February 22, 2016

As U.S. adopts EMV technology, will hackers revamp tactics?

Switch to chip cards improves security and decreases fraud, but isn't foolproof—as Canada has seen

FEATURED STORY BY RODIKA TOLLEFSON, THIRDCERTAINTY

Visa has released data showing adoption of Visa chip cards by U.S. banks and merchants is gathering steam.

But the capacity for Europay-Mastercard-Visa (EMV) chip cards to swiftly and drastically reduce payment card fraud in the United States is by no means assured.

Just look north to Canada, where EMV cards have been in wide use since 2011. Criminals have simply shifted fraudulent use of payment card accounts to online purchases—where the physical card does not come into play. Security and banking experts expect a similar pattern to play out in the U.S. where banks and merchants are under an October 2015 deadline, imposed by Visa and MasterCard, for adopting EMV systems.

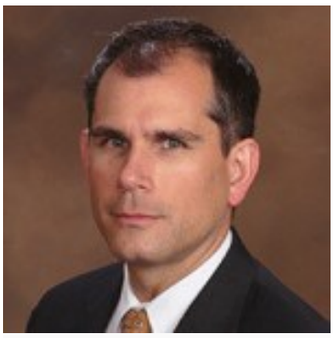
Free resource: *Putting effective data risk management within reach*

Heeding that deadline, major retail chains and big banks are now deep into implementation of EMV systems, thus driving up adoption numbers in the U.S. However, thousands of small and midsize businesses continue to remain on the fence.

SMBs slower to switch

SMBs are methodically assessing the risk vs. reward of racing to adopt EMV, Brian Engle tells ThirdCertainty. Engle is executive director of the newly founded Retail Cyber Intelligence Sharing Center, or R-CISC.

Company decision-makers are doing their due diligence, factoring in the potential for fraud, the cost of implementing EMV technology, and the risk of chargebacks, he says.



Brian Engle, Retail Cyber Intelligence Sharing Center executive director

"From a transactional volume perspective, some are going to accept risks and move at a rate that's more appropriate for the size of their organization," Engle says.

There's no question the United States is in EMV saturation mode. As of the end of 2015, Visa tells us:

- The volume of chip transactions in the U.S. increased from $12.1 billion in November to $15.8 billion in December, a 30 percent pop.
- Seven out of 10 Americans now have at least one chip card in their wallet.
- 93 percent of consumers are aware that the transition to EMV is happening.

Cryptogram makes things more complicated

Unlike magnetic-stripe cards, EMV cards are more difficult to counterfeit because the chip contains a cryptogram. When the card is inserted into the POS terminal—vs. being swiped—the cryptogram creates a token that's unique to each transaction, and all the information is encrypted as it's transmitted to the terminal and the bank.

This process actually takes a few seconds, during which the consumer must leave his or her card inserted in the POS terminal. U.S consumers are in the process of modifying their behavior at the checkout stand. Patience for a few seconds is required. But those precious seconds of inconvenient waiting represent an investment in tighter security.

But not as tight as when you use a chip card in Canada or Europe. That's because EMV cards not only generate a one-time authorization token, they are also designed to require the user to enter a PIN as a second factor of authentication. However, PIN compliance was not part of the October 2015 deadline. Thus most EMV in-store transactions in the U.S. still require only a signature, which, of course, any imposter can forge.

Criminals, on the other hand, won't be able to hack into store networks and steal any useful transactions data, at least not any in which chip cards were used.

"Even if you steal the information, it becomes very difficult to use it. You'd get a long string of letters and numbers that can't do anything," explains Ben Knieff, senior analyst for retail banking at Aite Group, an independent research and advisory firm that specializes in financial services.

Criminals reportedly were able to breach Wendy's customer magnetic strip payment card data, recently. That data breach was disclosed after numerous stolen card numbers were subsequently used at other merchants, and the trail led back to Wendy's.

This kind of credit card fraud is exactly why U.S. financial institutions are migrating from the magnetic-stripe cards to new technology that uses a much more secure chip.

Aite Group estimates that EMV will significantly reduce U.S. counterfeit card fraud—from an estimated peak of $3.61 billion in 2015 to $1.77 billion in 2018.

Even so, the technology is not foolproof since bad actors can use other tricks. "The EMV technology is still hackable," says Scott Schober, president and CEO of Berkeley Varitronics Systems Inc., which specializes in wireless threat detection. "However, hackers are going to go after the simple hack."

Scott Schober, Berkeley Varitronics Systems Inc. president and CEO

Identity theft experts anticipate that fraudsters will simply shift their attention to merchants that use mobile payments—or don't use a physical POS terminal at all.

"For bad actors, when one avenue dries up, they will look for other ways," says Numaan Huq, a Canada-based senior threat researcher with Trend Micro's Forward-Looking Threat Research Team.

Some transactions safer than others

In Canada, where point-to-point encryption is now standard for retailers, Huq says he feels very safe when using a credit card in stores. But at places like hotels? Not so much.

That's because hotels collect credit card information for reservations and when that system is hacked, all the data is compromised. The same goes for various service providers, like medical offices.

"Bad actors will find new avenues, and I expect over time, the fraud levels (in the U.S.) will go up again," Huq says.

That's what happened in Canada, the U.K. and other countries that have adopted EMV. Canada, for example, saw a 54 percent decline in counterfeit cards and 133 percent jump in "card-not-present" (CNP) fraud between 2008 and 2013, according to Aite Group research.

"In the past, most of the tools hackers used were extremely crude," Schober says. "But advances in technology are making it much easier to compromise people online."

Aite estimates that CNP fraud in the United States will grow from $2.9 billion to $6.4 billion, as hackers shift their tactics.

But, Knieff says, criminals have one thing going against them—online credit card fraud is not a scalable "business." Criminals can't buy 40 TVs from amazon.com, for example.

"Application fraud—using stolen or synthetic identities to open new accounts … becomes much more attractive," he says. "Yes, CNP will increase, but it will not increase geometrically because it's hard to scale."

Many organizations may not even be ready to focus on securing their online systems. Engle, of R-CISC, uses a hockey analogy, saying retailers are "trying to skate to where the puck is going." That is, at the moment they're still trying to figure out the transition to EMV.

SMBs particularly vulnerable

In the meantime, smaller businesses face an increased risk.

"The fraudsters will utilize POS malware until they can't, and those smaller retailers are going to continue to be in their cross-hairs," he says. "The ability to impact small retailers at a high rate is very profitable for them."

Attacks on large retailers take a lot more time and resources, Huq says.

"A small mom-and-pop shop is a no-brainer to hit," he says, adding that mobile payments, especially, are a concern because of proliferation of malware, particularly for Android systems.

"It's easy to use for small businesses because it costs less," he says. "But in the future, I think this will be a new way for bad actors to steal credit card data."

More stories:
Human factors could undermine chip-and-PIN security
Switch to 'chip & sign' credit cards still leaves users exposed
How to build customer loyalty by keeping data secure