WHITE PAPER

U.S. POISED TO JOIN WORLDWIDE EMV MOVEMENT

Driven by a combination of the high costs of PCI compliance and the convergence of many forces driving adoption of NFC mobile payments, U.S. acquirers and merchants may be poised to begin migration to the EMV secure payments infrastructure.

VeriFone®
THE WAY TO PAY™

EXECUTIVE SUMMARY

The U.S. payments industry has relied on magnetic stripe-based card technology for decades, but most other countries have or are in the process of transitioning to the EMV chip card standard. EMV ensures a card is authentic by utilizing encrypted data stored on the card (although it does not encrypt the actual transaction). Now, mandates and incentives are laying the path for U.S. adoption of EMV -- in part to drive adoption of NFC mobile payments -- and early implementers will gain an advantage over competitors with solutions that are available now. But merchant migration may be easier, less costly and provide more benefits than many realize, especially when used with end-to-end encryption.

CONTENT

THE WINDS OF CHANGE

Until recently, discussions about EMV adoption in the U.S. have been in the abstract -- with few proponents, and a healthy dose of skepticism that the U.S. payments industry could ever be motivated to transition from magnetic stripe-based payment cards.

EMV - an acronym of Europay International, MasterCard and Visa, which in 1994 joined to initiate the specification - has been or is in the process of being adopted by every developed country (including Canada) other than the U.S., as well as most emerging countries. Both American Express and JCB subsequently joined with MasterCard and Visa in ownership and management of EMVCo, an entity to manage and extend the specifications, while Europay was absorbed by MasterCard.

The U.S. has resisted moving to EMV because despite some proponents such as WalMart, the payments ecosystem comprised by card brands, processors, acquirers and merchants has largely been content with the magnetic stripe-based infrastructure. But in August 2011, Visa announced a Technology Innovation Program (TIP) and liability shift for the U.S. that sets out an EMV migration plan that includes incentives for adoption, and potential penalties for those who don't go along. Early in 2012, MasterCard announced a roadmap for EMV adoption with its own set of incentives and liability shift. Subsequently, Discover announced a 2013 EMV mandate for acquirers and direct-connect merchants and also disclosed that it had already accepted EMV in the U.S. at certain WalMart locations. American Express followed the other major brands with its own timeline, with an early 2013 mandate for processors and financial incentives for merchants beginning in the second half of that year.

Visa's announcement of TIP overtly tied the U.S. migration effort to EMV for both contact-based and contactless payment acceptance. "The adoption of dual-interface chip technology will help prepare the U.S. payment infrastructure for the arrival of Near Field Communication (NFC) - based mobile payments by building the necessary infrastructure to accept and process chip transactions," according to Visa.

The major incentive from a merchant perspective is that Visa will "eliminate the requirement that eligible merchants annually validate their compliance with PCI DSS if at least 75 percent of their Visa transactions originate from "dual-interface EMV chip-enabled terminals" and if they comply with other qualification criteria. Visa will require U.S. acquirer processors and sub-processor

service providers to be able to support merchant acceptance of chip transactions no later than April 1, 2013. A MasterCard executive told PaymentsSource that a merchant running 75% of card transactions through an EMV terminal with both contact and contactless capabilities by 2013 would receive 50% relief on PCI testing. American Express indicated merchants " will be eligible to receive relief" from PCI Data Security Standard (DSS) reporting requirements if POS locations where 75% of transaction occur "are enabled to process American Express EMV chip-based contact and contactless transactions."

Because the card brands are implementing a liability shift to acquirers and away from issuers, if merchants don't move to these new EMV acceptance devices, they eventually will become liable for fraudulent card transactions that would have been prevented if they were processed over EMV terminals. Currently, card issuers largely absorb liability for fraudulent card transactions.

CHIP & PIN (OR SIGNATURE)

Visa and MasterCard pronouncements on their EMV roadmaps have stirred some confusion over Chip & PIN and Chip & Signature. There's a common misperception that EMV is synonymous with "Chip and PIN" but that is not accurate. Chip and PIN is just one flavor of EMV that has been widely adopted and was implemented in the UK under that name in the past decade. But other countries have opted for a "Chip and Signature" approach.

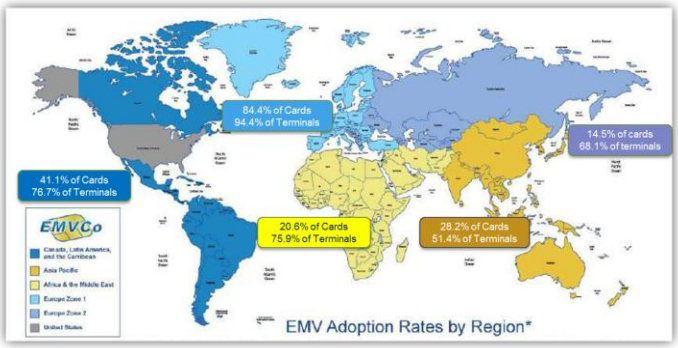
Visa has indicated that EMV in the U.S. doesn't have to mean Chip & PIN and that has been interpreted as favoring Chip & Signature. What Visa actually said was, they "will continue to support a range of cardholder verification methods (CVMs) with EMV chip, including signature, online PIN and no-signature for low-value, low-risk transactions." Therefore, they'll accept Chip & PIN and other variations.

MasterCard, which also supports different flavors of EMV, has talked about a liability hierarchy, which essentially means that liability for EMV fraud is going to rest on the shoulders of whichever party in the processing chain has the weakest implementation of EMV. The Merchant Advisory Group, which includes Walmart, Target, Sears, CVS Caremark and many others, has strongly endorsed Chip & PIN as a requirement for U.S. EMV adoption. Clearly PIN is more secure than signature, so it makes sense to default to this option as the best shield against fraud liability.

WHY EMV?

Adoption of EMV cards now stands at more than 40% around the world, excluding the U.S., and EMV acceptance device adoption is at more than 70%, according to EMVCo. The U.S. is essentially alone in resisting migration to this standard.

EMV was initiated to provide a worldwide standard for interaction between integrated microprocessor (chip-based) “smart cards” and approved payment devices and ATMs. This standard encompasses credit, debit and contactless payment transactions.



These chip-based cards can support a range of applications, but the primary usage common around the world is to perform payment transactions that store encryption data for authentication. As part of the transaction authorization, the card uses the data to prove it is authentic. Encrypted data on chip cards has been used for more than ten years to prevent cloning of payment cards. If it is combined with PIN, consumer authentication and the prevention of non-repudiation are achieved.

For general payment applications, an EMV terminal reads data stored on the chip card for offline transactions and authenticates that it is legitimate, thus preventing use of stolen or cloned cards. Strong cryptographic functions are used to authenticate the card and cardholder to ensure validity and authenticity.

Magnetic stripe cards, on the other hand, do not have the same kind of data storage and have no microprocessor; therefore, magnetic stripe cards cannot contain the same security features as chip cards because there is no dynamic data element and cards are easy to clone. With magnetic stripe cards, the cardholder’s data is encoded on the magnetic stripe on the back of the card, similar to a tape recorder. When the card is swiped, all of the cardholder data, such as the account number, name, and expiration date, is sent in one direction from the payment terminal to the authorization network, which checks the information, authorizes the charge and provides a payment guarantee to the merchant.

U.S. RESISTANCE

Efforts to promote chip cards for payment in the U.S. have largely fallen flat up to this point. Issuers were reluctant to replace mag-stripe cards with more expensive chip cards; merchants essentially refused to invest in new terminals that could read the cards. And consumers never were provided with a compelling case on why they should even care.

A key element in the U.S. resistance is the fact that mag-stripe has worked very well. Unlike much of the rest of the world, online card authentication is common and relatively inexpensive in the U.S. and the cost of fraud has been relatively stable and built into the price for managing online transactions.

As interest faded in the U.S. for chip cards, the payments industry focused on contactless as the next transformation of transactions. Chip-based cards can be used with radio technology to enable contactless payments. But here again, merchants perceived no incentive to invest in contactless payment devices, card issuers declined to do a wholesale conversion from mag-stripe to contactless, and consumers for the most part had no idea why they should be concerned about the ability to complete a transaction with a savings of microseconds.

NFC FORCING MOBILE TRANSFORMATION

A compelling case for EMV can be made at just about any point in the payments value chain. But for the most part, given that mag-stripe works well, risk is relatively well managed and consumers are happy with the status quo, there has been reluctance all around on bearing the cost of migration.

Rapid consumer adoption of mobile phones and smart phones is the impetus for new forms of communication, social media, and is widely expected to lead to quick adoption of mobile payment capabilities.

Mobile technology, and more specifically NFC (Near Field Communications), is dramatically tilting the playing field and easing retailer resistance to investing in innovation at the point of sale.

Rather than seeing NFC as just another payment acceptance technology, retailers view this as a technology providing a converged solution for integrating payment with applications that increase traffic and sales.

Emerging online services such as digital couponing, loyalty, location-based social media, and value-added applications will drive customers into stores. But those shoppers will expect merchants to integrate these new services with their payments in one transaction.

NFC, a radio-based interaction protocol compatible with existing contactless payment standards, is increasingly being incorporated into mobile smartphones to bridge the previously disparate worlds of the Internet and the bricks & mortar retail environment.

With NFC-enabled phones, consumers will be able to get information instantly and pay for products or services from their mobile phone-based electronic wallets with just a tap or wave at any NFC-enabled payment device. In addition, because NFC supports two-way communication, merchants can entice consumers with digital coupons, promotional messages sent directly to their smart phones or interactive loyalty solutions.

NFC uses the same radio transmission frequency (13.56 MHz) as contactless chip cards. But NFC is a more interactive, multi-use technology that makes it possible to integrate contactless payment with intelligence embodied in a smartphone or other device.

NFC chips embedded in mobile phones allow the phone to operate as either a card or a reader. So, while an NFC–enabled phone can simply emulate an existing contactless card, it can also read tags embedded in other devices, such as an NFC poster or kiosk, and to engage in two-way communications with another NFC chip-enabled device. Because it can operate in a passive mode, the NFC-equipped phone is able to conserve battery power; but the user can easily access applications to turn the phone into NFC active mode. For more on NFC, see http://www.verifone.com/nfc

Interest in NFC soared in 2011 as Google introduced Google Wallet and three wireless service providers -- AT&T, Verizon Wireless, and T-Mobile -- formed a joint venture called Isis with a similar concept that has since won support from MasterCard, Visa, American Express, and Discover.

RULES ARE CHANGING

NFC may be the key driver in making EMV viable in the U.S. However, there are many business factors that are converging to make EMV more relevant to the U.S. payments industry.

First off, while the relative cost of card fraud has been relatively consistent and has been built into the fees structure for card acceptance, it still represents a huge sum of money and issuers are eager to transfer liability for those costs to the merchant.

It is difficult to precisely catalog the losses from card fraud in the U.S., but according to a report by a senior economist with the Federal Reserve Bank of Kansas City, it amounts to more than $3 billion annually, spread among card issuers ($2 billion), point-of-sale merchants ($837 million), and mail order, telephone and Internet merchants ($900 million).

Furthermore, organized crime efforts to exploit payment cards has resulted in increasingly sophisticated efforts that have resulted in large heists such as a crime ring that in 2008 was charged with stealing 45 million credit and debit cards from a number of national retailers, and in January 2009 an assault on Heartland Payment Systems that compromised an estimated 130 million card accounts. More recently, New York City law enforcement officials charged “members of five organized forged credit card and identity theft rings based in Queens County and having ties to Europe, Asia, Africa and the Middle East” with stealing personal credit information of thousands of unwitting American and European consumers “and costing these individuals, financial institutions and retail businesses more than $13 million in losses over a 16-month period.”

Rather than adopt EMV, the U.S. payments industry was driven by the card brands to adopt Payment Card Industry (PCI) standards issued by the PCI Security Standards Council. While undoubtedly increasing the security of card payments overall, PCI standards are expensive for merchants, who must audit their internal systems to ensure compliance, and vendors who provide hardware, software and services and who have had to implement new requirements into their products and services.

But the biggest merchant complaint about PCI is that compliance certification only reflects a moment in time, and subsequent changes to their systems can unknowingly create potential breach points that can leave them liable for resulting damages.

Visa's TIP program seems aimed at leveraging those complaints to fuel a faster migration to EMV than anyone would have imagined. Announced in August 2011, the program was actually introduced earlier in the year for all regions other than the U.S.

The incentive of forgoing annual PCI DSS validation is a tremendous opportunity for merchants to invest in new payment devices that accept EMV transactions that accommodate both chip cards and NFC. Visa and MasterCard are advising that acquirers enable their systems to support EMV payments.

The fraud liability shift represents a huge potential penalty to merchants that don't make the investments: As NFC Times reported after Visa's August 2011 announcement, "Perhaps the biggest incentive Visa is offering to merchants to move to chip begins in October 2015 with a liability shift that would saddle merchants with losses for fraudulent transactions that could have been prevented if the merchants had installed chip terminals. Gasoline retailers have two additional years to comply. At present, card issuers bear the cost of most fraudulent transactions, noted Visa." Both MasterCard and Discover have indicated they will also adopt a 2015 deadline for general adherence, with MasterCard, Visa and American Express also confirming an additional two years for gasoline retailers.

Aside from security, there are other compelling reasons to move to EMV. With the rest of the world moving to EMV, it will become increasingly difficult for mag-stripe cardholders to pay for transactions overseas and some large U.S. issuers have announced limited EMV card issuance for U.S. travelers abroad. Similarly, once overseas issuers do away with the mag-stripe completely, as the European Payments Council has already recommended, U.S. retailers may find themselves unable to accept card payments from foreign visitors.

IMPLEMENTATION ISSUES AND SOLUTIONS

EMV migration in the U.S. does not have to be costly and difficult. EMV card-acceptance devices are readily available -- as a global supplier, VeriFone, for example, has been selling in overseas markets EMV-capable versions of the payment devices it provides in the U.S. Additionally, dual interface PIN pads will enable retailers to adapt older non-EMV systems to the new payment requirements.

For large retailers, the return on investment will be obvious. Many are already eager to adopt NFC in order to take advantage of the broader range of benefits, but simply need more hard evidence for the business case, which the card brands' financial incentives will likely provide. As Visa notes, "Merchants qualifying for TIP can reap meaningful savings through the reduction of costs associated with annual PCI DSS validation, and will have the opportunity to re-invest those savings into additional payment technology infrastructure to support dynamic data processing." With MasterCard, merchants in 2015 could achieve 100 percent fee relief for compliance testing.

For smaller merchants, it may be more difficult at first to make that business case because most are not currently required to conduct annual audits. However, acquirers do have the ability to require such audits even with Level 4 merchants, and as those acquirers invest in the EMV infrastructure, it's hard to imagine they won't require their smaller merchants to go along for the ride. In addition, in 2017 those merchants who don't have EMV will be saddled with the liability shift, with the likelihood that a fraudulent transaction event could threaten their existence.

For small and medium sized businesses (SMB), the best option may be for a bundled, turnkey service that integrates hardware, software, end-to-end encryption and value added services. VeriFone's PAYMEDIA encompasses payment acceptance systems, intelligent gateway services, and managed services that include VeriShield Total Protect and automated software updates. Rather than paying upfront for new hardware, a monthly subscription-based pricing model eliminates upfront hardware costs and ensures compatibility with new requirements and services as they become available.

EMV AND END-TO-END SECURITY

While EMV limits the exposure of merchant payment transactions to fraud and misuse, it does not protect cardholder information that under EMV is still transmitted in the clear during the transaction. EMV can be viewed as part of an overall security portfolio for protecting all aspect of card transactions.

VeriFone's VeriShield Total Protect, Secured by RSA – the only solution of its kind – applies sophisticated encryption and tokenization to secure cardholder information, from insertion to processing and back.

VERIFONE – YOUR EMV EXPERT FOR A NEW ERA

EMV is a global standard and VeriFone has global experience in developing EMV payment system solutions and peripherals that have achieved EMV Level 1 and Level 2 Type Approval. The complexity of migrating to EMV chip card standards can pose significant challenges for acquirers and merchants. Since the inception of EMV, VeriFone has provided internationally an unmatched line of EMV-compliant hardware and software – as well as training and support – to deliver complete solutions for meeting Visa's migration plan.

We're also working closely with our partners to ensure that all payment applications designed to run on these devices will be EMV-compliant. VeriCentre Estate Management solution can be utilized to centrally manage your device base to handle simultaneous downloads efficiently and at the least disruptive times.

VeriFone's EMV solutions:

- Accept a broad range of EMV card functionality including Dynamic Data Authentication (DDA) functionality and enciphered PIN
- Feature application separation to support multiple applications running securely on the terminal
- Support VeriShield file authentication to help prevent intrusion into the system's applications
- Offer 32-bit processing power to handle the performance demands related to EMV compliance across borders, and across hosts

VeriFone supports the global EMV movement. Our experience and expertise with EMV will help guide you through these upcoming changes from start to finish and as mandates change over time.

For more information contact your VeriFone or reseller representatives. Visit www.verifone.com/emv-us.

[i] David Huen, PaymentsSource, "MasterCard EMV Liability Standard Leans Toward Chip-And-PIN," January 31, 2012. http://www.paymentssource.com/news/MasterCard-EMV-Liability-Standard-Leans-Toward-Chip-And-PIN-3009389-1.html

[ii] Visa Technical Bulletin, "Visa Expands Technology Innovation Program for U.S. Merchants to Adopt Dual Interface Terminals," August 9, 2011, http://usa.visa.com/download/merchants/bulletin-tip-us-merchants-080911.pdf

[iii] EMVCo, "Worldwide EMV Deployment"http://www.emvco.com/about_emvco.aspx?id=202

[iv] Richard J. Sullivan, Federal Reserve Bank of Kansas City. "The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy." May 21, 2010.

[v] PYMNTS.com, "International Identity Theft and Counterfeit Credit Card Operation Based in Queens." October 7, 2011.

[vi] Dan Balaban, NFCTimes.com. "Visa's U.S. Migration Plan for EMV Supports Contactless and NFC," August 9, 2011. http://www.nfctimes.com/news/visa-s-us-migration-plan-emv-supports-contactless-and-nfc

[vii] "Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?" February 2011. http://www.smartcardalliance.org/resources/pdf/Payments_Roadmap_in_the_US_020111.pdf