DEPTH. FOCUS. SERVICE.

MERCATOR ADVISORY GROUP

PARTNERING FOR SUCCESS: NAVIGATING THE EMV IMPLEMENTATION PROCESS

A Mercator Advisory Group Research Brief Sponsored by Moneris Solutions

November 2014

Contents

Figures

The EMV Standard

Reducing Counterfeit Card Fraud

The EMV standard was developed in the 1990s to mitigate card-present fraud in Europe and other markets where online, real-time connectivity to issuers' authorization systems was not widely available. The unique data provided by the EMV chip embedded in payment cards with this standard makes it nearly impossible for fraudsters to produce counterfeit cards. Fraud related to counterfeit cards has essentially been eliminated in countries where EMV was widely adopted.

Reducing Card Theft Fraud

The incidence of two other types of fraud—lost/stolen and card-not-received fraud—has been greatly reduced as well by requiring EMV cardholders to enter a personal identification number (PIN) rather than a signature when they perform a transaction using their EMV cards to verify that the customer is the legitimate cardholder and not someone using a stolen card. The earliest implementations of EMV used *offline PIN*, whereby the chip itself verifies the PIN. Other markets have used *online PIN* verification, with the PIN verified with the issuer online in real time. Some issuers prefer online verification because offline PIN capabilities require a more expensive chip solution.

Countries with nearly 100% online availability such as Canada (and now the United States) have upgraded to EMV in order to stop the shift of card fraud to these markets and to ensure that payment cards issued in these countries will be readily accepted in world markets where EMV is the widely accepted card standard. To facilitate the transition, card networks have set dates when fraud liability will be determined by a merchant's and issuer's relative investments in EMV technology. Additionally, card networks have offered incentives to merchants who upgrade their terminals prior to the dates for liability shift dates.

Chip and PIN vs. Chip and Signature

So far, most U.S. issuers have opted to issue EMV cards that require only a signature for cardholder verification. No PIN is required. Omitting PIN capabilities from the cards reduces the cost burden for the issuing banks. Issuers are also concerned that requiring cardholders to enter a PIN at the point of sale would complicate the checkout experience for cardholders. That is because the U.S. has become accustomed to signature verification over several decades, and since consumers tend to carry multiple credit cards, they could find it difficult to remember unique PINs for all of them. "Chip and signature" implementations forgo the benefits of potential reduction in lost/stolen and card-not-received fraud that EMV affords, however. Therefore it is possible that "chip and PIN" will eventually become standard in the U.S. as it is in many other countries.

Prior to the data breach at Target stores in 2013, and the many more data breaches that occurred in 2014, the payments industry seemed to be anticipating a prolonged, gradual roll-out of EMV cards and terminals that would almost certainly begin with implementation of chip and signature as a first step. These data breaches have led few

major issuers and merchants to accelerate their migration to EMV and have raised awareness of the added security inherent in a chip and PIN implementation despite the likely inconvenience to cardholders of having to remember multiple PINs.

Very shortly after the Target data breach, the NRF, Walmart, and Target expressed support for chip and PIN technology. Issuers, namely Chase and Barclaycard, soon followed. Barclaycard has at least one chip and PIN card in the market today, and Chase has announced plans to begin issuance by year end. Most recently, President Obama himself encouraged use of chip and PIN technology in an Executive Order (signed October 17, 2014[1]) covering government payment card programs. The first wave of EMV issuance in the U.S. will be primarily chip and signature, but current momentum suggests that chip and PIN might not be far behind. Merchants and independent software vendors (ISVs) should select a processor that can deploy solutions supporting issuers' evolving strategies.

Card Network EMV Road Maps

Each of the major card brands has by now published a road map charting a timeline for the transition to EMV as well as the penalties for parties that do not comply. For the conversion of point-of-sale systems, four common milestones are addressed by all four major U.S. networks, as shown by the timeline in Figure 1:

- ✓ Relief from requirements to report PCI compliance testing results for early conversion
- ✓ Merchant acquirer capability requirement
  - o Merchant fraud liability shift
  - o Fraud liability shift for gasoline retailers

Figure 1: Road Map for Introducing EMV to the U.S. Market

Source: Mercator Advisory Group

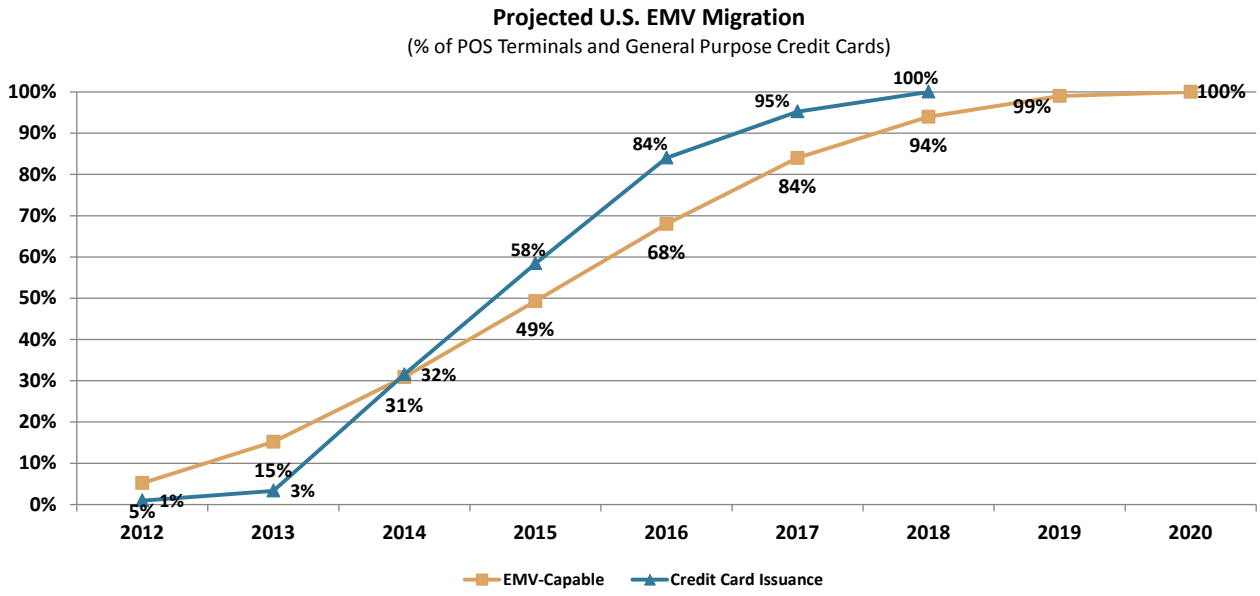
[1] http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions

Outlook: EMV Adoption in the United States

Credit Card Issuance

Figure 2 presents Mercator Advisory Group's forecast for EMV adoption in the United States, which we previously published in an August 2014 research note titled *Preparing for 2015: The Year of the Liability Shift*. Merchants and issuers are following typical upgrade cycles for their POS terminals and payment cards. Consequently, Mercator anticipates that complete migration of POS terminals will lag reissuance of credit cards by a couple of years. Many of the largest U.S. credit card issuers have already made significant progress converting their key portfolios to EMV. We expect about 58% of general purpose credit cards will be EMV compliant by the end of 2015, a significant increase from the 3% of cards that we estimate was compliant at the end of 2013. EMV-compliant transactions will quickly become commonplace. In 2016, Mercator estimates that U.S. consumers will complete EMV transactions totaling $950 billion using credit cards alone.

Figure 2: The Majority of Credit Cards Will Likely Be Compliant with EMV Standard by 2015



Source: Mercator Advisory Group estimates

Debit Card Issuance

A much smaller percentage of debit cards than credit cards will be EMV compliant by the end of 2015—Mercator estimates between 10% and 15%. Much of the delay in debit portfolio conversion is due to complications resulting from the passage of the Durbin Amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Amendment, in addition to lowering debit interchange, gave merchants new rights with respect to routing debit transactions to the lowest-cost network. The Federal Reserve interpreted the Amendment to intend each debit card to have two unaffiliated networks, one signature network and one PIN network.

The Retail Merchant Council sued the Federal Reserve Board, however, claiming that cards should have four network options in total, two unaffiliated PIN networks and two unaffiliated signature networks. This debate stalled EMV debit issuance because such network routing options are not part of the original EMV specification and would require substantial development and collaboration of the numerous signature and PIN debit networks operating in the United States. An appellate court has since ruled against the Retail Merchant Council, thus giving the green light for financial institutions to begin issuing EMV debit with only two network options.

Meanwhile, Visa and MasterCard have led the development of a common EMV application identifier (AID) to support routing between the PIN and signature networks that financial institutions make available. All of the major debit networks have already adopted the common AID. On September 30, 2014, Bank of America announced the first large-scale conversion to EMV debit in the United States. Other leading debit issuers will likely also begin EMV debit issuance in 2015.

Acceptance

From the perspective of EMV acceptance, many U.S. merchants have been apathetic toward the pending industry conversion. Mercator Advisory Group estimates that just fewer than half of all POS terminals in the U.S. will be EMV-capable by the end of 2015. This percentage of capable terminals counts those that have all the hardware (but not necessarily the software) required to process an EMV transaction. The percentage of POS terminals that will have been configured with the software as well and therefore will actually be able to read a chip card will be much smaller.

A limited number of very large merchants such as Walmart have already begun processing EMV transactions. And some others, both large and small, are already preparing for next year's liability shift. Midsized merchants, large enough to have a nuanced processing environment, but not so large as to have sufficient internal IT resources, are most in need of a reliable EMV partner to manage the transition. Merchants that haven't started the process but want to be compliant by October 2015 should choose a processor that has experience completing conversions quickly and on schedule.

Impact of EMV on Merchants

Implementation Pains

Contrary to speculation that emerging technologies would allow new payment providers to disrupt the existing payment landscape, it will likely be EMV—a very familiar technology—that will have the greatest near-term impact on the retail industry. The two primary concerns for merchants considering how best to address the new EMV mandates are costs and customer experience. Unfortunately, there aren't many options on the cost side. Some processors may offer a free EMV terminal or two, but merchants need to budget for the costs related to installing, testing, and certifying the hardware infrastructure necessary to process EMV transactions.

Merchants have much more control over how they will manage the customer experience through this transition than they do over the cost elements. Checkout times will likely be slower than they are today. POS terminals take more time to read a chip than a mag stripe, and it will take time for cardholders to become accustomed to the new process. Until then, inexperienced cardholders will likely question cashiers about how to use the chip reader terminals, extending checkout queues even longer. Some degree of the usual implementation pain can also be expected such as an inability to read the chip, unfriendly error messages, PIN/signature confusion from the terminal, and other issues yet to be discovered. Merchants can mitigate checkout delays, though, by properly training front-line employees and by enabling contactless readers.

Mobile Payments and Security

The launch of Apple Pay in October 2014 has created some division among merchants with respect to acceptance of contactless payments. A few merchants who are MCX members have turned off contactless readers, and therefore Apple Pay acceptance, to promote CurrentC, the MCX mobile payment solution expected to launch in 2015. The most significant implication of Apple Pay though, is that it has reignited interest in Near Field Communications (NFC) as a technology for mobile payments. The application has demonstrated that mobile payments don't have to be as awkward or slow as in some previous initiatives. Card networks and issuers have heavily promoted Apple Pay and other NFC-based mobile wallets, which will support consumer adoption. Apple Pay is just the first implementation of the card networks' tokenization initiatives that will improve payment security within the merchant environment. It is important for merchants to certify contactless acceptance now, so they can quickly accept new payment methods as they become available. Merchants that are unable to accept new methods of payment, particularly types that improve cardholder security, could be perceived as risky.

Finally, 2014 is going to be remembered for the incredible number and scope of data breaches that occurred at major U.S. retailers. Consumers are frustrated with these lapses in security. Many are aware of the so-called chip card technology widely used in other countries, which has been widely discussed in various media outlets. Merchants that don't demonstrate a commitment to security risk losing the business of security-minded customers.

What to Look for When Selecting a Security Partner

The issue of payments security is much bigger than just EMV. EMV is an essential component to any payments security strategy, but end-to-end encryption and tokenization are also important for locking down a payment environment. Merchants should look for a security partner that can deliver all three.

EMV Processing Experience

The process of EMV development, certification, and testing is time-consuming and often frustrating. Merchants and ISVs can minimize some of their difficulties, however, if they work with a processor that has experience with EMV processing. Even though the U.S. payments environment has many distinctive qualities, processors that have worked with the card networks to implement EMV in other countries have found ways to simplify the process. For example, merchants can greatly condense the certification and testing processes by integrating with a payment solution for EMV and contactless that is precertified as compliant by one or more of the card networks. In doing so, merchants can be confident that their system will pass all mandatory EMV test cases. System validation can occur within 7–10 days following the integration instead of the typical 8–12 weeks for a customized solution.

Merchants and ISVs need to certify compliance with each of the card networks after they have completed the testing phase. Card networks charge for this service and often take weeks to respond to a merchant's request. Some processors have been designated as certified agents of one or more card networks. This allows the merchant to deal with one authorized party, minimizing cost and delay in waiting for the network certification. Merchants that want to integrate directly with their processor's host system should partner with a company that provides tools to manage this process (for example, a network-approved simulator for testing various EMV transactions). Some processors also offer customized training seminars for merchants that are unfamiliar with the EMV specification but find it necessary to manage their own integration processes.

Integrated payments software adds yet another layer of complexity to an EMV implementation, particularly for firms that have more than one ISV partner, because integrated applications need to function as a cohesive infrastructure. Every application integrated with payment processing must pass hundreds of network-specific test cases in order to attain certification. ISVs that partner with processors that support multiple EMV devices with consistent embedded software can provide substantial benefits to their merchant clients. For example, leading solutions can contain EMV-related testing to payment modules without impacting other ISV software. Precertified solutions can be leveraged here too, and leading processors have developed tools that can reconcile card brand nuances to streamline product validation. Finally merchants and ISVs that partner with processors that can certify on behalf of one or more networks can avoid potentially lengthy queues to certify directly with the networks.

End-to-End Encryption (E2EE)

Encryption and tokenization are two highly complementary products to EMV, and interest in both technologies has been growing over the past year. Encryption is a critical tool that secures data in motion, as in the case of an authorization request. Mercator Advisory Group recommends that merchants add encryption services at the same time as they move to EMV because "E2EE" is quickly becoming the de facto standard in the market. Most major processors have an end-to-end encryption solution in market today. And they don't necessarily have to be implemented at the same time as EMV, although minimizing costly touch points to systems is advantageous. Merchants that integrate with a processor's payment solution have the advantage of being able to easily deploy encryption when needed. What is most important is for merchants to choose a true "end-to-end" solution. Applications that operate within the certified PIN transaction security (PTS) device are able to encrypt account data the moment a card is inserted, swiped, tapped, or manually entered into the terminal. Because data remains encrypted until it reaches the processor, merchants never have access to sensitive information, which can greatly reduce the scope of PCI compliance.

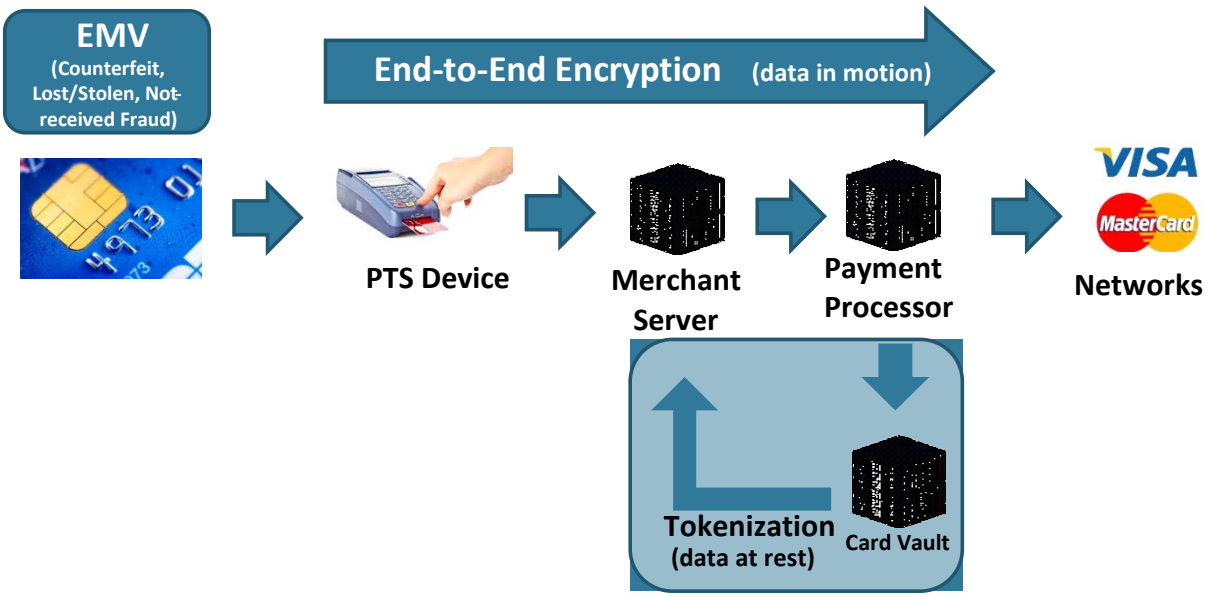
Tokenization

Tokenization is an equally critical tool, but unlike encryption, its focus is on securing data at rest. Merchants often store customers' payment card data to track purchases (often to support loyalty programs) and to facilitate refunds or perform follow-on transactions Tokenization solutions replace card data with a unique numerical token. The leading processors have tokenization solutions today. An important consideration for merchants choosing a tokenization solution is whether it uses "format-preserving" tokens. In this approach, the token is in the same format (15 or 16 digits) as the primary account number (PAN). Format preservation is important for integration with many common accounting and reporting software systems. Additionally, format-preserving tokenization allows merchants to confirm payment with customers by referencing the last four digits of the account number.

A Layered Approach to Payment Security

Figure 3 summarizes critical payment security solutions offered by leading processors. Merchants that implement a layered approach to security that includes EMV, encryption, and tokenization benefit from reduced PCI-compliance costs and greatly reduced liability in the event of a network intrusion.

Figure 3: Implementing a Layered Approach to Payment Security



Source: Mercator Advisory Group

Case Study: Learning from a Market Leader

To illustrate best practices around EMV implementations in a country where EMV is fully deployed, we interviewed one of the first merchants to begin processing EMV transactions in that country. This organization is a national retailer that operates several business units, as well as an issuer of credit cards. The company decided to work with its existing acquirer, Moneris Solutions, to tackle the migration to EMV. Moneris was chosen in part because of its willingness to collaborate, which entailed customizing a payment integration solution as well as bringing card networks, retail operations, and card operations together to develop enterprise-wide strategies. Moneris also provided a dedicated technical integration engineer who worked with the client through every phase of its EMV implementation, including application development, integration, certification, pilot, and roll-out, and who even provided post roll-out support.

Starting in 2008, the company upgraded more than 1,000 terminals across its businesses. Charge-backs declined 70% in the first year of the roll out. The retailer also partnered with Moneris to develop and deploy an end-to-end encryption solution, which made the company's security environment much easier to manage, especially with respect to PCI compliance. The retailer has also activated the contactless function on its terminals over time. Contactless continues to be a popular method of payment with consumers, which is common in the country.

One of the most important take-aways from this retailer's implementation, among the first its country, is not to underestimate the need to train cashiers. Retailers should educate employees on what EMV is and how the new cards operate, set a formal fall-back policy (when is it O.K. for a cashier to swipe a card with an EMV chip?), and set guidance for what cashiers should do if a customer forgets a card in the terminal. More than anything, merchants shouldn't expect that consumers will get all the information they need about EMV from their financial institution.

Steps to Implementation

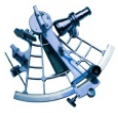
The following list highlights the major steps that merchants must complete to process EMV transactions. Merchants should be prepared to take the lead with the nontechnical elements of the migration process (steps numbered 1–5 and 9). Processors should be able to provide some amount of staff assistance, training materials, and other tools to assist with system integration, testing, and certification, although larger merchants might have sufficient internal IT resources.

1. Assign a person to manage the EMV conversion process.
2. Determine the importance to your organization of meeting liability shift dates.
3. Evaluate proposals from at least a few processors, and score each on EMV capabilities, other security offerings, customer support, pricing, and ability to meet desired project timeline.
4. Engage your processor for technical and operational consulting
5. Assess migration impact on POS technology and business operations.
6. Integrate with processor payment solution or host system.
7. Perform scheme, exception, and acceptance testing.
8. Obtain scheme certification.
9. Develop and implement a training program for front-line employees.
10. Deploy POS software and hardware (if it is not already in place).

The Value of Experience

U.S.-based merchants and ISVs in need of EMV integration and processing services should look for processors that can bring international implementation experience to the table. Companies like Moneris Solutions have invested in developing particular expertise in working with merchants to support the EMV migration process. Moneris first started preparing its host system for EMV in 2003 and has been processing live, EMV-compliant credit and debit card transactions since 2005. More than 90% of all in-store transactions processed by Moneris are chip and PIN transactions, of which approximately 7% are contactless transactions. Numerous merchants have used the company's POS Pad application to simplify the certification and testing process. And Moneris has also developed proprietary encryption and tokenization solutions to round out its suite of payment security products.

Copyright Notice



About Mercator Advisory Group

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver pragmatic and timely research and advice designed to help our clients uncover the most lucrative opportunities to maximize revenue growth and contain costs. Our clients range from the world's largest payment issuers, acquirers, processors, merchants and associations to leading technology providers and investors. Services include *Banking Channels, Credit, Commercial and Enterprise Payments, Debit, Emerging Technologies, International, and Prepaid practices*, which provide research documents and advice; *CustomerMonitor Survey Series*, which report and analyze primary data collected in our biannual consumer surveys; and *Consulting Services*, which enable clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans; offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training. Mercator Advisory Group is also the publisher of the online payments and banking news and information portal PaymentsJournal.com. Visit www.mercatoradvisorygroup.com.

About Moneris

Moneris was created as a joint investment between RBC Financial Group and BMO Financial Group (including Chicago-based Harris Bank) in December 2000. As one of North America's largest providers of payment processing solutions, Moneris offers credit, debit, wireless and online payment services for merchants in virtually every industry segment and processes more than three billion transactions, annually. Moneris also offers electronic loyalty and stored-value gift card programs. With more than 350,000 merchant locations, Moneris provides the hardware, software and systems needed to improve business efficiency and manage payments. Moneris is the industry leader because we focus all of our energies on the three key elements of processing - technology, innovation and people. These strengths differentiate us in the marketplace and allow us to deliver exceptional value in transaction processing