

ADVERTISEMENT

RSAConference™2024
San Francisco | May 6 – 9 | Moscone Center

REGISTER NOW

DIVE INTO A WORLD OF
CYBERSECURITY INSIGHTS!

REGISTER FOR AN ON DEMAND PASS.



Security Architecture, Endpoint/Device Security,
Endpoint/Device Security, Endpoint/Device Security,
Endpoint/Device Security, Endpoint/Device Security



The long and winding road: EMV adoption

Karen Epper Hoffman June 1, 2015

Payment cards in the United States are finally starting to get much smarter. After much debate, some resistance, concerns and a number of retail breaches, smart cards, also commonly known as chip cards, are gradually replacing the magnetic stripe cards that have been in circulation for decades in the U.S. market. Unlike the magnetic stripe, these payment cards come equipped with an embedded integrated circuit (where the data resides), which is “dipped” into a reader, rather than swiped like a magnetic stripe card. The cards have already been in use around the globe – particularly in the most advanced commercial countries in Europe, Asia and South America – for as long as a dozen years now. In fact, the technology behind these chip cards is typically referred to as EMV for Europay-MasterCard-Visa, the card brands initially behind the chip card technology standards and specifications.

“We are way behind the rest of the world,” says Deborah Baxley, principal for Capgemini Financial Services. “We

ADVERTISEMENT

RSAConference™2024
San Francisco | May 6 – 9 | Moscone Center

DIVE INTO A WORLD OF
CYBERSECURITY INSIGHTS!

REGISTER NOW AND
WATCH ON DEMAND.

REGISTER NOW



**GET DAILY
EMAIL
UPDATES**

SC Media's daily
must-read of the

need to set a date.”

Indeed, in the United States, which boasts the world's largest credit card and debit card base in the world, financial institutions that issue payment cards and the merchants that accept them have virtually crept toward chip-based cards and terminals. Chip card implementations only began domestically in the past three to four years, when the major card brands came out with their plans to support a chip card infrastructure for the United States. Merchant acquiring banks were mandated to start supporting new EMV data standards in April 2013. In upwards of four years, U.S. card issuers have been replacing credit and debit cards as they are lost or expire, typically with hybrid cards that have both a magnetic stripe and a chip.

And perhaps, most notably, merchants have an eye toward October 2015, when new rules will shift the liability for most fraud losses in a face-to-face environment (not phone or online commerce) from the issuer of the consumer's card to the merchant. Specifically, if fraud results from the compromise of a mag-stripe card transaction, the merchant will be held liable if it is not equipped to accept EMV-compliant chip-card transactions.

By the end of 2014, the Smart Card Alliance – a nonprofit that aims to “stimulate the understanding, adoption, use and widespread application of smart card technology” – and its related EMV Migration Forum, estimated that the United States had approximately 120 million EMV-compliant cards, out of a total of 1.2 billion debit and credit cards in circulation total, and 4.5 million EMV-enabled payment terminals installed out of a total of 12 million POS terminals in place at merchants, according to Randy Vanderhoof, director of the EMV Migration Forum and also executive director of the Smart Card

most current and
pressing daily
news

Business Email*

By clicking the Subscribe button
below, you agree to SC Media
[Terms and Conditions](#) and
[Privacy Policy](#).

SUBSCRIBE

Alliance.

The final push toward the 2015 liability shift is now underway for retailers, supermarkets and drug and convenience stores. The goal is certification of EMV functionality in the second quarter, providing a path for store rollouts in the third quarter, according to Patricia Walters, senior vice president for corporate EMV strategy at Vantiv, a Cincinnati-based payment processing and technology provider. "Large numbers of issuing banks and credit unions are putting cards in the market," says Walters, "largely utilizing their natural reissue cycle to offer their customers the new and more secure functionality."

But, for as far as the industry players have come, Capgemini's Baxley believes that less than half of merchants will be ready to process EMV chip-based transactions by October 2015, when the liability for in-person payment fraud shifts to merchants. She estimates about seven in 10 U.S. payment cards will have a chip. And, more to the point, even if the card has a chip and the point-of-sale terminal accepts chip cards, there is no guarantee that the payment will not be run as an old-fashioned non-EMV-compliant magnetic stripe or swipecard transaction, since the frontline staff who are taking payments may or may not be aware and trained on the new technology and method of transaction.

"It's not like a switch is going to flip on come October," Baxley points out.

A spate of recent high-profile data attacks that hit big merchants like Target and Home Depot did raise concerns about payments fraud and motivate some merchants, says Baxley. Wal-Mart Stores, for one, has been "gung-ho" about its move to EMV at its points-of-sale, she adds. But, many smaller and mid-sized retailers

ADVERTISEMENT



SOC Analyst
APPRECIATION DAY™

NOMINATE your
SOC STARS to the
SOC ANALYST
APPRECIATION
DAY Awards Program

Nominate

BROUGHT TO YOU BY



especially those with slim margins, simply see the cost of adding new chip card-reading terminals and EMV-compliant middleware – and going through a certification process – as a costly proposition with little short-term payback, even if they will have to cover the cost of fraudulent transactions when the liability shifts. “A lot of mid-sized merchants figure they’re not going to be the first place for counterfeiters anyway,” Baxley says.



Some industry observers believe this sentiment will change over the next year. In the rest of the world, the assumption of liability for loss has proven to be that catalyst, according to Sam Curry (*left*), chief technology and security officer at Arbor Networks, a Burlington, Mass.-based

provider of DDoS protection for enterprises. He says that the best predictor for behavior will be actual losses hurting the retail or payment chain. That, he says, will prompt the rapid adoption of the new infrastructure.

“Where the real losses happen, real action will be taken,” Curry says. “At the moment, the liability, for the most part, lies with the card issuers. The key will be ‘who is stuck paying for fraud and when?’”

According to recent research from Javelin Strategy & Research, a Pleasanton, Calif.-based company that provides independent insights into customer transactions, the big-box national retail chains are expected to be fully ready by October, with that readiness trickling down to regional chains in 2016, with more than half of U.S. POS terminals to be EMV-ready by the end of this year, says Nick Holland, Javelin's head of payments

research.

“However, there is a long trail of retailers (58 percent) in the U.S. that have less than 20 employees, and it could take many years for these to transition since they are either unmotivated or still blissfully ignorant about EMV,” Holland says. In fact, as of 2013, more than half of the 500 small and micro merchants surveyed by Javelin “had little or no knowledge of EMV.”

Holland adds that on the issuer side, “there is momentum building and certainly we are seeing an acceleration of portfolio replacements.” Just last year, Holland says, it was anticipated that most issuers would take three years to entirely replace their card portfolios with EMV-compliant chip cards. But as of early 2015, Holland says that many issuers are shortening this rollout timeframe to 18 months or even nine months. “However, as with the merchants, there is a long trail of regional banks and credit unions in the United States that may drag behind with deployment,” he adds.



Boston-based independent research and advisory firm Aite Group offers a similar assessment: 70 percent of credit cards, 41 percent of debit cards and 59 percent of POS terminals in the country will be EMV-capable by the end of this year, according to Julie Conroy (*left*), research director for

the Aite Group's retail banking practice. “The issuers are in good shape, with the little guys trailing a bit,” says Conroy. But she echoes the sentiment that for merchants, the reality of buying, installing, testing and certifying a whole new system for payment is making

more work and delaying their efforts. In particular, getting all their new POS terminals certified for use with all payment brands, transaction configurations and types is creating a “huge bottleneck” for the merchant community.

The Smart Card Alliance along with its sister organization, the EMV Migration Forum, has been working actively with financial institutions, merchants, middleware, hardware and software providers and other industry participants to help smooth the path for the acceptance of EMV chip cards (the EMV Migration Forum has grown to 180 members). A lot of its work over the past two years has been related to helping define the technical roadmap for issuers, transaction processors and payment brands, according to the group's Vanderhoof. While he estimates that only about one-tenth of U.S. payment cards sported a chip entering 2015, he estimates that the number of chip cards will grow five-fold by the end of this year – to 600 million, or about half of the U.S. credit and debit cards in circulation. He expects a “huge ramp-up” with many payment cards simply expiring and being replaced by a new card with a chip.

It may take a while – and a great deal of effort – but proponents say that EMV chip cards are worth the struggle. “There is a real commitment to get there for merchants,” says Liz Garner, vice president of the Merchant Advisory Group, a Minneapolis-based organization that lobbies for merchants' interests in the payments industry. “Many merchants see a tremendous benefit to it.”

Vanderhoof says many more merchants will come online with their EMV compliance closer to the October liability shift, since that is when they will start to see a perk for conducting chip card transactions. Up until then, there's

“no incentive other than to get experience with EMV chip cards and do internal testing with their new systems.” Once the liability for counterfeit card fraud shifts directly to the merchants, they will have considerable incentive to use the more secure chip cards, or be exposed to potentially greater fraud with magnetic stripe. (Note: Gas pumps and ATMs are not expected to be chip card compliant until October 2017.)

“Simply stated, EMV just stops counterfeit card fraud in the card present environment,” Vantiv's Walters says. EMV gives issuers the ability to cryptographically authenticate that the card is legitimate, something they do not have today with mag stripe technology. If it is possible to know that the card is not counterfeit, she adds, it stands to reason that the transactions initiated by this card are also not counterfeit. Hence, the result is stopping counterfeit transactions initiated by the card whenever the chip is used.

Magnetic stripes are like miniature tape cassettes that can easily be overwritten with stolen data, while chips are more like miniature computers that cryptographically validate themselves. “The advantage of an EMV card is that the chip is much harder to clone than a magnetic stripe,” Walters says. The chips are not supposed to give up the secret keys that would be necessary in order to create a clone. Chip-and-PIN cards, specifically, also make it more difficult to steal and use a physical card since the thief would need to know the PIN to use the stolen card.

David Pollino, senior vice president and enterprise fraud prevention officer at Bank of the West, a San Francisco-based financial services holding company, says that banks and merchants are “making good progress,” despite some initial reluctance to embrace EMV. More merchants, he says, are recognizing the benefit of

potentially lowering fraud by using the more complex and more secure chip cards to conduct transactions and make counterfeiting cards more difficult, especially in the face of the major data breaches that have made headlines.

While using the EMV chip makes cards harder to clone, critics point out that since many U.S. merchants and banks do not (or will not) require chip cards to be authenticated by a personal identification number – as they are in most other countries that have EMV in place already – chip card transactions themselves will not be as secure. Many merchants do not want to move to the chip-and-PIN transactions that are common outside the United States, since they don't want to dissuade American consumers. But, by rolling out “chip and sign” instead, it remains possible for a fraudster to steal a physical card and make a purchase by faking the real cardholder's signature. Industry observers also point out that as long as merchants or banks continue to support magnetic stripes, the data stolen from a non-EMV merchant can still be used for fraud.

However, a silver lining of EMV taking so long to evolve is that the cost of EMV-compliant terminals, cards, software and middleware has decreased substantially. Aite Group's Conroy points out that in the early 2000s, an EMV-compliant POS terminal typically cost as much as \$1,500. “And now it's hard to find a ‘regular’ terminal that is not EMV compliant,” she says. Similarly, top issuers would pay roughly \$3 per card for chip cards just three years ago, while now a large issuer pays less than half that for their chip cards.

“The notion of cost will vary greatly among players,” Arbor Networks' Curry says. For card issuers, he explains, it means a dent in transactions and a rise in help-desk calls owing to voice channel fraud. Additionally, some

consumers can get frustrated and others likely will take a while to learn about the new system. For retailers who get onboard with equipment, it will cost very little. But those who don't, he says, will suffer from being the best avenue for fraudsters, their certification will be at risk, they will be burdened with higher rates for transactions, and they could see a loss of business, eroded customer confidence and so on.

Still, many industry insiders maintain that while EMV still faces several hurdles before it becomes truly mainstream, the payments technology is starting to pick up steam. "Once the ecosystem is committed to the new status quo, it should move fairly quickly," says Curry. "The examples of other geographies are there and should be looked to for lessons learned and new processes. Change is always alien to large, process-driven companies, but the affected companies need to realize that they need change and should move to embrace it."

[sidebar]

EMV and PCI DSS:

Delivering a punch

Alone, neither EMV or the Payment Card Industry Data Security Standard (PCI DSS), which sets comprehensive standards to protect payment card transaction from end to end, can defend against dedicated attackers. But, according to the PCI Security Standards Council, when EMV works in tandem with Payment Card Security Standards (PCI DSS 3.1 was released in April), they create a "powerful" force to protect data, bolster security and reduce fraud.

The council notes that the two work together to create a layered approach to securing multichannel transactions.

In fact, EMV chips provide an additional level of authentication at the point of sale. On top of the EMV chip at the POS, PCI Standards protect the POS device, as well as offers layers of additional security controls that business can use throughout the transaction process and across payment channels.

Among those controls are patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees and having clear processes for handling sensitive payment card data. Indeed, the two initiatives may have no choice but to work together. While the PCI Council has laid out the standard, it is the card brand that is responsible for enforcing regulations and issuing any potential fines or fees.

A more extensive version of this chip card article is available [here](#).



Karen Epper Hoffman

Related



NETWORK SECURITY

Hardware cybersecurity leader, Flexxon, introduces Server Defender

[SC Staff](#) May 17, 2024

Flexxon's Camellia Chan on advanced engineering at the hardware layer.



IAM TECHNOLOGIES

Are users ready to go passwordless? Why it's better to move slowly

[Paul Wagenseil](#) February 12, 2024

The most promising passwordless technology isn't enterprise-ready. Focus on feasible IAM upgrades that will strengthen your security posture until passwordless solutions mature.



ENDPOINT/DEVICE SECURITY

Qualcomm, Lenovo flag multiple high impact firmware vulnerabilities

[Menghan Xiao](#) January 4, 2023

Qualcomm on Tuesday disclosed nearly two dozen security vulnerabilities in its chipsets, including the company's flagship suite of Snapdragon processor chips and affecting products that range from cars to powerline communications.

ADVERTISEMENT



SOC Analyst APPRECIATION DAY™

THOUGHT TO YOU BY **DEVO**

NOMINATE your **SOC STARS** to the **SOC ANALYST APPRECIATION DAY Awards Program**

Nominate



ABOUT US

[SC Media](#)

[CyberRisk Alliance](#)

[Contact Us](#)

[Careers](#)

[Privacy](#)

GET INVOLVED

[Subscribe](#)

[Contribute/Speak](#)

[Attend an event](#)

[Join a peer group](#)

[Partner With Us](#)

EXPLORE

[Product reviews](#)

[Research](#)

[White papers](#)

[Webcasts](#)

[Podcasts](#)

Copyright © 2024 CyberRisk Alliance, LLC All Rights Reserved. This material may not be published, broadcast, rewritten or redistributed in any form without prior authorization.

Your use of this website constitutes acceptance of CyberRisk Alliance [Privacy Policy](#) and [Terms & Conditions](#).