The U.S. Migration to EMV: Considerations for the Payments Environment

In 2015 the payments industry is taking aggressive steps toward modernizing credit and debit card processing with the much-publicized shift to EMV technology. The chip-enabled card will improve security and better protect consumers from card fraud. Card issuers and retailers are spending millions to upgrade cards and point-of-sale terminals in advance of an October 1st deadline when the liability for fraudulent purchases will shift to the party -- either the issuer or retailer -- that still relies on magnetic-stripe processing. Once EMV becomes widespread, EMV adoption promises to improve payment card security for card-present transactions, although many security challenges will remain. This brief attempts to highlight issues involved in the migration to EMV and to shed light on further work needed to promote comprehensive payment system security.

Kandice Alter and Anna Neumann --- May 18, 2015

Until now, the U.S. payment card industry has lagged other developed economies in adopting more secure chip-embedded EMV cards, primarily due to the sizable investment associated with upgrading an estimated 1.2 billion credit and debit cards, and 12 million point-of-sale (POS) terminals[1]. Additionally, fraud rates remain fairly low in spite of massive retail payments breaches in recent years that have exposed, by most estimates, over a hundred million consumer card accounts. As such, card issuers and the card networks have historically chosen to accept and absorb fraud as a cost of doing business. But the relentlessness of retail POS breaches is exacting a significant cost above and beyond fraud losses. Retailers have spent sizable sums on breach response in efforts such as consumer notification, credit monitoring for impacted consumers, and legal costs. Card issuers have spent millions re-issuing compromised cards, investing in resources to monitor card usage, and addressing potential and actual unauthorized card activity. And an estimated one in four Americans have had personal and financial information compromised and are at risk of financial fraud and identity theft, or simply dealing with the inconvenience of frozen accounts and reissued cards[2].

Chip-enabled cards have emerged as the industry's tool of choice for combatting POS card theft that has fueled a robust underground network for card fraud and counterfeiting. As an incentive for merchants and card issuers to upgrade to EMV technology, card networks Visa and MasterCard established October 1st as a liability shift deadline for adoption of EMV in the U.S. The liability shift extends responsibility for fraud losses due to unauthorized charges to the entity in the payment channel (either the bank or merchant) unable to transact a card payment as an EMV transaction. Issuing banks are currently held liable to pay for fraudulent purchases on magnetic stripe cards swiped at a POS terminal. But after Oct 1, should a retailer accept an EMV chip card and process it as a regular magnetic stripe transaction in the absence of an EMV terminal, the retailer – no longer the card issuer – would now be liable for any fraudulent charges that might occur as a result. Until the U.S. has fully transitioned to chip cards with all retailers able to accept them, it will be necessary for issuers to include the magnetic stripe on chip-enabled cards, and magnetic stripe card data will remain a target of POS malware.

What follows are some areas of concern with the transition to EMV.

As the liability shift deadline approaches, the conversion to EMV chip-enabled cards and EMV point-of-sale terminals will be well below 100%, with smaller banks and merchants lagging.

Most industry estimates peg the EMV card conversation rate to be over 50% by the end of 2015. Many consumers already have chip-enabled cards, and according to recent studies, roughly, 75% of credit cards and 40% of debit cards are estimated to be converted to EMV cards by the fall.[3] The large majority of chip cards are coming from large issuers – Bank of America, etc. Smaller banks are converting cards more slowly due mainly to cost: chip-embedded cards cost as much as ten times what magnetic stripe

[1] Statistics from CreditCards.com and EMV Connection

[2] Based on a survey by Harris Poll in March, 2015: "Data Breaches Affect One in Four Americans," Credit Union Times; April 21, 2015

[3] "Issuers Forecast U.S. Shift to Chip Cards To Be Nearly Complete by 2017," BusinessWire; May 4, 2015; and "Are Small Retailers and Banks Likely to Miss the EMV Deadline?" PYMNTS.com; April 21, 2016

cards costs to manufacture[4]. Some banks will be issuing cards in mass to prepare for the shift, rather than issuing cards over yearly expiration cycles. The conversion of debit cards lags behind credit cards mainly due to the fact that issuers have to program the cards to allow merchants to route transactions through multiple debit routing networks, making the upgrade process more complicated.

Retailers also face significant costs as POS terminal upgrades can run an estimated $200-$1000 per device.[5] Mainly the largest retailers such as Walmart, Target and Costco have terminals in place and are starting to enable them. Aite Group estimates that 59% of terminals will be EMV-enabled by the end of 2015.[6] A recent Aite Group survey points to concerning statistics about the conversion of small/medium sized businesses (SMBs). A third of small businesses surveyed were unaware of the EMV standard, and among those that were aware, just a little over 60% have completed or were working on the transition.

Many SMBs may be at greater risk for absorbing fraud costs with the liability shift in October. These firms are typically the least equipped to prevent and combat cyber threats and may, as a result, become richer targets of hackers. This includes not just retail stores but healthcare providers, universities, and other entities accepting cards for payments.

The card networks and payment system providers and integrators are stepping up initiatives to educate SMBs on EMV and the migration process but complete conversion to EMV terminals is expected to take several years.

Card issuing banks heavily favor chip and signature authentication over chip and PIN verification for card-present transactions, an approach that doesn't fully take advantage of EMV's security features.

The liability shift deadline makes clear for institutions and merchants the risk of non-compliance, but gives latitude to card issuing banks in determining how they implement EMV. Most banks are opting to implement chip and signature authorization citing consumer convenience as the driver, along with concerns the overall process change could slow down transactions as retail employees and customers adjust to EMV terminals and processing. Many issuers view the added step of entering a PIN complicating the transaction for the consumer who may be weary of having to remember multiple PINS and passwords, which could ultimately lead to attrition or lost sales. With the average card-using consumer holding 3.7 different credit cards at a given time[7], few banks want to have the only card in a consumer's wallet requiring a PIN.

In spite of recent large retail payments breaches, the cost of fraudulent, unauthorized transactions remains low – roughly $10 for every $10,000 in transactions on credit and signature debit cards[8]. Banks

[4] Estimates vary and actual costs are impacted by such factors as volume and design requirements. See "EMV in the U.S.: It Will be a Long Ride," PYMNTS; June 13, 2014
[5] Many variables influence these costs including service agreements, volumes, etc. See "The $8.5B Shift to New Credit Cards Won't Fix Security Issues," Entrepreneur; March 3, 2015
[6] "More Than Half of U.S. POS Terminals to Be EMV Chip-Enabled by Year End," Business Wire; April 12, 2015
[7] See Credit Card Ownership Statistics at credidcards.com
[8] See the 2013 Federal Reserve Payments Study

contend that chip and signature authentication provides protection against the counterfeiting of cards which constitutes the majority of fraud.

But retailers and consumer groups are questioning the decision to forego PIN authentication, viewing it as a necessary measure in further securing transactions by verifying the legitimacy of the cardholder at the checkout, and minimizing fraud losses resulting from lost or stolen physical cards.[9]

Chip and PIN authentication takes full advantage of EMV's security features, and has been the mandate in most other countries where EMV has already been implemented.

The October 1st liability shift provides incentive and momentum for the transition to EMV, but until magnetic stripe cards and terminals are removed from transactions, card theft and counterfeiting will not be eliminated.

Consumers holding combination EMV and stripe cards are still at risk of having account data stolen during a POS transaction. Issuers will need to produce combination magnetic stripe and EMV cards until the vast majority of retailers have fully converted to EMV terminals, which may take up to 5 years for a critical mass of EMV merchants.[10]Any retailer continuing to use magnetic stripe terminals remains a target for POS malware which can continue to export usable cardholder data even from EMV-enabled cards that also carry a magnetic stripe. Additionally, In recent retail data breaches, POS scraping malware is responsible for stealing over a hundred million credit and debit cards, and only a portion of those cards currently show up on carder forums where hackers sell cards for counterfeiting. These stolen accounts could still be at risk for counterfeiting and fraud even after the legitimate cardholder's card is reissued as an EMV card.

Chip-embedded EMV cards will protect against counterfeit fraud in card-present transactions, but provide no added protection for the card-not-present environment. The EMV upgrade could, in fact, drive fraud to other types of transactions such as on-line retail.

When the UK implemented EMV nearly 10 years ago, fraud from counterfeit cards declined 56% from 2005 to 2013. But card-not-present fraud (mainly e-commerce fraud) increased 79% from 2005 to its peak in 2008, when on-line merchants began employing better analytics and security features.[11] As the number of on-line transactions continues to increase and easy POS malware targets decline, fraudsters will undoubtedly search for new ways to infiltrate e-commerce.

To combat this expected shift in fraud from in-store purchases to online purchases, e-commerce merchants will need to be more vigilant in detecting and stopping fraudulent transactions. Currently, e-commerce merchants avoid adding extra security steps to the checkout process to make payments more convenient for their customers. As e-commerce fraud increases, merchants will need to consider

[9] "Diverse Groups Call for the Implementation of Chip and PIN Technology," PR Newswire; April 30, 2015
[10] "EMV Adoption in the U.S.," Rippleshot; May 5, 2015
[11] Ibid.

implementing tools such as behavioral analytics and 3-D Secure (an extra security screening to verify a cardholder's identity) to prevent major losses[12].

Additional tools such as tokenization and encryption can help to prevent fraud in both the card-present and card-not-present environments. For example, tokenization of a customer's card data at the physical POS removes the customer's card account number from a merchant's system, replacing it with a dummy token value. Even if criminals breach the merchant's system, they would not be able to use stolen token values to make online purchases. As the shift to EMV continues and criminals shift to new types of fraud, industry players will need to work together to develop standards for, and make investments in these other security measures to stay ahead of changing fraud tactics.

CONCLUSION

EMV adoption is pushing forward in the U.S. largely because the card networks have set a liability shift deadline of October 1st as an incentive for banks and merchants to make the necessary investments in new card technologies. Small merchants and banks in particular will face high relative costs during the transition to EMV, and may not have the resources or expertise to meet this deadline. Until the vast majority of cards and terminals have been updated to allow for secure EMV transactions, card fraud will continue at the point of sale.

Even after transitioning to EMV, banks and merchants will continue to face the risk of data breaches and card fraud, especially in the card-not-present environment. At particular risk are e-commerce merchants, since the level of on-line fraud is expected to increase dramatically after card-present fraud becomes much more difficult.

Recently retailers and industry groups have raised concerns about the current state and progress of the transition, along with the liability shift deadline falling so close to the holiday shopping season. To date, the card networks remain firm in their original deadline but have been increasing outreach and providing tools to support retailers in upgrading to EMV.

As October 1st nears, we will continue to follow the U.S. implementation and what follows after the U.S. EMV deadline.

[12] See Aite white paper prepared for RSA "Card Not Present Fraud in a Post-EMV Environment: Combatting the Fraud Spike;" June, 2014