NEW. DIFFERENT. BETTER?

Will EMV really protect credit card data?

by M.V. GREENE

Ready ... or not? If only it were so simple for America's retailers. When it comes to the October 1 deadline credit card companies set for merchants to be equipped to accept new chip-based cards, the question for much of the past year has been whether retailers would be prepared.

Retailers who didn't meet the deadline can still accept both the new chip cards and traditional magnetic stripe cards, and will be able to do so for the foreseeable future. But they are getting a stick rather than a carrot in the form of increased fraud liability if they don't have a chip card reader and a chip card turns out to be counterfeit.

Up until October 1, banks absorbed fraud costs from counterfeit cards, but the cost will be now be borne by retailers, who already are liable for fraud costs if the card user is not the legitimate cardholder. (The change applies only to chip cards; rules for magnetic stripe cards remain the same.)

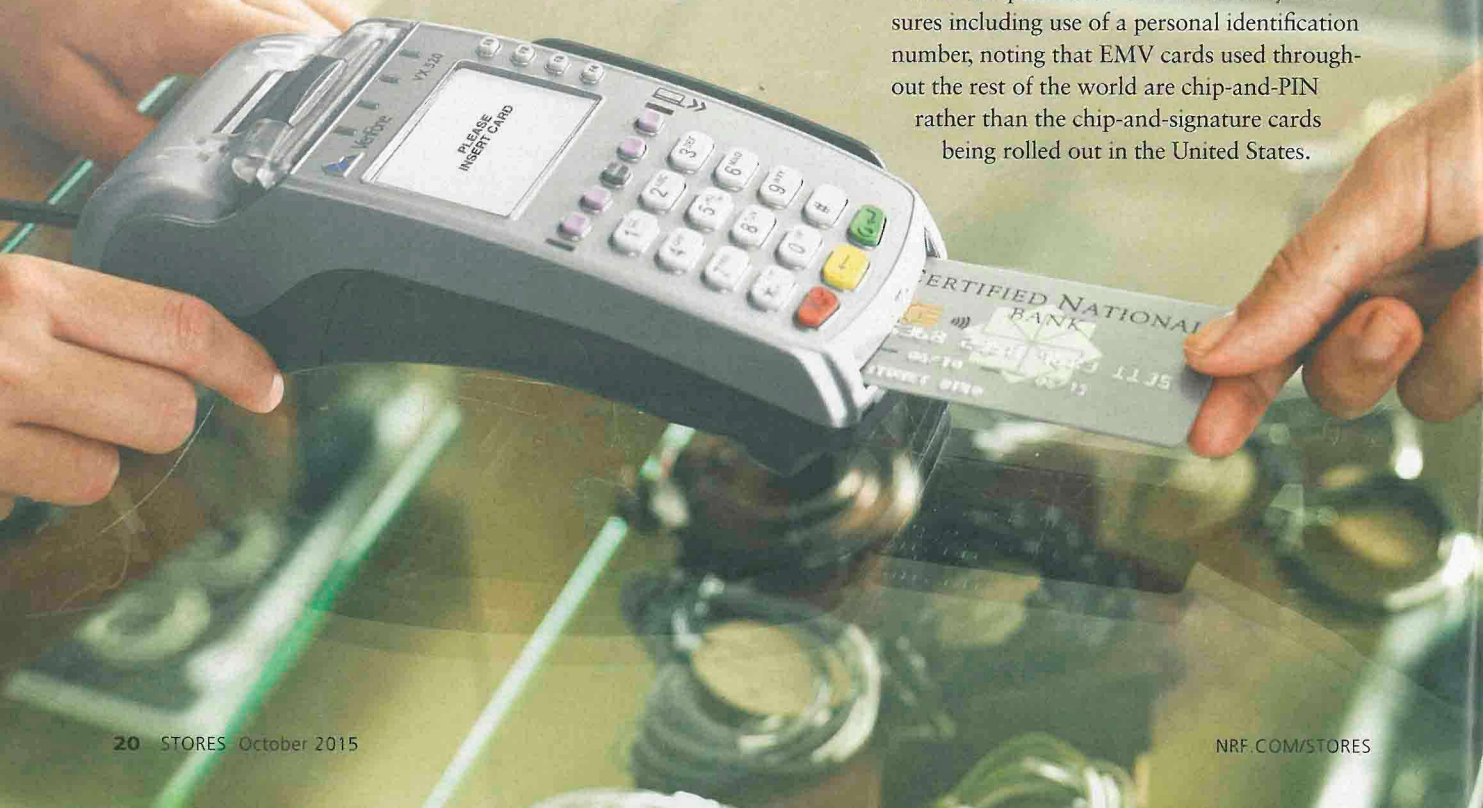
Implementation of chip card technology has been a multi-year tsunami sweeping across the payments industry. Visa, MasterCard, American Express and Discovery announced in 2011 that they would adopt the Europay MasterCard Visa technology and gave most retailers until this month to be ready. Pay-at-the-pump gas stations have until 2017.

The new cards, which store data on encrypted computer microchips that will eventually replace the magnetic stripes, are intended to offer improved security over the stripe technology in use since the 1970s.

BROADER MEASURES

The National Retail Federation and others in the retail industry agree that the new cards provide enhanced payment security but contend that they do not go far enough.

NRF has pushed for broader security measures including use of a personal identification number, noting that EMV cards used throughout the rest of the world are chip-and-PIN rather than the chip-and-signature cards being rolled out in the United States.



"The chips partially address the issue of counterfeit cards, but do nothing about lost or stolen cards because thieves will still be able to sign any illegible scrawl to 'prove' that they are the cardholder," says NRF Senior Vice President and General Counsel Mallory Duncan.

"More importantly, sophisticated criminals can circumvent the chips, so a chip alone is not foolproof. A PIN is a secret password that makes the card useless to a criminal whether the card has a chip or not.

"A chip card without a PIN amounts to locking the front door while leaving the back door wide open," Duncan says. "In today's world, you need to lock both doors. Consumers around the world have had both a chip and a PIN for a generation or more. Why should American shoppers have anything less?"

Banks have touted chip cards as a way to discourage hacking of consumer credit card data: If it's more difficult to create a counterfeit card from the stolen numbers, criminals will have little incentive to steal them in the first place.

But NRF Vice President of Retail Technology Tom Litchford says protecting the data at the source with technology like point-to-point encryption or tokenization is the more effective approach.

"Retailers are doing everything they can to make that [deadline] ... but they also realize that EMV is not the solution to the fraud problem in the U.S., and are taking additional steps to protect their customers' credit card data," Litchford says.

In a report issued this summer, research company IHL Group called EMV "Retail's $35 Billion Money Pit," and said the money would be better spent on securing data rather than securing cards.

"The single biggest problem with the EMV mandate is that it is focused on trying to solve last century's problem and completely ignores the reality that retailers are facing today," IHL President Greg Buzek says. "When EMV was introduced into Europe, it made tremendous sense. Today it stands in the way of real data security by stealing critical budget away from focusing on the risks that retailers face from online hackers."

VARIED READINESS

Regardless of the new system's effectiveness, the question has been how many merchants would have EMV up and running by October 1, and when — or if — those who didn't will make the move.

Javelin Strategy and Research has forecast that 166 million EMV credit cards and 105 million EMV debit and prepaid cards will be in circulation in the United States by the end of 2015. Javelin has put the price tag for EMV compliance at more than $8.6 billion, but NRF estimates the total at $35 billion when card readers, related equipment, software, installation, training and others costs are included.

Mercator Advisory Group, a consultant to the credit card and banking industries, projects that 58 percent of credit cards — but only 26 percent of U.S. card terminals — will be chip-ready by the end of 2015. An NRF survey released early this year found that 23 percent of retailers expected to be fully ready by October 1; another 66 percent planned to have at least a partial rollout in place.

"Retailer readiness varies widely," says Aaron Press, director of market planning, e-commerce and payments at LexisNexis Risk Solutions. "The challenge in making the shift to EMV is proportional to the complexity of the POS environment."

Press says some national chains like Walmart, Target and Macy's have already rolled out EMV, and most others will soon. But many retailers "clearly have work to do" while others are taking a "wait-and-see" approach, he says.

"Not all retailers see it as a priority yet," says Rob Cameron, chief product and marketing officer at Moneris Solutions Corp., which provides payment equipment for more than 350,000 U.S. merchant locations. "A lot of what we're doing is education around the liability shift and what it will mean for them in terms of chargeback risk."

Retailers in the hospitality field, particularly restaurants, have less financial exposure if a card transaction turns out to be fraudulent and

> "Consumers around the world have had both a chip and a PIN for a generation or more. Why should American shoppers have anything less?"
> **— Mallory Duncan, NRF**

are less likely to be targeted by criminals looking for merchandise they can fence.

"At a restaurant, [card thieves] might consume the food, but they are taking a risk by being there and using the card," Cameron says.

Forrester Research says "friction" in the payments marketplace is a factor and predicts that EMV will not achieve broad adoption until 2020.

In April, the Food Marketing Institute asked card companies to delay the October deadline to 2016, calling it "arbitrarily set." The bank-led EMV Migration Forum said a delay wasn't necessary, calling the target date an "incentive" for retailers to achieve compliance rather than a mandate.

Retailers are reporting that once they have the chip card-reading equipment in place, it is taking several months for certification to occur.

CERTIFICATION, IMPLEMENTATION ISSUES

NRF says the cost of chip readers, at an average of $2,000 each once all costs are included, is only one issue. Once installed, the equipment must be certified by the card industry, and certification is lagging. Litchford says card companies apparently underestimated the certification process: Retailers are reporting that once they have the equipment in place, it is taking several months for certification to occur; the logjam only increased as the deadline approached.

The card companies "just don't have the resources to handle the volume of certification requests that are coming in," Litchford says.

Press said some smaller merchants were unaware of the implications of the deadline and some were dubious when weighing the costs against potential fraud.

Consumers also seem to be jarred by the process. Some retailers say force of habit has consumers trying to swipe the new cards; others have properly inserted the chip cards but have forgotten to remove them after signing and walked away.

"No matter the size of the merchants, associate training is critical," Press says. "Employees need to know the right way to handle an EMV transaction to maintain a good customer experience, avoid unnecessary liability and spot potential fraud."

A late-summer survey conducted for NRF by ORC International found that 71 percent of consumers with credit cards had at least one chip card. But most consumers have more than one card, so that translates into chip cards accounting for only 43 percent of the cards in shoppers' wallets. Only 47 percent of those with a chip card had used it in a chip-card reader.

Sixty-two percent of respondents said they would rather use a chip-and-PIN card than chip-and-signature; 63 percent believe data is more secure with chip and PIN, and 83 percent of consumers who say PIN is more secure say the additional security is worthwhile even if they had to have different PINs for each card, according to the survey.

RE-EVALUATING THE BUSINESS

Amid all the wrangling between the card companies and the retail industry, EMV is prompting retailers to take a broader look at how they do business. Much of that has to do with the opportunity to deploy mobile payment systems, Cameron says.

"A lot of retailers are using the shift as an opportunity to re-evaluate how they want to service their customers and how they want to run their businesses," he says. One key consideration is whether to continue with a traditional cash register presence or switch to a mobile system that might use tablets to provide checkout anywhere in the store. Another is investing in solutions such as cloud-based inventory management that can be integrated into point-of-sale equipment.

Alan Lipson, principal marketing manager for retail at analytics and software company SAS, says retailers need to place EMV in the context of a fuller cybersecurity approach.

"EMV is a steppingstone. You have to think of it like peeling an onion," he says. "There are many different layers."

From a broader cybersecurity context, Lipson notes that the customer data stolen in high-profile retail hacks in recent years was taken from retailers' servers, not at the POS.

"EMV does solve part of the problem at the POS," Lipson says. "It is making the POS transaction more secure. But that in and of itself is not going to solve everybody's cybersecurity problem. There are still going to be hacks. There are still going to be breaches of data." **STORES**

M.V. Greene is an independent writer and editor based in Owings Mills, Md., who covers business, technology and retail.