ROCHESTER BUSINESS JOURNAL
RBJ

Special Report
Local banks are getting ready to migrate to the global standard for secure payments.
Page 13

ROCHESTER BUSINESS JOURNAL
MAY 22, 2015
SPECIAL REPORT
Banking and Finance Quarterly

VOLUME 31, NUMBER 8 WWW.RBJDAILY.COM MAY 22, 2015

American banks getting ready to roll out EMV credit cards

The technology provides greater security against credit and debit card fraud

By MIKE COSTANZA

Photo by Kimberly McKinzie

"Right now, 37 percent of credit card fraud is the type that will be mitigated by chip technology," says Sandy Roberts, senior vice president at Canandaigua National Bank & Trust Co.

EMV chips, long used to fight credit and debit card fraud abroad, finally have crossed the sea. Financial institutions are getting ready to make the shift, migrating to the global standard for secure payments.

"We intend to convert over 70 percent of our credit and debit plastics by the end of the year to chips," says Dina DeMerell, director of credit card chip rollout for Chase Card Services at JP-Morgan Chase.

Other banks that do business in the Rochester area also are issuing EMV-equipped cards to their customers, or are slated to do so. For those that adopt the new technology, the cards present a higher level of security. Those that avoid doing so could suffer financial losses.

EMV chips are microprocessors; when implanted in a credit or debit card, they introduce a level of security that other cards cannot match. Developed through a joint effort by the credit card associations Europay, MasterCard and Visa—resulting in the name—the technology has come to be the gold standard for card security.

The U.S. has lagged behind other nations in the shift to EMV cards, though that is set to change. Major credit card associations are deploying the cards in this country or preparing to do so. On Oct. 1, enforcement of new liability rules that promote the use of the EMV cards will begin.

An EMV card's greater security arises from the way it functions at the point-of-sale. Each regular card bears a magnetic strip, or magstrip, that contains the card's number and other data required for transaction approval. By swiping the card through a card reader, the bearer electronically tenders the information.

Thieves have found ways to obtain credit card information at the point-of-sale.

"The vast majority of the compromises that occur are through data breach compromises, like Target and Home Depot, where a large number of card numbers are compromised," says Doug Johnson, Washington, D.C.-based senior vice president at American Bankers Association.

Perpetrators then use the numbers to create counterfeit credit or debit cards. According to Johnson, the process might only involve changing the magstrip information on off-the shelf gift cards. Once altered, the cards are sold on the open market; there are sites that cater to the trade.

Target Corp. suffered a massive breach in late 2013, possibly because hackers placed malware on the retailer's sales terminals. For about three weeks, every point-of-sale swipe at one of Target's terminals gave crooks the magstrip information they needed to counterfeit another card. As many as 110 million credit and debit cards were compromised.

While such incidents cost the merchants involved—Target's loss came to almost $150 million—banks also suffer from point-of-sale fraud. Not only are the financial institutions liable for the cost of the initial, legitimate sale, but they also have to cover transactions that are subsequently made with counterfeit cards.

"If there's counterfeit fraud that results because information is compromised at a merchant, that fraud is charged back to card issuers," says DeMerell, who is based in Ann Arbor, Mich.

Credit and debit card fraud resulted in $11.27 billion in losses in 2012 alone, a Nilson Report found. Card issuers incurred 67 percent of the losses, mainly through point-of-sale fraud with counterfeit cards.

EMV cards subject point-of-sale transactions to a higher level of security. Whenever a card is inserted into an EMV-enabled reader, its chip generates a unique code that is used to approve that transaction, and only that one. Once the transaction goes through, the code becomes useless to swindlers.

"They can't replicate the data to create a fake card, and therefore a new transaction," explains Leanne Hughes, M&T Bank Corp.'s administrative vice president for consumer affairs.

Because they contain the microprocessors, EMV cards are also much more difficult to replicate than magnetic strips. To encourage merchants to accept EMV cards, MasterCard, Visa and other credit card associations have instituted new rules concerning financial liability. As of Oct.1, banks and merchants that do not make use of the technology could suffer.

"If a customer is holding a chip card but the merchant hasn't updated their capabilities to accept chip cards, then that liability will move from the issuer to the merchant," DeMerell says. "They will be responsible for any fraud that happens as a result of a breach at point-of-sale."

On the other hand, if the customer only has a standard, magstrip card, the bank foots the bill for the fraud.

Banks are unable to state how much they will save with EMV cards, though they expect point-of-sale fraud to drop as merchants adapt to their presence.

"Right now, 37 percent of credit card fraud is the type that will be mitigated by chip technology," says Sandy Roberts, senior vice president at Canandaigua National Bank & Trust Co.

EMV cards have already made an impact in the United Kingdom, according to DeMerell.

"When they implemented chips, they had over a 55 percent decline in counterfeit fraud," she says.

Some banks are incorporating the new technology into their ATMs as well. Chase has already installed 45,000 of the EMV-capable devices and plans to add 60,000 more, DeMerell says.

Though EMV cards present obvious benefits, they also have drawbacks. Their success depends upon their acceptance.

"The real value of the chip here in the U.S. isn't going to be fully realized until the whole industry moves to chips," DeMerell says.

EMV cards also come with a larger price tag.

"The main drawback for banks in general is the cost of the EMV card is anywhere from two times to four times as much as a traditional card," says Charles Guarino, senior vice president at Five Star Bank.

Banks also have to absorb the cost of adapting to the new cards. M&T, which began issuing EMV cards to its commercial customers in 2014, has upgraded its transaction authorization, fraud detection and other appropriate systems in order to adapt to them.

"We've had to put in place a number of technology initiatives in order to make sure that this goes off without a hitch," Hughes explains. "There certainly is a lot of work in the background."

Hughes says her bank expects to issue EMV debit cards this June.

Merchants who choose to process EMV cards will have to take on additional expenses, by buying or renting the new, more costly card readers. Some might not be willing to shoulder those burdens, and others might not be able to.

"The one thing that we've heard over time is concern over the cost of the technology for the business," ABA's Johnson says. "The ability of smaller merchants to deploy EMVs through new readers has been a concern."

Finally, EMV cards only make their magic at the point-of-sale, and even that is limited. Fourteen percent of payment card fraud comes from the use of lost or stolen cards. Perhaps more important, 47 percent of frauds occur online, and that is expected to grow as EMC cards proliferate.

"The enhanced security will … shift the liability toward that part of the system that has the least security," Johnson says.

Despite these concerns, banks in the Rochester region are issuing EMV cards or preparing to launch the process. Even as those efforts bear fruit, those in charge of card rollouts recognize that criminals are ready to thwart them.

"The fraudsters are going to become more sophisticated," Roberts says. "We see new areas of risk."

Mike Costanza is a Rochester-area freelance writer.