PAYMENTS INDUSTRY INSIGHTS
published by TSYS

Will Losses In Consumer Confidence In Payments Accelerate EMV?

With next steps still unclear, retail breaches spark a sense of urgency

by Charles Keenan

Will the recent security breaches at national retailers be enough of a catalyst for adoption of the EMV payments standard in the United States? Probably, but it will be years before the payments standard is ubiquitous, industry veterans say.

At first glance, upgrading to EMV (originally developed by Europay, Mastercard and Visa) seems like a no-brainer in the wake of breaches at retailers Target Corp. and Neiman Marcus Group. The stakes for issuers and retailers are higher than just outright fraud losses, says Randy Vanderhoof, director of the EMV Migration forum.

"The data breaches were a wake-up call," Vanderhoof warns. "It goes beyond just looking at the business case for how much fraud retailers are exposed to, but what would be the cost of a major breach in terms of consumer confidence and reputational loss."

New impetus

Yet it remains to be seen how fast merchants and retailers will adopt EMV. In Europe, for example, it took upwards of a decade for EMV to become widely used.

For those inside the payments industry, it's common knowledge that most merchants in the U.S. are required by October 2015 to install EMV terminals or risk assuming on the liability for fraudulent transactions. Yet adoption has been hindered by a general ambivalence by merchants and issuers.

Throw consumers into the mix, and that attitude just might be changing. The Target and Neiman Marcus POS breaches prompted hearings on transaction security on Capitol Hill, and some retailers and issuers have stepped up timetables to shift to chip cards. Target, for example, announced in early February it is accelerating a move to chip for its proprietary credit card to the first quarter of 2015, six months earlier than originally planned. Banks have also stepped up inquiries with card processors.

EMV: Net security gain

EMV most likely wouldn't have prevented the breaches, but it would have stopped fraudsters from copying the cards, the sophistication of which makes counterfeiting them much more difficult than doing so for magnetic stripe cards. For each transaction, EMV chips generate a unique cryptogram, which can't be used again for subsequent purchases. "Even if the data was scanned from memory, criminals would not have been able to make an EMV card," says John Latimer, chief risk officer for TSYS."

Factors slowing adoption

That said, a number of issues might mean EMV will take longer than expected to implement, experts say. "It is going to take years before it makes a difference," says Avivah Litan, an analyst at Gartner, a consulting firm in Boston. The main issues include:

BECOME A CONTRIBUTOR

SUBSCRIBE

ARTICLE ARCHIVE

by topic

Consumer Behavior
Contactless/NFC
Credit
Debit
Emerging Payments
Executives
Fraud
Game Changers
Global
Healthcare
Legislation
Loyalty
Merchants
New Trends
Prepaid

High Cost: Implementation is estimated to be about $6 billion, 75 percent of which will be borne by merchants, estimates consulting firm BetterBuyDesign. Target expects the total cost, including installing terminals in its 1,800 U.S. stores, to be about $100 million.

Low Bases: There are about 1.1 billion credit and debit cards in circulation represented by the four main network brands — American Express, Discover, Mastercard and Visa — according to The Nilson Report. Yet at this point, there are only 15 million chip cards issued in the United States, according to estimates by the EMV Migration Forum.

In a perfect world, if all merchants installed compliant terminals by the deadline, issuers would have to replace at an average pace of roughly 2 million cards a day by October 2015. Meanwhile, just 10 percent of terminals are now EMV compliant, according to the EMV Migration Forum.

Debit Delay: Still up in the air is the Federal Reserve Board's interchange and routing rules on debit cards. An appellate decision in the retailers' favor would require a revision of routing rules, which would affect how cards will be programmed.

> In a perfect world, if all merchants installed compliant terminals by the deadline, issuers would have to replace at an average pace of roughly 2 million cards a day by October 2015.

Until there is a resolution — expected in the late spring — issuers will likely not begin to produce debit cards. "We are in this kind of dead zone right now," Vanderhoof says.

Merchant Resistance: Under EMV, issuers can issue chip-and-PIN or chip-and-signature cards. But retailers as a group prefer chip and PIN. Mallory Duncan, general counsel at the trade group National Retail Federation, sees no benefit in going with a signature option, since fraud can still be perpetrated at the point of sale with a stolen card.

The NRF also does not advocate EMV itself, preferring a more open system. "We are willing to support the banks to a more fraud resistant system," Duncan says. "But EMV is only one brand of soft drink. There is no reason why the entire retail industry should necessarily lock itself into only drinking that cola."

Alternatives to EMV

And other payment methods exist. There could be a chip-and-PIN card not using EMV. There's NFC, short for Near-Field Communications, which has been touted as a way to pay by using mobile devices. Cloud payments are another possibility.

> Until there is a resolution — expected in the late spring — issuers will likely not begin to produce debit cards.

But all of these lack the global scale of EMV, notes Maarten Bron, director of innovations in the transaction security unit of Underwriters Laboratories Inc., a product testing company based in Northbrook, Ill. "With technology, the sky is the limit," he says. "But a payments system only starts to have relevance if it connects supply with demand on a large scale."

Another possibility is issuers' insistence on more immediate solutions with magnetic stripes. The Target breach, for example, exploited a vulnerability of the terminals, where unencrypted data was stored in a memory cache for authorization.

Encrypting that data and adding unique tokens to each transaction could be done quickly, says David Robertson, editor of *The Nilson Report*. "If you did that, you would go a long way to making sure there wasn't any kind of fraud from a data breach."

So EMV might see the light of day in the U.S., just not tomorrow.

ABOUT THE AUTHOR

Charlie Keenan has written about payments since joining the American Banker as a staff reporter in 1997. His work at the American Banker included writing about credit and debit cards, merchant processing and bank stocks. He later freelanced for the Banker and industry publications such as Banking Strategies, Bank Director, Community Banker and U.S. Banker. He also writes about investing, insurance and health care, and is based in Los Angeles.