First Data
b›yond the transaction

A First Data White Paper

EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions

For almost two decades, interest in a chip-based payment standard such as EMV barely reached a simmer in the United States. Recently some of the card brands signaled their intentions to support EMV-enabled payments in the U.S. and now the country's collective interest is heating up. Merchants, financial institutions, and every other organization with a stake in the electronic payments process want to understand the impacts of such a standard. In the absence of a government mandate and strict guidelines on how to adopt the smart chip standard, our industry has the opportunity to formulate our own plans and timeframes, albeit with a global backdrop. Clearly there is a need to reduce card fraud and increase security in the U.S. market. Now is the time for thoughtful consideration of the issues and meaningful discussion among all stakeholders to ensure we develop a chip-based infrastructure that works for all. This paper puts the issue of EMV in the United States into perspective for merchants and FIs.

By:
Dom Morea, SVP and Division Manager, Advanced Solutions and Innovation

Contributors:
Philip Christiansen, VP, Credit Services, Global Product Management, First Data
Bruce Dragt, SVP and Division Manager, Payment Acceptance, First Data
G. Russell Randolph, VP, Network, Debit and ATM Solutions, Global Product Management, First Data

© 2011 First Data Corporation. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.

Introduction

For almost two decades, interest in EMV[1] barely reached a simmer in the United States. Recently several card associations stirred the pot and now interest in the smart chip standard is heating up among almost every player in the electronic payments value chain. Financial institutions,[2] merchants, acquirers/processors, card brands, and hardware and software vendors all want to understand the current state of EMV in the U.S. Is it finally time to take a seat at the implementation table, a table at which much of the world has been sitting for several years?

The term "EMV" refers to a specification for the technical requirements of chip-enabled payment devices, generally credit and debit payment cards with embedded microchips, and how the cards interact with point-of-sale and ATM infrastructures. There are many "flavors" of a chip-based payment standard, including using chip + PIN only or chip + choice (the option of using either PIN or signature) as cardholder verification tools; the majority of EMV implementations globally have focused on chip + PIN enablement. Whatever the format, smart chips are the basis of the technical standard behind more than 1.24 billion payment cards and 15.4 million POS terminals,[3] with almost all of those cards and acceptance devices residing outside the United States. Europe, Canada, Latin America and Asia/Pacific are all in various stages of EMV chip migration and usage, leaving the U.S. region—the largest user of payment cards in the world—as the last major hold-out for implementing the otherwise global standard.

Payment industry experts generally agree that a chip-based standard will come to the U.S., but the predictions of when and in what form vary dramatically. While pundits have been saying the U.S. is far from ready for it, there is a distinct possibility that the change may come sooner rather than later.

Visa's recently-announced roadmap for an accelerated migration to EMV is a prod (more information about the plan is included later in this paper), but it's not the guiding impetus bringing about the current evaluation in the U.S. Oddly enough, the major factor that could push our industry toward EMV is recent legislation that had little to do with smart cards. In the wake of the Durbin Amendment and banks' dramatic loss of interchange revenue, every dollar lost to fraud now looms large. Aite Group reports that card fraud in the U.S. already costs the card payment industry (primarily issuers) $8.6 billion[4,5] a year and industry experts are concerned losses will rise as fraud migrates to the U.S. from smart card-enabled countries. Perhaps now more than ever, banks have good reason to evaluate the extent to which embedded smart chips can reduce their losses from card fraud.

---

[1]The original founders of the EMV standards body were Europay, MasterCard and Visa, from which the acronym "EMV" was derived. See www.emvco.com for details about the specification.

[2]References to "financial institutions" and "banks" in this paper are intended to include credit unions.

[3]EMVCo, LLC

[4]Aite Group report, "Card Fraud in the United States: The Case for Encryption," January 2010

[5]All currency amounts are in U.S. dollars in this paper unless otherwise noted.

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 2

On the merchant side of the house, Richard Mader, the executive director of the National Retail Federation's Association for Retail Technology Standards, says merchants have been waiting for clearer directions from issuers and processors before making the investment in chip card infrastructure. It is expected that many industry players will put forward guidelines or even directives around the payment standard, likely resulting in a sea of not-so-standard approaches that must be reconciled.

Visa and MasterCard have signaled some of their intentions, though none of the card associations have come out with full guidelines. However, Visa has announced a plan that includes a liability shift to acquirers. Once a sufficient number of financial institutions begin issuing smart cards en masse, merchants need to decide whether to process the cards using EMV technology or to accept financial liability for fraud losses that they will ultimately be responsible for.

The decision to migrate the U.S. payments industry to a chip-based payment standard will not be a simple one, and implementation will be complex. There are many stakeholders, large and small, who are intricately bound together in the payments ecosystem. A change in one area, such as at the ATM or the POS, can't be effective unless the entire ecosystem gets behind the migration. The purpose of this paper is to put the EMV issue in perspective for U.S. merchants and financial institutions that may now be feeling the pressure to act.

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 3

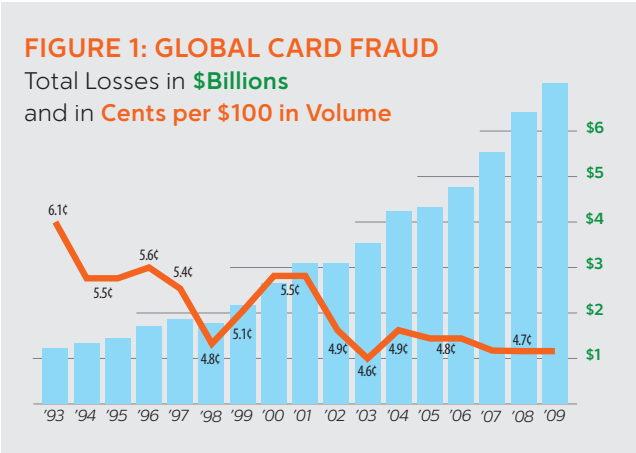
An Overview of EMV

EMV is the technical standard that ensures chip-based payment cards and terminals are compatible around the world. The term refers to Europay, MasterCard and Visa, the three companies that originally developed the specifications in 1994. Today the EMV standard is managed by EMVCo, LLC, which is equally owned by American Express, JCB, MasterCard and Visa. Detailed information about EMV and the technical specifications are available on www.emvco.com.

A chip-based payment transaction occurs when a microprocessor, generally embedded in a plastic card or a personal device such as a mobile phone, connects to an EMV-enabled POS (contact or contactless). The smart chip securely stores information about the payments application and performs cryptographic processing. This provides an additional form of card authentication, validating the legitimacy of the payment type being used.

Why now?

Losses from card-related fraud are increasing and the smart chip enables more robust cardholder verification to protect against consumer-level fraud, such as counterfeiting or lost/stolen cards, for EMV transactions. On a global scale, the absolute losses from card fraud are steadily increasing, even though the ongoing battle against fraud is driving the rates downward.[6] (See Figure 1.) As regions such as Europe, Canada and Asia/Pacific continue to mark positive results in the battle against card fraud, the pressure on the U.S. to migrate to the chip-based standard becomes stronger. Aite Group says that card fraud costs the U.S. card payments industry an estimated $8.6 billion per year.[7] According to The Nilson Report, the figure is expected to reach $10 billion by 2015.[8] And experts predict U.S. card-not-present (CNP) fraud will rise dramatically as neighboring regions complete their EMV deployments.



Source: The Nilson Report, #951, June 2010

Reduced revenues in the wake of the Durbin Amendment[9] *are forcing financial institutions to re-examine their fraud losses.* Banks impacted by these recent legislative changes are expected to lose, on average, 45 percent of their debit interchange revenue as a result of the Durbin regulation.[10] Revenue losses of this magnitude force a renewed focus on fraud losses which many financial institutions had previously considered manageable. As Aite Group analyst Julie Conroy McNelly puts it, "The revenue off the cards no longer can absorb the fraud hit."

---

[6]The Nilson Report, #951, June 2010

[7]Aite Group report, "Card Fraud in the United States: The Case for Encryption," January 2010

[8]The Nilson Report, #951, June 2010

[9]The Durbin Amendment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 regulates the interchange fees that financial institutions can charge for the use of their payment cards.

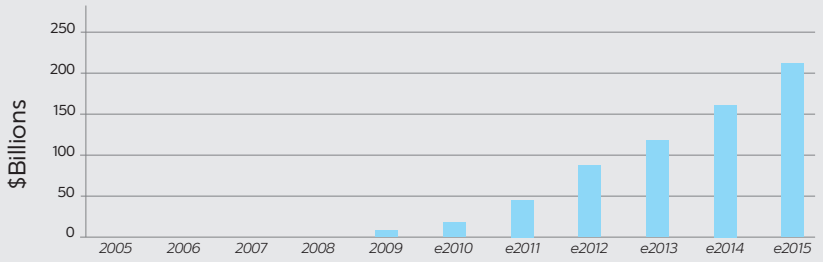
[10]"Debit Interchange Regulation: Another Battle or the End of the War?", Simpson Thacher & Bartlett LLP, July 23, 2011

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 4

Interest in mobile payments is growing. Aite Group forecasts that U.S. mobile payments will reach $214 billion in gross dollar volume in 2015, up from $16 billion in 2010—a 68 percent compound annual growth rate between 2010 and 2015.[11] (See Figure 2.) The ability to have secure, convenient mobile payments based on a standard infrastructure such as EMV is critical to acceptance of mobile payments, as is the widespread ability for consumers to make contactless payments. Many POS equipment manufacturers are building both contact and contactless as well as mobile capabilities into their EMV-enabled devices; therefore the upgrade to this equipment gives customers a choice and provides a catalyst for driving mobile adoption even faster.

FIGURE 2: U.S. MOBILE PAYMENTS GROSS DOLLAR VOLUME ESTIMATED THROUGH 2015



Source: Aite Group, Nov. 2010

Cardholders traveling from a non-EMV-enabled country to an EMV-enabled country are finding it increasingly difficult to use their cards. Merchants that accept smart cards may refuse to accept magstripe-only payment cards, which are used in the U.S., for a variety of reasons including real or perceived technical incompatibilities. Aite Group reports that cardholders who experienced a difficulty using their card abroad are very likely to alter their behavior after the trip to use that "problem card" less. Although this customer segment is relatively small, U.S. payment card issuers missed out on nearly $4 billion in 2008 charge volume and approximately $78.8 million in interchange fees because of problems cardholders had with their cards while traveling abroad.[12]

The situation will get much worse if regions outside the U.S. discontinue the practice of accepting magstripe cards, as could be the case in Europe soon. Due to the success of the chip-based standard in Europe, the European Payments Council (EPC) announced in 2009 that it would consider a ban on magnetic stripe cards within the next couple of years.[13]

Magnetic stripe technology is beginning to reach its end of life. The magstripe technology in current use on payment cards is more than four decades old and is inherently insecure. It's far too easy for thieves to produce counterfeit cards using cardholder data stolen in scores of data breaches or skimmed from individual cards. Consequently, the U.S. payments industry continues to invest heavily in supplemental security methods to compensate for the weakness of magstripe security. But even if the U.S. market migrates to EMV, magstripe cards will not go away overnight. Banks will need to issue cards that are both chip-enabled and magstripe—at least for a while in order to provide the consumer with acceptance ubiquity in the U.S. and elsewhere.

---

[11]Gwenn Bezard, "U.S. Mobile Payments: The Time Has Come," Aite Group, November 2010

[12]Aite Group

[13]Beverly Blair Harzog, "U.S. magnetic stripe credit cards on brink of extinction?", August 4, 2009, www.creditcards.com

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 5

Global EMV Usage

EMV is employed today in more than sixty countries and every major economic region of the world except the United States. According to EMVCo, 40 percent of total cards and 70 percent of total terminals deployed outside the U.S. are based on the EMV standard.[14] What's more, Visa reports that EMV chip implementation is accelerating globally, with 62 percent of cross-border transactions conducted via a chip card at a chip terminal.[15] The chart in Figure 3 provides an overview of the global adoption by major regions. U.S. data is not included despite there being some cards and some terminals in this market; transactions in the U.S. are not processed as EMV-compliant transactions today.

FIGURE 3: WORLDWIDE EMV DEPLOYMENT AND ADOPTION AS OF Q1 2011

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America and the Caribbean	207,715,356	31.2%	3,900,00	76.5%
Asia Pacific	336,602,681	27.9%	3,480,000	43.0%
Africa and the Middle East	233,003,747	17.6%	345,000	60.7%
Europe Zone 1 (SEPA countries)	645,472,323	73.9%	10,5000,000	89.0%
Europe Zone 2	27,516,286	12.7%	513,600	65.4%
United States	Not reported	Not reported	Not reported	Not reported
Totals	**1,240,310,393**	**40.1%**	**18,738,600**	**71.1%**

Note: Figures reported in Q1 2011 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally. Figures do not include data from the United States.

Source: EMVCo, LLC

Europe in particular has embraced EMV chip + PIN cards (the use of chip cards and PINs for cardholder verification), largely due to a mandate from the European Payments Council (EPC) as part of the full implementation of the Single Euro Payments Area, SEPA. The EPC has been driving a single rulebook so more than 8,000 banks throughout Europe can process credit and debit payments in a standard fashion.

Adoption of the EMV standard in Asia/Pacific has been relatively swift. Government mandates, fraud prevention initiatives and industry competition are driving adoption in Japan, Malaysia, Korea, Indonesia, Taiwan, Australia and many other countries. Even global events shape the market. China's central bank and China UnionPay, the country's domestic card brand, pushed for EMV adoption in the major Chinese cities in order to prepare for the influx of international tourists attending the 2008 Beijing Olympics and the 2010 Shanghai World Expo.

[14]EMVCo, LLC. Figures reported in Q1 2011 represent the latest statistics from American Express, LCB, MasterCard and Visa, as reported by their member financial institutions globally. Figures do not include data from the United States, although some cards and terminals are deployed there.

[15]Visa Bulletin, "Visa Announces U.S. Participation in Global Point-of-Sale Counterfeit Liability Shift," August 9, 2011

 ©2011 First Data Corporation. All rights reserved.

In the Middle East, the United Arab Emirates central bank is encouraging financial institutions to move to EMV. In Africa, South Africa has seen swift adoption, with more than a million MasterCard-branded EMV cards issued by the end of 2008, and more than one-fourth of all POS devices upgraded to accept EMV cards.[16] In the Americas (not including the U.S.), Canada, Brazil and Mexico are far along in their deployments. Canada's payment association, Interac®, has set deadlines for the industry: all ATMs in the country must be EMV chip + PIN compliant by the end of 2012, and merchant terminals must be compliant by the end of 2015.

In the realm of major financial markets, the U.S. stands alone in its hesitancy to adopt a smart chip payment standard. As we'll explore in more detail below, there are many reasons to reconsider this hold-out position.

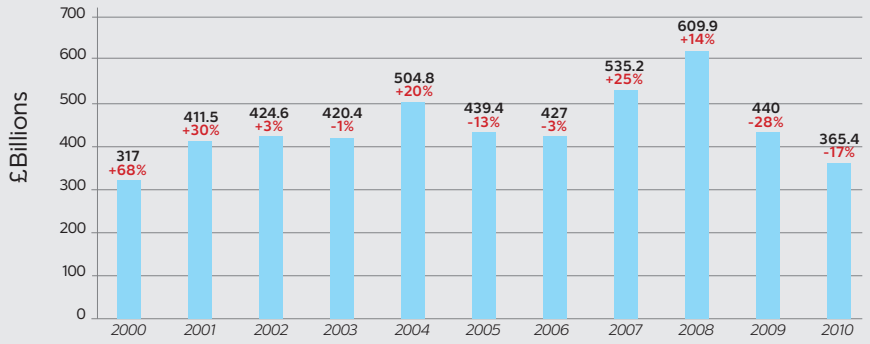
Positive results in an early-adopter country

As one of the earliest adopters of chip + PIN cards, the U.K. has been a sort of pilot program for other countries which are observing the results.

The U.K.'s overall reduction in fraud losses is impressive, no matter what angle the data is looked at. Payment card fraud losses in the U.K. dropped from 18 basis points to 12 basis points between 2001 and 2008 according to First Data. (The U.K. adopted EMV in 2001.) Success continued as total fraud losses on U.K. cards fell by 17 percent between 2009 and 2010 to £365.4 million. (See Figure 4.) This is the lowest annual total since 2000 and was preceded by a fall of 28 percent in 2008. In the past two years, card fraud losses against total turnover—at 0.074 percent—continue to decrease and have now fallen by 40 percent.[17] Those numbers are even more extraordinary when considered along with the fact that card usage and transaction volumes continue to grow even as these fraud rates fall.

FIGURE 4: FRAUD LOSSES ON U.K.-ISSUED CARDS, 2000-2010

Red numbers indicate percentage change on previous year's total



Source: Financial Fraud Action U.K.

However, the U.K. Payments Administration (formerly APACS) says the U.S. reluctance to adopt EMV is impacting the U.K. market. While overall domestic card fraud in the U.K. dropped 32 percent in 2007, counterfeit card fraud increased by 46 percent the same year. APACS claimed this was "due to fraudsters copying U.K. cards and using these stolen cards in countries which do not yet have chip + PIN."[18] (The situation improved somewhat by 2009, when CNP fraud dropped by 19 percent and showed the first ever decrease since 1999. It fell yet another 15 percent in 2010.[19] APACS cites the increasing use of sophisticated fraud screening detection tools by retailers and banks as the reason for the decrease.)

---

[16]Banking & Payments Asia, "EMV: The Story So Far," May 2009

[17]Financial Fraud Action U.K, "Fraud, the Facts 2011"

[18]Tracy Kitten, www.bankinfosecurity.com, "Is U.S. Ready for Chip & PIN?" Jun 1, 2010, http://www.bankinfosecurity.com/articles.php?art_id=2593&pg=2

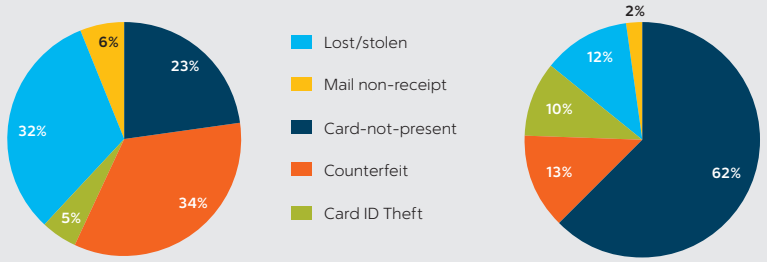
[19]Financial Fraud Action U.K, "Fraud, the Facts 2011"

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 7

The chart in Figure 5 shows U.K. card fraud losses by type, shown as a percentage of the total losses, in the years 2000 and 2010. The data clearly shows that lost/stolen or counterfeit cards accounted for a much smaller percentage of overall fraud at the end of the decade while CNP fraud became the source of almost two-thirds of all fraud losses.

FIGURE 5: U.K. CARD FRAUD LOSSES SPLIT BY TYPE (AS PERCENTAGE OF TOTAL LOSSES)



The chart in Figure 6 provides a breakdown of each type of card fraud over the decade in which chip + PIN was adopted in the U.K. The types of fraud EMV best addresses—counterfeit, lost/stolen, and mail non-receipt—all showed marked decreases over the decade.

FIGURE 6: ANNUAL FRAUD LOSSES ON U.K.-ISSUED CARDS IN £MILLIONS, 1999-2009

Fraud Type	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	% change '09/'10
Card-not-present	72.9	95.7	110.1	122.1	150.8	183.2	212.7	290.5	328.4	266.4	226.9	-15%
Counterfeit	107.1	160.4	148.5	110.6	129.7	96.8	98.6	144.3	169.8	80.9	47.6	-41%
Lost/stolen	101.9	114.0	108.3	112.4	114.4	89.0	68.5	56.2	54.1	47.7	44.4	-7%
Card ID theft	17.4	14.6	20.6	30.2	36.9	30.5	31.9	34.1	47.4	38.2	38.1	0%
Mail non-receipt	17.7	26.8	37.1	45.1	72.9	40.0	15.4	10.2	10.2	6.9	8.4	22%
TOTAL	317.0	411.5	424.6	420.4	504.8	439.4	427.0	535.2	609.9	440.0	365.4	-17%
Contained within this total/breakdown by location												
U.K.	213.4	273.0	294.4	316.3	412.3	356.6	309.9	327.6	379.7	317.4	271.5	-14%
Fraud abroad	103.5	138.4	130.2	104.1	92.5	82.8	117.1	207.6	230.1	122.6	93.9	-23%

Source: Financial Fraud Action U.K.

 ©2011 First Data Corporation. All rights reserved.

Visa's Plans to Accelerate Chip Migration and Adoption of Mobile Payments

At this writing, the Federal Reserve Board has not come forth with a policy recommendation for smart cards, preferring instead to let the payments industry decide what to do. In that context, Visa has taken a first step with an announcement outlining the organization's roadmap for what it calls dynamic authentication. The outline includes a proposal on a timeframe for industry conversion; the format for the technology (dual-interface chip technology incorporating both contact and contactless); and a carrot-and-stick method to garner industry acceptance.

Visa's strategy is as much about moving the market to contactless payments as it is about EMV adoption. "By encouraging investments in EMV contact and contactless chip technology, we will speed up the adoption of mobile payments as well as improve international interoperability and security," according to Jim McCarthy, global head of product at Visa, Inc.

Find Visa's full announcement here: http://corporate.visa.com/media-center/press-releases/press1142.jsp

Merchant incentives to upgrade to EMV chip-enabled terminals

The first of three initiatives in Visa's plan to encourage the adoption of dynamic chip authentication technology is aimed at merchants:

Effective October 1, 2012, Visa will expand its Technology Innovation Program (TIP) to the U.S. TIP will eliminate the requirement for eligible merchants to annually validate their compliance with the PCI Data Security Standard for any year in which at least 75 percent of the merchant's Visa transactions originate from chip-enabled terminals. To qualify, terminals must be enabled to support both contact and contactless chip acceptance, including mobile contactless payments based on NFC technology. Contact chip-only or contactless-only terminals will not qualify for the U.S. program. Qualifying merchants must continue to protect sensitive data in their care by ensuring their systems do not store track data, security codes or PINs, and that they continue to adhere to the PCI DSS standards as applicable.

Requirements for acquirer processors to support chip acceptance

The second Visa initiative is aimed at acquirers to ensure that merchants' EMV payments can be accommodated:

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. Chip acceptance will require service providers to be able to carry and process additional data that is included in chip transactions, including the cryptographic message that makes each transaction unique. Visa will provide additional guidance as part of its bi-annual Business Enhancements Release for acquirer processors to certify that their systems can support EMV contact and contactless chip transactions.

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 9

Introduction of U.S. liability shift policies

The third Visa initiative sets dates for a shift in fraud liability from card issuers to merchants' acquirers in order to further encourage chip adoption:

Visa intends to institute a U.S. liability shift for domestic and cross-border counterfeit card-present point-of-sale (POS) transactions, effective October 1, 2015. Fuel-selling merchants will have an additional two years, until October 1, 2017 before a liability shift takes effect for transactions generated from automated fuel dispensers. Currently, POS counterfeit fraud is largely absorbed by card issuers. With the liability shift, if a contact chip card is presented to a merchant that has not adopted, at minimum, contact chip terminals, liability for counterfeit fraud may shift to the merchant's acquirer. The liability shift encourages chip adoption since any chip-on-chip transaction (chip card read by a chip terminal) provides the dynamic authentication data that helps to better protect all parties. The U.S. is the only country in the world that has not committed to either a domestic or cross-border liability shift associated with chip payments.

MasterCard Shifts Liability for ATM Transactions

On September 1, 2011, MasterCard announced it will extend its existing EMV liability shift program for inter-regional Maestro ATM transactions as part of an effort to align technology efforts to prevent and manage fraud. The liability shift covering the United States will be effective on April 19, 2013. Seth Eisen with MasterCard Worldwide explained the mandate, saying "To be clear, we are not mandating the U.S. ATMs must accept EMV cards. Rather, we are saying that if a chip card is presented at an ATM that does not accept a cross-border transaction, then the liability shift occurs." The shift places the liability for fraud losses on the ATM host owner.

The First in a Long Chain of Discourse—More to Come

The announcements from Visa and MasterCard are just the start of a much larger conversation, one that must include all players along the payments value chain. The range of impacted stakeholders must be part of the decision-making to help ensure a cohesive payments environment in the U.S. Organizations that get educated on the business and technical implications of a chip-based payment standard—and become actively involved in the industry's evolution—will profoundly affect the success (or failure) of a smart card migration in the U.S.

 ©2011 First Data Corporation. All rights reserved.

Comparing the Upsides and the Downsides of Smart Card Adoption

It's obvious to most that U.S. adoption of a chip-based payment standard holds many benefits, but it doesn't come without downsides to be contemplated as well. Issuers, acquirers and merchants will have decisions, costs and efforts involved in enabling EMV within their systems including chip production, card issuance, operating system updates, consumer education efforts and/or new equipment purchases. We listed some considerations below that may help impacted businesses evaluate their individual ROIs.

Security enhancement and potential fraud shift

The advantages of chip cards over magnetic stripe cards are recognized by many; chip cards can be an important part of a layered security approach. However there is still debate in the U.S. as to whether our implementation of EMV should be chip + PIN only or if chip + signature should be accepted as well. The EMV technical standard doesn't dictate how, or even if, the cardholder must be validated. An application embedded on the chip at issuance is steered by the card brand's and issuer's preferred cardholder verification methods (CVMs), typically in the form of a PIN or a signature, but occasionally no CVM is used as in the case of low value transactions or unattended POS locations.

The major markets that have already deployed EMV have all adopted chip + PIN as the dominant authentication method. One reason for doing so is to accommodate offline PIN verification which is unlikely to be used much in the U.S. The combination of a smart chip and the online authorization process we currently use in the U.S. far exceeds anything possible with magstripe technology. The card's chip working in conjunction with a PIN provides the type of two-factor authentication that combats the use of lost or stolen cards—via a cryptogram in the chip to authenticate the card's validity and a PIN entry to validate that the person using the card is the cardholder. And adding additional layers of data protection in the forms of encryption and tokenization protect cardholder data in ways that EMV alone can't.

What isn't covered from a security standpoint? Chip + PIN at the physical point-of-sale specifically solves for card-present fraud but does not resolve the question of card-not-present fraud. The statistics for the U.K. and other EMV-enabled countries bear out the fact that thieves will follow the path of least resistance—which in the case of smart chip enablement is shifting to CNP channels such as Internet banking, eCommerce and mail or phone orders. For example, Canada experienced a 25 percent increase in CNP fraud from 2009 to 2010, just at the time when chip + PIN was rolling out on a massive scale throughout the country. For the same period, total card fraud of all categories rose by only 2.05 percent.[20]

While overall CNP transactions are still a small portion of all card payment transactions, the percentage is on the rise. With the volume of CNP transactions growing rapidly, fraud losses from this category are also on the rise.

[20]Royal Canadian Mounted Police, http://www.rcmp-grc.gc.ca/scams-fraudes/cc-fraud-fraude-eng.htm

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 11

There are solutions to address this problem, although none has seen significant widespread acceptance. One solution that exists today puts a small EMV-compliant card reader in the hands of the individual consumer to authenticate his card for online purchases or banking sessions. This solution has a long way to go before it is widely implemented. It's also feasible that an NFC card reader could be built into or attached to devices like PCs and tablet computers.

Another way that online credit and debit card transactions can be authenticated is via a protocol known as 3-D Secure. Services based on the protocol have been adopted by MasterCard (MasterCard SecureCode), Visa (Verified by Visa), JCB International (J/Secure) and American Express (SafeKey). The basic concept of the protocol is to tie the financial authorization process with an online authentication which is often a password that is verified by the issuing bank. To date, adoption is low. To accept payments that are authenticated in this manner, merchants have to subscribe to a service that can be costly and can, at times, create unwarranted transaction failures. Moreover, 3-D Secure disrupts the customer experience to steer the consumer to a third party website, resulting in significant cart abandonment rates.

Other authentication mechanisms are readily available to fight CNP fraud, as well. They include Short Message Service (SMS) authorization codes and Universal Serial Bus (USB) security tokens. When these types of approaches have been used in Europe, the results have been good.

Conversion and implementation efforts and costs for all stakeholders

Probably the biggest issue for implementing EMV in the United States is the time and cost that would be required for full implementation. Just what would it take to replace more than 15 million point-of-sale devices,[21] more than 360,000 automated teller machines,[22] 609.8 million credit cards, and 520 million debit cards?[23] Javelin Strategy & Research estimated the total cost at $6.75 billion to replace all those POS terminals; an additional $1.4 billion to issue smart chip-compliant cards; and about $500 million for ATM upgrades. All told, it could be an $8 billion proposition to implement the new anti-fraud technology.

The costs, however, deserve further analysis.

Some of the costs may already be sunk. The Smart Card Alliance reports that some of the transition expenses have already occurred as merchants and financial institutions upgraded their systems for PCI compliance and regular replacement cycles. What's more, global players such as payment processors and POS and ATM device makers have already modified their products and services to accommodate EMV in other countries; they are essentially EMV-ready for the U.S. market with some modifications. Wal-Mart and other major merchants have already installed EMV-enabled terminals at the point-of-sale.

In addition, merchants may see offsetting savings that lessen the implementation costs. For example, a significant portion of the cost will be borne by merchants who already balk at the burden that card security places on their businesses. Multi-lane merchants are likely to spend at least $500 per lane in the migration process.[24] If merchants choose to participate in the program, Visa's incentive to install EMV POS terminals that can accept both contact and contactless payments may offer merchants some relief around the burden of PCI validation. Depending on the size and scope of the merchant, reduced spending on PCI validation could offset at least some of the cost of new POS devices.

---

[21] The Nilson Report

[22] ATM & Debit News says there were 360,659 ATMs in service in 2007

[23] Ben Woolsey and Matt Schulz, "Credit card statistics, industry facts, debt statistics," http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php

[24] "How Soon 'til United States of Chip and PIN?", Digital Transactions, October 2010

 ©2011 First Data Corporation. All rights reserved.

As for financial institutions, there would be a significant cost to replace all the magstripe cards ($1.4 billion to issue EMV-compliant cards as cited by Javelin). Smart chip cards, however, have a longer shelf life: the embedded microchips can be flash-updated as needed to accommodate new or changed applications. The cards become an asset rather than a pure expense, which changes the way banks account for the cost of cards. Although the costs of EMV-enabled cards are still more expensive than traditional magnetic stripe cards, the cost of producing the chip-enabled plastics is coming down, lowering the barrier of replacing more than a billion bank cards.

CFOs of every player involved in a smart card rollout will certainly be scrutinizing their expected ROI. Looking at the industry in total: if the cost of EMV implementation is approximately $8 billion, and the annual cost of card fraud is $8.6 billion, and there is a two or three year phase-in, then the cost of EMV implementation could be recovered quickly and all players could gain from a lower overall card fraud rate.

Put into an overall context with the benefits, the implementation costs may be a worthwhile investment in order to reap the long-term benefits such as vastly reducing the payments fraud problem, further enabling mobile and future emerging commerce technologies, and bringing about compatibility with other EMV-enabled countries. The ultimate decisions will be made by individual merchants and issuers based on implications specific to their respective businesses.

Global standard

When the U.S. migrates to a chip-based payment standard, it will essentially put the world's major markets on one global fraud protection standard for face-to-face payments. This will reduce cross-border fraud and make it easier for travelers to use their cards internationally. Not only will American travelers be able to use their cards abroad, but foreign travelers coming to the U.S. can use their cards here, thus enabling more electronic payments. Additionally, having a global standard deployed the world over will set the stage for the eventual retirement of transactions based on less secure magstripe technology, further reducing the opportunities for card fraud. When the players in the payments value chain only have to support one set of technical standards for card fraud protection, they can focus their resources toward more revenue generating projects and reduce costs.

Mobile payments facilitation

EMV and mobile payments require similar behind-the-scene infrastructures for several portions of payments transactions. And while mobile payments grow, it is more and more obvious that a standard system such as EMV is critical for mobile payments.

Customers' needs and wants are changing, leading us to the precipice of a great rise in mobile payments. (See Figure 1.) According to Aite Group, there are several factors that have quietly been laying the foundation for mobile payments to grow. They include the rapid consumer adoption of smart phones; carriers' and handset manufacturers' adoption of Near Field Communication (NFC) chips; consumers' continued embrace of mobile commerce (mCommerce); and a nationwide increase in mobile banking adoption. Aite Group predicts that mobile payments will see a 68 percent compound annual growth rate between 2010 and 2015.[25]

Speaking at the Mobile Payments Industry Roundtable last year, Dennis Lockhart, president of the Federal Reserve Bank of Atlanta said, "Mobile is a transformational enabler of financial commerce in every human endeavor, particularly in developing countries." The ability to have secure, convenient mobile payments based on a standard infrastructure is critical to acceptance of mobile payments.

---

[25]Aite Group report, "U.S. Mobile Payments: The Time Has Come," November 2010

 ©2011 First Data Corporation. All rights reserved.

In spelling out its roadmap for EMV adoption, Visa emphasizes the importance of EMV to mobile payments. The announcement reads, "The adoption of dual-interface chip technology will help prepare the U.S. payment infrastructure for the arrival of NFC-based mobile payments by building the necessary infrastructure to accept and process chip transactions that support either a signature or PIN at the point-of-sale."[26]

Everyone benefits from mobile payments, including financial institutions, merchants and customers. The Smart Card Alliance cites the following benefits of NFC mobile proximity payments:

- Reliability at the POS
- Security
- Ease of use and convenience
- Wallet functionality
- Value-add applications

Flexibility

Smart cards hold the promise of new revenue sources as they provide an opportunity to launch additional services enabling marketing offers, loyalty programs, identity verification and more.

Additionally, the chip can be programmed to perform numerous functions, and the applications on the card can be updated as needed by the card issuer. This is good news for financial institutions that no longer would have to issue new cards to change the applications; new instructions can be downloaded to the chip via a customer's visit to the bank branch or ATM.

Lack of central direction and regulation

As we mentioned earlier in this paper, despite the signs that U.S. industry players are getting restless, there is no indication that the Federal government will nudge us closer to a smart card implementation through legislation. In "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Richard J. Sullivan, senior economist at the Federal Reserve Bank of Kansas City wrote, "As the central bank of the United States, the Federal Reserve has responsibility to ensure that payments are safe, efficient, and accessible. Confidence in the safety of payments is particularly important. Thus far, the role of public policy has been to encourage the card payment industry to develop its own standards and procedures that limit fraud. Whether this policy stance is sufficient depends on the effectiveness of industry efforts to limit fraud in light of the dramatic shift towards card payments."

It's too early to tell if this hands-off policy will hinder or help the smart card adoption issue. Other regions found it necessary to have financial regulators impose guidelines and deadlines on participants to enforce universal adoption. In Europe, for example, the Single European Payments Area required 38 countries to complete the migration to EMV by January 2011. In Canada, Interac Association, the national debit switch, established the migration dates for cards and terminals. While we want to believe that the U.S. payments industry can act on its own behalf, it just might take an act of Congress plus oversight by the Fed to get the process going and to mandate that all players participate by specific deadline dates.

Right now, though, each impacted business determines if the benefits outweigh the efforts.

---

[26]Visa press release, August 9, 2011, http://corporate.visa.com/media-center/press-releases/press1142.jsp

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 14

Implications of Smart Card Adoption in the U.S.

Smart Card adoption in the U.S. is an industry-wide issue, and there is substantial education required for all participants to understand what chip enablement means to them.

For financial institutions

Financial institutions should start considering what a smart card implementation might mean to their businesses and look into options for issuing new chip-based credit and debit cards to their customers. This list is by no means comprehensive, but these are some considerations: Contact only? Both contact and contactless? What applications to store on the chip? How to update the chip after issuance? How best to educate the cardholders about using the cards?

The cost of the cards, along with the potential expense balancing opportunities, is another consideration. The typical cost of a magstripe card is about $0.15, whereas First Data estimates a chip-based card can cost, on average, between $2–$4. Though this is a considerable difference, financial institutions should see the initial costs of the chip card offset over time by the reduction in fraud and the savings of not having to reissue cards when making application changes. What's more, the new cards can be accounted for as an asset rather than merely an expense.

Mobile payments—whether supported by EMV or not—introduce a new complexity to the market because there are so many new business models and new players. For example, companies like Google, Verizon, PayPal and Amazon are now in the payments space, and financial institutions need to understand how to compete against them or partner with them to leverage the technologies and business models these companies offer.

The largest implication for banks is the high potential for card-present fraud reduction. Card fraud has always been a concern but it was considered manageable; the revenue from card interchange was sufficient to cover the losses. The Durbin regulations have changed that equation. With less revenue from interchange, banks may need to look at reducing losses from fraud. This could be issuers' biggest consideration regarding smart card implementation.

The card fraud liability shift is important too. Visa has announced dates for merchants to be smart chip-compliant or their acquirers assume the liability for fraudulent card use at the POS. Of course, this shift assumes that financial institutions have already issued EMV-compliant payment cards. The shift policy gives both merchants and banks incentive not to lag behind in smart card deployment.

For merchants

Merchants of all sizes—from single location to nationwide—have many decisions to make. While Visa is the first of the card brands to come out with its directives on implementing smart card technologies, more announcements will likely come. (It's important to note again that there is no government-enforced mandate at this time; Visa's roadmap is an industry call-to-action.) Merchants are starting their education process and beginning to formulate plans.

To implement smart card acceptance, merchants would be responsible for upgrading/replacing their POS devices and assume the cost of doing so. Smaller merchants will likely follow the advice of their acquirer; larger merchants will do their own research and make an educated choice. There is a level of effort to understand what the new POS devices can and can't do, and there are many device options on the market. A major decision is whether to deploy contactless along with a contact connection. Though Visa's incentives "require" both, the choice belongs to the merchant. All merchants

 ©2011 First Data Corporation. All rights reserved.

will want to future-proof their investment as much as possible. The cost of an EMV terminal will be determined by the features, functionality, quality, support and form. Upgrade or purchase costs will vary greatly among manufacturers and their models. Many manufacturers and payments players are adding new functionalities into the EMV-enabled equipment to position merchants to be ready for future innovations by making their equipment more innovation-agnostic.

Merchants will need to coordinate with their acquirer/processor to accommodate the transaction messaging for EMV-based payments. More data is sent to the acquirer from an EMV-compliant transaction than is sent from a magstripe-based transaction. Both message types will need to be supported while merchants continue to accept magstripe cards along with the new EMV cards and contactless devices.

Another decision for merchants and their acquirers to coordinate in smart card acceptance is whether to require a PIN, a signature or neither for cardholder authentication in a debit transaction. The Durbin Amendment gave this authority to merchants for the first time for debit cards and it is just now being phased in for magstripe transactions. This decision is also based on what issuers allow on their chip-based cards.

As EMV is deployed, there will be procedural changes at the POS. Customers who are unfamiliar with the chip-based cards, phones and fobs will need to be shown the proper way to insert or tap their cards in or over the devices and then to authenticate their identification. Employees will need to understand these new procedures in order to help customers and to explain the security benefits as customers complain or ask questions.

And then there's the issue of liability shift. Today financial institutions bear the brunt of the liability for fraud, but a new policy likely will assign liability to acquirers in certain instances. Merchants will want to get a full understanding of when and how liability will shift to their acquirer/processor and ultimately to them.

There are positive implications for merchants as well. For example, most EMV-enabled POS equipment will include contactless technology, allowing merchants to accept contactless and mobile payments which will provide a higher level of convenience for customers and will speed up the check-out time. In addition to faster transactions, some of the new smart chip-enabled POS devices will also help drive loyalty and repeat business by pushing offers out to mobile phones and redeeming the offers through the devices themselves. Moreover, customers will appreciate the higher level of security and feel more confident about using their cards with the merchant. While smart cards won't solve every security problem, they will go a long way toward boosting customer confidence at the POS.

For consumers

Smart card usage is largely an education issue for most consumers. Since they are accustomed to swiping their magstripe cards at the POS, they will need instructions to insert the card into the terminal and leave it there while entering the PIN, or to tap the card against a contactless reader for a speedy checkout. Contactless payments in particular will need to be promoted by both banks and merchants as very few consumers use this method of payment initiation today. Discover reports that only 5 percent of contactless cards on the market today are ever used for a contactless transaction, and total contactless transactions are only 0.03 percent of the total debit market. Usage will need to be much higher than that to justify the investment in contactless chips and POS readers.

Consumers who are hearing the term "liability shift" in the news may have the misconception that they will be responsible for all costs if their card accounts are used without their authorization. This, too, is an educational undertaking for the banks and merchants.

A positive development for consumers is that they will be able to use their cards as they travel internationally without fear of payment rejection. Since EMV is a global standard, there should be no acceptance problem due to technical incompatibilities.

 ©2011 First Data Corporation. All rights reserved.

Conclusion

We don't claim to have a crystal ball to know when all of this will come together in the U.S. market, but we feel confident in saying that some form of chip-based payment standardization is coming to the U.S. Clearly the need to reduce fraud and increase security exists, and now some of the industry's largest players are starting to put incentives in place to encourage merchant, acquirer and financial institution migration.

Thoughtful discussion and deliberation among all stakeholders

The Federal Reserve Bank of Atlanta president Dennis Lockhart sums up this country's unique situation thusly: "The U.S. has a large noncash infrastructure that does not exist in other countries. One challenge for stakeholders is to decide collectively on the rails and infrastructure to use while considering cost issues. Attempting to establish different payment infrastructures at the same time may not work well. With the right infrastructure, some of the key players can align, new applications will be developed, and consumers will use the service. Otherwise, disruptive innovators will figure out solutions to provide services in a way that may not be optimal for security reasons."

Your organization is a key player in this very serious game. We recommend you conduct a full assessment to understand the impact of EMV on your business. Be a part of the industry discussions so you can understand and influence how the payments ecosystem moves forward with smart card implementations.

Plan ahead

What can merchants do now to prepare?

- Engage a POS provider and begin assessing what a smart chip enablement plan would look like for upgrading all consumer-facing POS devices.
- Speak to your third-party POS software providers to understand their strategy to become EMV compliant.
- Discuss with your processor when they will be ready for smart card processing and discuss other ways you can reduce fraud and data theft risks as part of a comprehensive payments security plan.

What can card issuers do now to prepare?

- Assess the equipment and operational requirements, and set up parameters, controls, and procedures that support the issuance of smart cards, and subsequently facilitate the processing of authorizations and transactions initiated by these EMV devices. Issuers should also engage applicable vendors and providers to map out a potential plan. For some issuers, this may mean evaluating the possibility of outsourcing card production currently done in-house.
- Quickly enact an EMV-issuance strategy for cardholders that travel internationally and who are being denied when they use their magnetic stripe payment cards when paying abroad.
- Determine what a chip card implementation strategy would look like to coincide with card reissuance cycles and meet the October 1, 2015 timeline.
- Develop an education plan to help consumers understand smart cards and the benefits.

Get educated

It appears some form of EMV will eventually come to the U.S. marketplace. Now is the time to get educated so you can understand the issues and the choices ahead. First Data recommends the following reading list to learn more about chip technology and related security measures for the payments industry.

 ©2011 First Data Corporation. All rights reserved.

Mastercard, Ex1041, p. 17

First Data Market Insights white papers:

- Key Trends in Merchant Security: A Multi-Layered Approach that Will Dramatically Reduce Risk
- Why Wait for EMV to Solve Your Fraud Problems? One-Time Use Card Numbers Can Reduce Debit Fraud Now

EMVCo white papers and other resources:

- A Guide to EMV
- EMV Contactless Mobile Payments

EMVCo has an associates member program to allow stakeholder parties to provide technical and business input to decisions regarding the EMV specification. Learn more about the program at http://www.emvco.com/about_emvco.aspx?id=184.

To keep abreast of updates to the technical specifications for EMV, sign up to receive automatic notifications when new information is posted to the EMVCo website. You may register for free through the EMVCo Contact Us page.

Smart Card Alliance white papers:

- Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?
- Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud
- The Mobile Payments and NFC Landscape: A U.S. Perspective

Additional security layer options from First Data:

- The First Data TransArmor solution for end-to-end encryption and tokenization
  - Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance
  - A Primer on Payment Security Technologies: Encryption and Tokenization
  - Implementing Tokenization Is Simpler Than You Think
- The STAR CertiFlash solution for debit fraud
  - Why Wait for EMV to Solve Your Fraud Problems? One-Time Use Card Numbers Can Reduce Debit Fraud Now

 ©2011 First Data Corporation. All rights reserved.

The Global Leader in Electronic Commerce

Around the world every day, First Data makes payment transactions secure, fast and easy for merchants, financial institutions and their customers. We leverage our unparalleled product portfolio and expertise to deliver processing solutions that drive customer revenue and profitability. Whether the payment is by debit or credit, gift card, check or mobile phone, online or at the point of sale, First Data helps you maximize value for your business.

About the Author

Dom Morea is SVP, Advanced Solutions and Innovation at First Data Corporation where he is responsible for leading the company's efforts in transformational initiatives such as Mobile Commerce and Personalized Marketing. Morea, a 20-year+ veteran of the financial services industry has been with First Data since 2004; when he rejoined the company as SVP, Product and Business Development to lead product management for the company's merchant acquiring division.

Morea has also previously held management positions at Credit Suisse and Citibank. He serves on the boards of several influential organizations such as Smart Card Alliance, ViVOtech and PNC Merchant Services and has been a featured speaker at a number of payments and mobile industry forums including CTIA, NACHA, Card Forum and the DRF. Morea is a Cum Laude graduate of Hofstra University.

Contributors

Philip (Phil) Christiansen is VP of Credit Services for the Global Product Management division of First Data and is responsible for the oversight of credit product offerings provided to the financial institution market, including general purpose credit cards, retail closed-loop credit cards and consumer loans.

Bruce Dragt is SVP of Payment Acceptance at First Data Corporation, responsible for driving product development globally across the company's suite of merchant products. These products include core acquiring, eCommerce, International Currency Solutions, Leasing, TASQ, TeleCheck and security products

G. Russell (Russell) Randolph is VP of Network, Debit, and ATM Solutions at First Data Corporation. In this role, Randolph is responsible for global product development and manages First Data's network, debit and ATM solutions for the financial institutions market.

For more information, contact your First Data Representative or visit firstdata.com

 ©2011 First Data Corporation. All rights reserved.

1781

Mastercard, Ex1041, p. 19