for any damages incurred by the fraudulent use of the card. However, if a retailer uses an EMV-compliant POS terminal, but the customer's bank hasn't issued him or her a chip-and-PIN card, liability would fall with the bank.

While retailers likely will be pleased with the greater security EMV cards offer, the new system comes with some drawbacks as well. Some experts say that EMV transactions will likely take a few seconds longer to process than swipe-and-pay transactions. As this time adds up over the course of a day at a busy retail store, businesses may see increased wait times and longer lines, which can frustrate some retailers.

Further, the investments made to install the new machines could become costly for some retailers. Many POS systems that support both sign-and-swipe as well as EMV cards cost between $500–$1,000. Retailers will need to support both technologies until all cards are changed over to the new format. Retail industry groups estimate the total cost of the switchover to retailers in the United States to be around $35 billion.

David Russell, a principal security engineer for CDW, says this changeover period is a confusing time for most retailers, who also must deal with compliance issues related to the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS mandates security measures related to credit and debit card transactions. "I doubt that anyone would argue that EMV isn't a good thing that will make transactions more secure," Russell says. "But just adding an EMV system won't necessarily guarantee PCI compliance. EMV won't solve all security issues, such as the proper handling and disposal of paper records, so even if a vendor installs EMV, they should still want to work toward PCI compliance to protect themselves and their customers."

The second main security component of the new card is its use of a PIN number for card verification, which functions similarly to how debit cards use PINs, says Carlos Soto, senior vice president of technology operations with the Tech Writers Bureau. When a customer pays with a debit card, a portal is opened up from the POS terminal to the issuing bank to confirm the real owner of the card, a process that requires a robust and secure database at the issuing bank. By contrast, credit cards are verified by having a store clerk check that a customer's signature matches the one on the back of the card, something Soto says rarely happens.

Rosenblum agrees that signature-based verification is no guarantee of safety. "I have trouble writing on those pads on a good day," she says. "My signature ends up just being a couple loops and a wavy line, and most people don't even put any effort into it. Without requiring the PIN, you are still going to see fraud."

The Arrival of Digital Wallets

Many retail consumers are taking a new approach to payment that goes beyond standard credit cards and even EMV cards: the digital wallet. It's yet another factor that retailers need to consider when deciding when and how to upgrade their POS machines.

"A digital wallet is basically the process of taking your payment data and adding it to your smartphone," says Carlos Soto, senior vice president of technology operations with the Tech Writers Bureau. "The recent launch of the Apple Pay system in conjunction with banks and credit card companies shows how this can work to make payments even more secure for customers."

Consumers using a digital wallet add credit card data to a smartphone, which is translated into a device account number and encrypted on a special chip. A shopper can pay for merchandise simply by waving a phone in proximity to a near field communication reader at a store. The credit card numbers are never shown or shared with store employees, nor is the name of the customer. This reduces the chance of someone stealing the card or personally identifiable information associated, since this information never actually becomes part of the POS transaction.

Customers who lose their phones are still protected by security measures such as biometric authentication or a PIN lock that prevents anyone but the owner from using the device. For further security, users can remotely wipe most phones in the event of a loss or theft.

Paula Rosenblum, managing partner of Retail Systems Research, believes that programs such as Apple Pay and its inevitable competitors will certainly be a factor in the retail market that businesses must consider. "My advice to retailers when overhauling their POS systems for EMV is to go ahead and spend the extra $35 or so that it will cost to add Near Field Communications (NFC) to those readers too," Rosenblum says. "That way, they will be ready for anything."

All 10 of the largest U.S. credit card issuers are issuing chip-based credit and debit cards and expect most of their portfolios to be updated by the end of 2015.

SOURCE: cardhub.com, *"2015 EMV Migration Report"*

59% The percentage of U.S. retail locations that will be EMV-compliant by the end of 2015

SOURCE: Javelin Research & Strategy, *"2014 PULSE Debit Issuer Survey,"* June 2014

Sources for article:

Paula Rosenblum
Managing Partner, Retail Systems Research
prosenblum@rsrresearch.com | 305.757.1357

Carlos Soto
Senior Vice President, Technology Operations, Tech Writers Bureau
csoto@techwritersbureau.com | 202.413.7896

David Russell
CDW, Former Qualified Security Assessor for the PCI Council
davirus@cdw.com | 608.298.1138

To learn more about how CDW can help retailers use technology to get an edge on competitors, visit CDW.com/retail.