First Data
b›yond the transaction

A First Data White Paper

EMV in the USA: Best Practices and Lessons Learned

Introduction

Industry buzz about implementing an EMV-enabled[1] payment infrastructure in the United States is becoming louder and more frequent. EMV provides the promise of reduced card payment fraud and enhanced global payments interoperability, and when combined with additional layers of security (like encryption and tokenization), it will undoubtedly benefit the entire payments value chain. As the U.S. payments industry considers the various options of chip card adoption, issuers and merchants are beginning preparations for this new era of payment acceptance.

In recent months, the major card networks (including Visa, MasterCard, Discover and American Express) have sought to provide merchants, acquirers, issuers, and ATM operators with preliminary implementation guidelines by issuing EMV roadmaps. In addition, industry groups like the Secure ID Coalition, Smart Card Alliance and Merchant Advisory Group have published their own roadmaps and recommendations. With some EMV readiness deadlines (for processors, specifically) coming as soon as April 2013, merchants, issuers, financial institutions and ATM operators should begin developing their strategies for full implementation.

With so many players involved in the process, it is no surprise that there are varying opinions and some uncertainty about what EMV will look like as it rolls out in the U.S. market. This paper seeks to clarify some of this confusion by exploring various EMV implementation options and discussing some best practices that have emerged from successful EMV rollouts that have taken place around the world in recent years.

What will EMV look like in the US?: Considerations and Options

Now is the time to decide the direction that the U.S. implementation of EMV should take. The decisions around building a new payment infrastructure must focus on what will best serve the U.S. market as a whole, as well as consider the EMV experiences and lessons learned by other countries. As the last major economy to migrate to EMV, the U.S. is in a favorable position to adopt the best practices and avoid the mistakes that other countries experienced.

Cardholder verification

Although EMV is often equated with "Chip and PIN," they are not the same thing. Chip and PIN is just one possible implementation of the EMV technology. In fact, the technical specifications for EMV-enabled cards do not require a PIN, or a signature, or any other form of cardholder identity verification. Rather, the issuing bank specifies which cardholder verification services are required for a transaction with rules it places on the chip. Regardless, it is widely accepted that the combination of *card validation via the chip*, and *cardholder authentication with a PIN* provides the greatest protection against common consumer-level attacks like fraudulent use of lost or stolen cards, counterfeit cards and skimming.

[1] EMV-enabled payment cards have an embedded microprocessor chip that encrypts transaction data uniquely every time the card is used. The technology makes it much harder for thieves to skim useable data from the card and clone it for counterfeit use. The term "EMV" is derived from the original developers of the technical standard: Europay, MasterCard and Visa. For more information see www.emvco.com.

Processors will be able to support all cardholder verification methods, but Chip and PIN may be the preferred path because it provides better security and falls in line with the standards outside the U.S.

- **PIN provides greater fraud protection** – PIN verification of the cardholder is more effective in protecting against fraud losses compared to signature verification. Based on 2008 debit card fraud data collected by the Federal Reserve Board of Governors, total fraud losses to all parties on signature based transactions per dollar volume were .13 percent, or 13 basis points. PIN-based transactions experienced a significantly lower fraud loss rate of .035 percent, or 3.5 basis points, per dollar volume. In the event that a card is lost or stolen, PIN verification is more effective in combating fraud than signature verification.[2]
- **Chip and PIN is a de facto global standard** – Most of the countries that have adopted the EMV technical standard for chip-based payment cards have also adopted PIN-based cardholder verification. This includes two of the most recent EMV rollouts: in Australia, Visa mandated that all Visa card transactions use PIN as the verification method, and in Canada, PIN was designated industry-wide as the mandatory verification method for all EMV transactions.
- **Chip and PIN is a proven solution** – Other countries that have already implemented Chip and PIN have experienced successful results. For example, the United Kingdom is one of the earliest adopters of Chip and PIN technology based on the EMV standard. Between 2005 and 2010, total card purchase volume grew 32 percent, while total card fraud decreased 17 percent. Lost and stolen card fraud is at its lowest level since the 1990s, and counterfeit card fraud is at its lowest level since 1998.[3]
- **U.S. must beware of Netherlands' Chip and PIN adoption parallels** – As countries in a particular geographic region begin implementing Chip and PIN standards, fraud rates in surrounding countries without EMV tend to experience increases in card fraud. As Europe was migrating to chip cards and PIN, the Netherlands had low card fraud rates and thus was slow to conform to its neighbors. Consequently, the fraud rate there skyrocketed from 1.5 percent in 2005 to 5 percent in 2009—an increase of over 300 percent.[4] The United States finds itself facing a similar situation now, with Canada and Mexico having recently adopted Chip and PIN. Failure to take swift EMV implementation actions will likely result in a substantial increase in card fraud.

Transaction authorization options

For a chip-based transaction, it's possible to authorize the payment using either an online or offline process. When online authorization is used, transaction information is sent to the card issuer for approval. When an offline process is used, the transaction information is transmitted from the terminal directly to the chip card itself for authorization by the chip. Transaction authorization is determined by issuer-defined risk parameters stored in the chip, rather than direct approval by the issuer. A hybrid process is also possible, whereby cardholder verification is conducted via offline PIN, and the transaction itself is authorized through online communication.

Online and offline authorization options both have advantages. Online authorization allows for an additional layer of security and fraud protection, since most fraud mitigation tools function online, in real-time. Online authorization also simplifies chip production, encryption key management and merchant infrastructure, and it saves cost and reduces overall complexity.

The primary advantage of allowing offline authorization is that it is consistent with global standards, ensuring compatibility and interoperability with international issuers' payment devices. In addition, it allows for transaction authorization functionality even in the absence of online connectivity (e.g., at a ticket kiosk or a farmer's market) as in Europe where almost 7 percent of all transactions rely on offline authorization.[5]

---

[2] Douglas King, Retail Payments Risk Forum working paper, "Chip-and-PIN: Success and Challenges in Reducing Fraud," January 2012
[3] Financial Fraud Action UK, Working Together to Prevent Fraud Euromonitor Data
[4] "Chip-and-PIN: Success and Challenges in Reducing Fraud", King, Douglas, Retail Payments Risk Forum, January 2012
[5] "As U.S. Chip Adoption Advances, Visa Provides Guidance", Ericksen, Stephanie, Perspectives on Digital Currency, January 13, 2012

Offline PIN considerations for issuers

For issuers that choose to verify cardholders using an offline PIN validation process, there are several items to consider pertaining to PIN management. The issuer must provide a process for customers to change their offline PINs (which could involve using ATMs, IVR, merchants' POS and/or in-branch services). In Europe, ATMs were updated to support cardholder PIN changes, and in Canada cardholders can also change their offline PINs at Canadian Post offices. If a card supports both online and offline PIN validation methods (as is the case for cards in most EMV countries), then separate online and offline PINs could exist. In this scenario, the issuer must either provide customer education on PIN management, or ensure that the PINs are synchronized to avoid cardholder confusion.

Card re-issuance strategies for issuers

Issuing new chip-based credit and debit cards to customers will perhaps be among the most significant expenses and logistical challenges faced by financial institutions as they migrate to EMV. As it was in Canada and Australia, the EMV rollout in the United States is likely to occur in stages. A phased implementation is more manageable and it allows for adjustments as needed along the way. As a result, issuers would be able implement a phased approach when it comes to card replacement. Rather than re-issue all cardholders' cards simultaneously, they may be able to issue chip cards as legacy cards expire, or according to some other parameters.

The deployment of trials and pilot rollout programs is an effective way to help issuers anticipate or avoid potential rollout complications. In Canada, a one-year EMV pilot in Kitchener-Waterloo (participated in by the major card networks) has been identified as one of the reasons that the nationwide rollout went as smoothly as it did. The key finding from the associated study was that a positive initial customer experience with EMV was a critical success factor for the adoption of the technology.

Some other Canadian financial institutions conducted trials with small, internal test groups of around 1,500 friends and family in order to work through education, customer support, messaging and FAQ tactics. The payments industry in Australia used a tiered rollout when implementing EMV. Issuers produced chip cards first, and once 20 percent of the market was chip enabled, the requirements for EMV-enabled POS devices were issued. This proved to be a successful strategy for solving the "chicken and egg" conundrum that had delayed EMV adoption in that region.

Instead of, or in conjunction with these types of pilots and trials, issuers may also wish to deploy a "portfolio strategy" when determining how best to conduct card replacement across their customer base. This would involve targeting specific segments of customers—for example, cardholders most likely to benefit from chip-based payments, such as international travelers who frequently use their cards outside the U.S. There are several benefits to this approach:

- Cardholders may already be familiar with EMV and therefore require less education.
- Opportunity to become "top of wallet" for card use in the U.S., leading to increased retention and incremental revenue.
- Ability to gain experience in issuance process/level of support and education needed to issue EMV cards

This strategy has been successful for the first U.S. EMV issuer, the United Nations Federal Credit Union (UNFCU)—which targeted international travelers for chip cards. One year after implementing this strategy, new account applications were up 158 percent, revolving balances were up 20 percent and purchases were up 18 percent.[6]

[6] "Smart Card Alliance Annual Conference Day One – EMV and the United States" , SCA Press Release, May 4, 2011
www.smartcardalliance.org/articles/2011/05/05/smart-card-alliance-annual-conference-day-one-%E2%80%93-emv-and-the-united-states

Chip interface selection considerations

A dual-interface chip can support both contact and contactless transactions, allowing consumers to pay the way they prefer—by tapping, waving or inserting the payment card. Contact may be preferable for high-ticket purchases, where the volume of transactions and the speed of individual transactions is not a factor. Contactless transactions may be preferable in high-volume, low-ticket situations where speed of transaction is important; for example, at a quick service restaurant. Whether contact or contactless, the same chip-based security features are present.

Many merchants are eager to benefit from newer payment options that chip-enabled payments can support. By supporting a dual-interface implementation of EMV-enabled cards and terminals, banks and merchants would gain the following benefits:

- It meets Visa's merchant requirement for the Technology Innovation Program (TIP) relief from PCI compliance reporting to Visa. To be accepted into TIP, eligible merchants are required to have at least 75 percent of transactions originate from dual interface (contact and contactless) chip terminals and be capable of processing end-to-end chip transactions.
- Similarly, MasterCard plans to offer compliance testing and fee relief based on account-data volume. A merchant running 75 percent of card transactions through an EMV terminal with both contact and contactless capabilities by 2013 would receive 50 percent relief on PCI testing. By 2015, a merchant running 95 percent of its transactions through an EMV terminal would receive 100 percent relief.
- It will likely aid in the adoption of mobile payments due to new POS equipment enabled with NFC contactless.
- It helps to maximize merchants' previous investments in POS devices by permitting the continued usage of compatible NFC terminals.
- It ensures global interoperability (compared to a contactless-only implementation, which wouldn't support many international cards)

Layered Approach to Security

As global experience demonstrates, the adoption of chip technology can reduce fraud at the POS but can also drive higher card-not-present (CNP) fraud. In tandem with bringing in EMV at the POS, the issue of CNP fraud needs to be addressed strategically with additional security layers such as fraud protection solutions and increased verification methods.

Much can be learned from the example of EMV rollout in the United Kingdom. According to the U.K. Payments Administration (formerly APACS), domestic card fraud in the U.K. dropped 32 percent in 2007 (Chip and PIN became mandatory in 2006), while counterfeit card fraud increased by 46 percent the same year. APACS claimed the increase was "due to fraudsters copying U.K. cards and using these stolen cards in countries which do not yet have Chip and PIN."[7] The situation improved somewhat by 2009, when APACS reported CNP fraud dropped by 19 percent and showed the first ever decrease since 1999. It fell yet another 15 percent in 2010.[8] APACS cites the increasing use of sophisticated fraud screening detection tools by retailers and banks as well as the industry's "Be Card Smart Online" campaign as the reason for the decrease.

The Importance of Layered Defenses

While EMV helps mitigate fraud at the POS, it does not protect cardholder data once the payment method and consumer are validated. The cardholder and the card itself have now been validated through EMV but the actual card data is sent in the clear unless the merchant has layered on an encryption and tokenization solution to protect and remove sensitive card data from the merchant environment. A layered approach to fraud and security is the only way to truly be protected. Two important layers include:

- **Card data security** – A strong encryption and tokenization solution can bolster the security of the entire payment transaction and reduce PCI compliance efforts.
- **Card fraud protection** – Layer EMV with encryption and tokenization plus online fraud and verification tools.

[7] Tracy Kitten, www.bankinfosecurity.com, "Is U.S. Ready for Chip & PIN?" June 1, 2010, www.bankinfosecurity.com/articles.php?art_id=2593&pg=2
[8] Financial Fraud Action UK, "Fraud, the Facts 2011"

Consumer Education and Customer Support

While payment associations, FIs and merchants have been reading about and discussing EMV for quite some time, this topic is new to most American consumers (only 4 percent have even heard of EMV).[9] They will need some amount of education–most likely in the form of a concerted industry marketing campaign—on why their payment cards are changing and how to use the new cards, in either a contact or contactless mode or both. Moreover, consumers are not accustomed to using a PIN with a credit transaction and would need to learn a new checkout procedure.

We can look to Canada for consumer reactions to the new cards and processes. Cardholders who were accustomed to signing credit receipts simply forgot to commit their new credit card PINs to memory. "The hardest thing for consumers and merchants when it comes to payments is changing the process at the point of sale," says Anne Koski, head of Business Credit Cards for Royal Bank of Canada. "If consumers are not used to entering a PIN for credit card transactions, it is going to take a while for them to get in the habit."[10] One potential remedy for avoiding the issue of "forgotten PINs" is allowing customers to set their own PIN rather than having a PIN assigned by the card issuer.

Another issue is that consumers sometimes forgot to take their cards with them after inserting them into a POS device for a transaction. In Canada, the impact was so significant that terminal prompts were changed to remind cardholders to remove their cards, and merchant training was revised to include reminding customers to take their cards with them.[11] Consumers also needed to be reminded by merchants to leave their cards in the card readers during the entire transaction for contact-based purchases.

None of these challenges are showstoppers that cannot be overcome with consumer education campaigns and careful planning by institutions and merchants to be sensitive to consumers' habits. Issuers should plan to use multiple touch points prior to card issuance to educate both merchants and consumers, including direct mail, websites, IVR, e-mail, videos, in-branch signage and FAQs. Financial institutions should also consider providing specialized EMV customer support for the next 3 – 5 years, as their full portfolios are converted to chip payments (the United Nations Federal Credit Union mentioned above implemented 24 x 7 customer service to assist with EMV-related questions as it began chip card rollout in the U.S.).

Merchants must plan to conduct thorough training to help employees learn to think "chip"—cards, mobile phones, contact, and contactless. Employees must also be trained on any necessary changes to the transaction handling process, as well as how to answer consumers questions about EMV. Furthermore, merchants should consider creating consumer-facing educational materials, as well as "EMV Payments Accepted Here" messaging.

A Blueprint for Implementation

Converting the entire U.S. national payments infrastructure from one system to another is a significant undertaking that may take years. At this writing, it is up to the industry stakeholders to get together and decide which approaches provide the most cost-effective path to optimal payments security. The U.S. Federal government has so far taken a hands-off approach, although at some point there could be legislation to mandate standards and timelines. In the meantime, members of the payments value chain are already formulating strategies and taking steps to prepare for an eventual migration to EMV-enabled payments. As stated previously, an April 2013 deadline looms for processors and acquirers: they must be capable of processing EMV payments by that date. Accordingly, processors like First Data are already taking the necessary steps to be EMV-ready by then. This means that the infrastructure required to facilitate EMV payments will soon be in place, regardless of any remaining uncertainty surrounding how financial institutions choose to issue chip cards or merchants choose to accept them.

---

[9] EMV Market Assessment Research Final Report, Conducted by Applied Research & Consulting LLC for First Data , November 2011 through January 2012
[10] Peter Lucas, *Canada Puts Down Chip Card Roots*, Digital Transactions, June 1, 2011, www.digitaltransactions.net/news/story/3176
[11] Ibid.

Collaboration is needed

An open, collaborative approach by all industry stakeholders will be the best way to develop a comprehensive, thoughtful and innovative standard for the "next generation" secure payment acceptance environment/infrastructure. What's more, timelines must be realistic for all stakeholders including issuers, acquirers, hardware manufacturers and merchants.

Sharing the costs

The costs of conversion are considerable, and will be borne by merchants and financial institutions. As in prior EMV rollouts in other countries, most recently Canada, if the card networks were to help share the cost of the technological transition, it could drive much faster adoption in the United States. The U.K. and Australian markets also were given interchange concessions by the card networks, which helped share the costs of purchasing and deploying new hardware and software that will benefit many stakeholders.

Conclusion

Because of EMV's proven ability to dramatically reduce card payment fraud, there is a steady drumbeat pushing the U.S. electronic payments industry toward implementation. Now is the time for all major stakeholder organizations to take a seat at the table to collaborate on what form the new payments infrastructure should take. There are many options to consider and decisions to be made, but from lessons learned around the world it appears that EMV in the United States will confer the greatest fraud reduction and usability benefits if it is based on Chip and PIN with online authorization, with dual-interface chips and terminals that support both contact and contactless transactions to help support the consumer push towards mobile payments. This combination would seem to serve the greatest need and provide the most security value. In addition, stakeholders must plan for ways to educate consumers to minimize their confusion and problems with adopting the new payment procedures.