The US may be forced to accelerate EMV adoption

The US lags behind most of the world in adopting EMV technology, and has not seemed overly concerned about catching up, argues Erin F. Fonté of Cox Smith. However, recent developments regarding the Durbin amendment, along with what could be the largest series of retail card breaches in the US, have seen many calling for widespread adoption of EMV in the US on an accelerated timetable, Fonté explains.

US EMV implementation

Many readers in the UK and Europe know that EMV stands for 'Europay, MasterCard, and Visa.' EMV is the global standard for interoperation of integrated circuit payment cards and point-of-sale terminals and ATMs. Card and cardholder authentication is carried out via reading information from a microchip embedded in the payment card, and by the cardholder entering a Personsal Identification Number (Chip-and-PIN) into the POS terminal or signing a sales receipt (Chip-and-signature).

EMV authentication also includes a cryptographic message that makes each transaction unique. This 'dynamic authentication' is considered to be a more secure form of authentication than the traditional magnetic strip currently used in the United States, and has been widely adopted in Europe and elsewhere.

In the US, Visa and MasterCard announced in 2011 and 2012, respectively, that to reduce the risk of fraud losses and identity theft, both networks were releasing strategies, timelines, and incentives for US merchants, issuing banks, and acquirers to move from magnetic strip authentication to the EMV standard by 2013, with liability shifts as an incentive for EMV adoption by 2015.

In August 2011, Visa announced three EMV initiatives:

- Expansion to the US of the Technology Innovation Program (TIP), which eliminates annual PCI validation requirements for merchants who have 75% of Visa transactions originating on chip-enabled terminals. To qualify for TIP, POS terminals must be enabled to accept contact and contactless chip cards and NFC contactless payments from mobile devices.
- US acquirers and processors must support chip transactions with dynamic authentication no later than 1 April 2013.
- Liability shift for domestic and cross-border counterfeit POS transactions effective 15 October 2015. Liability for fraudulent transactions at merchants, that at a minimum, have not installed contact chip terminals, will shift from the card issuing bank to the acquirer and the merchant.

In February 2012, MasterCard released a statement on EMV:

- MasterCard will have 'an immediate focus' on working with acquirers to aid them to support dynamic authentication by April 2013.
- MasterCard will introduce a 'liability hierarchy' in which the cost of fraud from lost or stolen cards will fall upon 'whichever party adopts the less secure approach.' This means merchants that install EMV terminals with chip-and-PIN capability will not be liable for lost-or-stolen fraud that occurs on EMV chip-and-signature transactions, effective October 2015.
- MasterCard will provide 'true financial benefits' to merchants that install EMV terminals: relief from PCI audits; a 50% reduction in data breach liability for card-reissuance and fraud costs for merchants processing at least 75% of transactions on EMV capable terminals; and effective October 2015, 100% relief of those costs if the merchant is processing 95% of transactions on EMV terminals.

The 'need' to embrace EMV

Many large retailers in the US have been pushing for EMV adoption to increase transaction security and reduce fraud. Other merchants have argued against adoption of EMV because of the large cost of upgrading point-of-sale terminals. Issuing banks in the US have also traditionally objected to

mandatory EMV upgrading because of the cost and inconvenience of cancelling magnetic stripe cards and issuing EMV cards.

However, in the wake of large data security breaches suffered by Target, Nieman Marcus, and Michaels stores, US attitudes toward EMV on all fronts - merchant, issuing bank, and consumer - may be shifting. The Federal Bureau of Investigation recently warned retailers in the US that the recent attacks against Target, Nieman Marcus and Michaels foreshadow what could become the 'new normal' in the US as hackers become increasingly sophisticated at breaking into 'antiquated payment systems.' Banks, retailers and policymakers have been slow to address the growing sophistication of cybercriminals, and it is possible that the entire US payments systems are becoming more and more vulnerable and continue to fall short of what is needed to defeat aggressive hackers that see dollar signs and multimillion-dollar paydays.

An industry group, including major American credit card issuers, is pushing for widespread adoption of chip cards by October 2015. Consumer groups want lawmakers and regulators in Washington DC to mandate a faster and more complete shift to EMV, but federal regulators have balked at forcing the banking industry to invest in new technology, especially if there is a chance that it might not thwart future attacks (Did I mention that EMV itself is 20 years old, and is itself vulnerable to various forms of hacking?).

This renewed call for changing all cards in the US over to EMV also comes at the beginning of what could be widespread disruption of payments systems, and players in the mobile payments space see the argument for EMV as a Trojan horse for entrenched payment networks to lobby for new terminals that accept both EMV and 'near-field technology' (NFC) chips embedded in mobile devices. So the EMV argument in the US has near-term ramifications for fighting fraud, and longer-term ramifications about whether mobile payments will use EMV-protected NFC card credentials stored on the phone, or whether mobile payments move to a 'single-use token' method where the payment account credentials never have to travel (whether encrypted or not) at all.

Impact of Durbin Amendment and swipe fee battles

The arguing and posturing of banks and retailers when discussing EMV adoption in light of the retailer data breaches is occurring when retailers have successfully gotten a Washington DC district court to overturn the Durbin Amendment rules regarding maximum debit card fees, which the retailers deem to be too 'bank friendly' and still too high based on actual issuing bank and network costs. Score one for the retailers.

Meanwhile, a US district court in New York recently approved a massive settlement in credit card interchange fee litigation brought by retailers over eight years ago. The initial proposed settlement would have been the largest single settlement in the history of antitrust law in the US (around $7.2 billion), but so many retailers opted out of the class action settlement that it is now down to just above $5.7 billion. Retailers who have opted out, including many large US retailers, intend to pursue litigation because they felt the settlement terms were too onerous on merchants (i.e. binding all existing and future merchants that accept Visa and MC to the settlement agreement). This litigation will continue.

It is not surprising that reactions to retailer data breaches have the same tone of rancor between banks and retailers that has existed in the US for the past several years. Bankers want retailers to cover more of the cost of data breaches. Retailers say bankers need to adopt more secure card technology. Lawmakers must decide whether to act to require tighter security or swifter disclosures.

US merchants typically pay fees totaling about 2 percent of the purchase price for credit-card transactions. These so-called swipe fees, also known as interchange, help card-issuing banks such as JPMorgan and Bank of America Corp. fund rewards programs and cover fraud costs. Lenders and retailers have sparred for years over swipe fees, which merchants have said are too high. In 2011, retailers won one round when lawmakers authorised a cap on fees for debit-card transactions, which has reduced banks' annual debit-interchange revenue by 50 percent, to about $8 billion.

Now banks and retailers are fighting over who should bear the costs of repairing the damage and adopting more secure payment technology. Retailers and consumer advocates in the US accuse banks of clinging to obsolete magnetic-stripe technology that has put merchants and their shoppers at risk.

An added wrinkle to EMV adoption in the US is not just the cost of adoption, but also the so-called 'dual network' requirement of the Durbin Amendment. In July 2013, the EMV Migration Forum, an industry group that has been working on ways to make EMV compliant with Durbin's mandate that merchants have a choice in debit-transaction routing, solved a

vexing problem related to EMV chip cards and the Dodd-Frank Act's Durbin Amendment. But whether that solution will smooth the way for deployment in the United States is less clear.

The EMV Migration Forum announced in early July 2013 that the group had settled on what it calls a 'recommended path' that steers between and among at least three competing solutions.

No debit card will be allowed to accommodate more than one solution, an approach that the group says simplifies card issuance as well as merchant acceptance. But rather than mandate any one solution, the recommendation leaves it up to issuers to decide which one to embed on any given card. MasterCard Inc. and Visa Inc. have both proposed solutions, and so has the Secure Remote Payment Council, whose debit-network members adopted technology from Discover Financial Services.

Each of the solutions presents a means of letting merchants and merchant processors identify networks supported by a given issuer and then route transactions to the preferred network. As a two-decades-old, proprietary standard deployed until now only outside the US, EMV does not normally allow for this routing choice. The so-called common AID solutions, or application identifiers, are expected to give EMV that ability for debit payments. In the EMV specification, the AID is a string of characters that identifies both the network brand and the specific type of card, for example, credit or debit.

Some observers say the new consensus on how to field a debit-routing solution could spur deployment of EMV in the US, the last major industrialised nation to adopt the technology, which replaces magnetic stripes with microchips. Observers differ, too, over whether merchants will be ready for the liability shift set by Visa and MasterCard for October 2015[1].

Some observers say the new consensus on how to field a debit-routing solution could spur deployment of EMV in the US, the last major industrialised nation to adopt the technology, which replaces magnetic stripes with microchips.

Retailer breaches and EMV adoption

Many industry observers in the US think that fallout from the recent retailer breaches may light the spark for accelerated and widespread EMV adoption in the US. In recent retailer testimony before the US Congress, retailers spoke on the sophistication of the cyber-attacks, the complicated forensic investigations used to detect and contain the malware, the need for EMV technology for card payments and the need for a concerted effort by public and private stakeholders to counter the growing, lucrative and sophisticated cybercriminal industry. The congressional hearings also focused on how quickly and expensive it would be for industry to implement EMV technology for payment cards[2].

Target stated that it will spend a lot of money in the short run implementing technology at its checkout counters to accept more secure EMV credit and debit cards. Target's Executive Vice President and Chief Financial Officer John Mulligan said upgrading the retailer's systems to handle EMV could cost the company up to $100 million[3].

Target also called for all stakeholders to take up the 'shared responsibility' of payments security as it announced an accelerated timeline for its own $100 million EMV migration plan. Target also said that now is the time for stakeholders to work together for a more secure payments environment in the US.

Target stated that it is also investing in solutions that will make mobile transactions more secure[4].

Conclusion

The EMV question is part of a much larger drama among banks, retailers, new payment entrants and regulators regarding the future of US payments systems. Concern about the vulnerability of magnetic stripe-based payment transactions, and breach incidents that are growing in sophistication and size, has many stakeholders questioning if the shift to EMV technology is now necessary to protect US payment systems integrity and stunt massive losses. Many mobile payments players see EMV as merely a weigh-station on the road to a more secure future using mobile payment transaction systems where token-based transactions may be a more secure option in the long run. In an environment where banks and retailers have continuing animosity, it is clear that they also have a common interest in adopting solutions that increase security and stop massive fraud losses.

Erin F. Fonté Shareholder
Cox Smith, Texas
efonte@coxsmith.com

1. Source: Digital Transactions, 'New Consensus on Debit Routing Removes EMV Obstacle But Leaves Timing Unclear,' 8 July 2013.
2. Mobile Payments Today, 'Target and Neiman Marcus: We Did All We Could,' 5 February 2014.
3. Krebs on Security, 'Target Hackers Broke in Via HVAC Company,' 5 February 2014.
4. Mobile Payments Today, 'Target puts EMV migration on fast forward,' 5 February 2014.