CSCU's payments solutions are tailored to what matters – *serving your members.*

EMV ESSENTIALS
FOR US CREDIT UNIONS

A Mercator Advisory Group Research Brief Sponsored by

CSCU
CARD SERVICES FOR CREDIT UNIONS

CSCU is the credit union industry's advocate, partner and leader in total payment solutions. Created by and for credit unions, we are driven by the same principles that guide the industry. We work exclusively with credit unions to provide a customized, holistic offering that maximizes value for both credit unions and their members. CSCU's services and offerings are focused on driving the growth and success of our nearly 3,000 member credit unions.

www.CSCU.net

8 Clock Tower Place, Suite 420 | Maynard, MA 01754
phone: 1(781) 419-1700 | e-mail: info@mercatoradvisorygroup.com
www.mercatoradvisorygroup.com

Table of Contents

8 Clock Tower Place, Suite 420 | Maynard, MA 01754
phone: 1(781) 419-1700 | e-mail: info@mercatoradvisorygroup.com
www.mercatoradvisorygroup.com

Introduction

Two major payments technologies are coming to the United States in the coming months and years. The first, NFC (near field communications), is generating plenty of buzz because it is all about contactless payments, smartphones, and mobile marketing. The other, the EMV smartcard standard, may be receiving less attention but it no less an impact on payment security, card issuance, and issuer planning than its contactless, smartphone-based cousin.

As these two approaches come forward at the same time, they have caused considerable concern and confusion among merchants and issuers alike. Facing a market-driven imperative around NFC (mobile commerce is hot!) and a security-driven imperative around EMV (counterfeiting magstripe cards is too easy!), merchants in particular are confronted by critical choices regarding their payment acceptance systems. Merchants operate in the real world of existing payment infrastructure and massive investments into that infrastructure.

The twin technologies of EMV and NFC are especially important to large merchants as they plan for new products and payment acceptance systems in a world that is increasingly homogeneous, where customers travel between regions and expect a consistent consumer experience. The payment step in the transaction cycle is a major element of that overall experience. Of course, layered into the customer experience is concern for payment security and PCI compliance.

Because it requires all cards and terminals to be replaced, EMV alone is a significant upgrade to the U.S. payments system. Every POS terminal and every ATM's card acceptance sub-system will require either replacement or enhancement. Fortunately, if it can be put this way, EMV presents an opportunity to upgrade POS terminals and ATMs to support both contact EMV and contactless transactions as well as other transaction types from cards, apps on smartphones, and NFC-equipped handsets. In other words, if an upgrade must be made—and it must—it is best to get it over with all at once. Services from Visa, MasterCard, payment processors, and other service providers may further ease message decryption and other concerns.

This Issuer Update answers key questions around EMV's arrival in the U.S., why credit unions should care, and suggests the next steps for a card issuer to consider.

8 Clock Tower Place, Suite 420 | Maynard, MA 01754
phone: 1(781) 419-1700 | e-mail: info@mercatoradvisorygroup.com
www.mercatoradvisorygroup.com

EMV Essentials

What is EMV?

EMV is a payment security approach based on smartcard technology that adds dynamic data to the transaction stream that, unlike standard static magstripe card data, renders replay of payment transactions impossible. More important, because every card is a small secure computer, containing a microprocessor, memory, and applications, EMV cards are impossible to counterfeit economically.

While improvements to magstripe security exist, EMV is the technology that the payment card brands and global financial institutions have chosen to stop card counterfeiting. The organization responsible for development of EMV standards is EMVCo, a consortium owned by MasterCard, Visa, AMEX and JCB.

EMV is now in wide global deployment (Table 1). Globally over 1.3 billion EMV cards are in circulation with 15.4 million EMV POS terminals as acceptance points. A 100% penetration rate of EMV cards and terminals is the eventual goal. The UK and Lithuania are already there, Ireland is one one hundredth of a percentage point away, and both Germany and France are within 5% of complete EMV deployment. Canada and Mexico are well along in their EMV roll-outs. 100% EMV deployment will be the long term goal for the U.S. as well.

Exhibit 1: Global Card and POS Terminal Deployment Rates, Q3 2011

Region	EMV Card Penetration	Cards Issued	EMV Terminal Penetration	EMV Terminals Deployed
Canada/LATAM/Carib	38.0%	259,549,827	80.0%	4,342,000
AsiaPac	20.2%	317,316,028	49.5%	4,174,000
Africa & Middle East	20.2%	25,882,716	66.4%	380,000
Europe Zone 1	80.6%	708,914,657	93.8%	10,985,000
Europe Zone 2	13.3%	31,739,128	71.1%	586,500
United States	< 1% -	~ 100,000	-	~ 100,000-

Source: EMVCo, 2011

But today, the U.S. is on a magstripe island, increasingly surrounded by EMV-based countries and, as a result, increasingly exposed to cross-border card fraud.

What is an EMV Card

An EMV card is a smartcard, a small computer. Each card is exactly the same size and thickness as a standard magstripe card. An EMV card is not swiped like a magstripe card. It is inserted into a slot on the POS terminal. On the face of the card is a metal contact. When inserted, the contact on the face of the card connects the card to the terminal and the two devices are then able to communicate. Of course, almost all EMV cards also have a magstripe for use at terminals that haven't been upgraded to EMV.

EMV also supports contactless payments. A card capable of both contact and contactless transactions is called a dual interface card. A dual interface card can be either tapped at the POS terminal for a contactless transaction or inserted into the EMV card reader for a contact-based transaction. From a risk perspective, both are equally secure. In Canada, nearly 100% of MasterCard-branded cards are dual interface cards. Importantly, the contactless EMV interface is the same one that smartphones equipped with near field communications (NFC) chips use so a POS terminal that supports both contact and contactless EMV is ready to accept mobile payments from smartphones.

Multiple Deployment Options

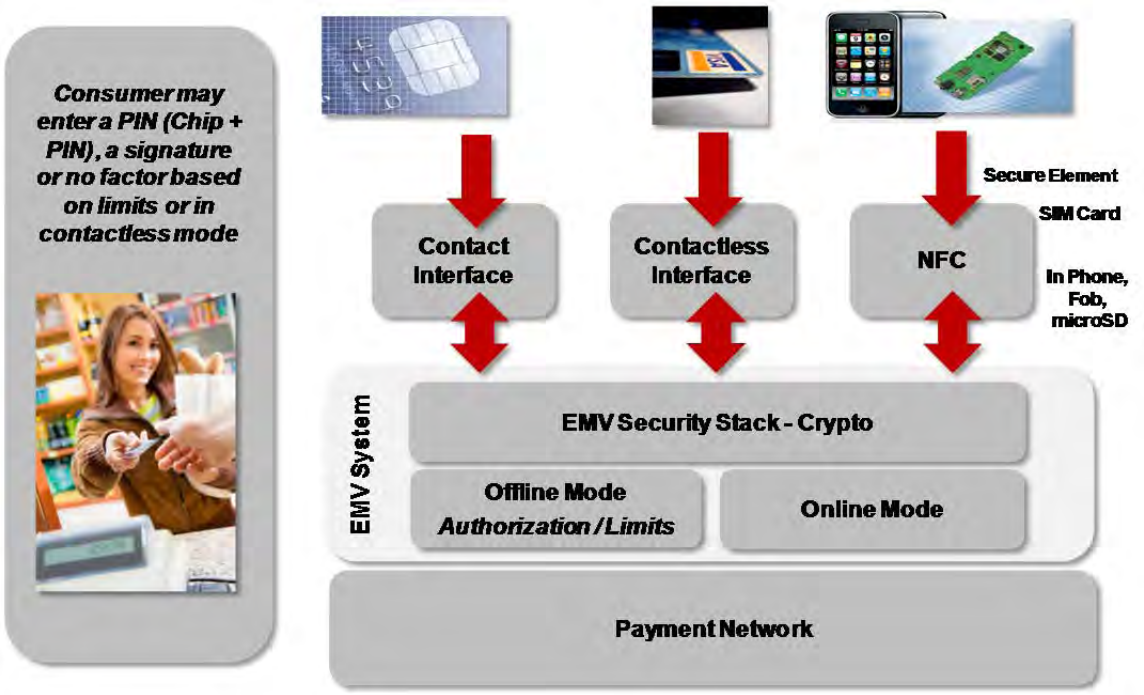
For many US readers, the term "EMV" has been synonymous with a contact-only, PIN-only technology. Often referred to as "chip-and-PIN" – the approach used in the UK and in other countries (Exhibit 3) – this is just one of the available deployment options. Signature-based EMV transactions via the contact interface exist as do, and this is important, contactless EMV transactions. The EMV standard supports credit, debit, and prepaid payment cards. And it can be built into smartphones armed with NFC chips (Exhibit 2).

EMV supports multiple cardholder verification methods (CVM) including signature, no CVM, and PIN. The PIN, and this is a critical distinction, may be offline or online. Offline PIN means the PIN is stored on the card and the validation step is conducted by the card and the terminal without going online to validate the PIN. The cardholder inserts the card into the reader, enters the PIN on the encrypting PIN entry device, and the terminal sends the PIN to the card to validate the number. Similarly, transaction size and velocity limits may be stored on the EMV card to further limit the need to go online.

EMV cards can be deployed for online authorization, called chip and signature. The decision of which authorization approach to employ is generally made on a national level (Exhibit 3). Because the U.S. is an "all online all the time" authentication environment, offline PIN and its associated higher costs (the card requires stronger cryptography and larger memory in each card) are not necessary to serve the needs of the domestic market.

As with the magstripe predecessor, EMV cards support credit, debit, and prepaid card issuance. Visa and MasterCard are suggesting that that the U.S. will be a chip-and-signature country for credit card transactions. That option certainly limits the changes that adding a PIN to all credit card transactions would require. While signature-based EMV debit cards will no doubt exist, Mercator expects debit card issuers to continue to employ online, host-based PIN authorization with their EMV debit cards to maximize their fraud loss performance.

Exhibit 2: EMV - Multiple Form Factors, Multiple Communications Links



Source: Mercator Advisory Group, 2012

Of course, expecting all security troubles to be resolved by one technology is wishful thinking. EMV deployment has suffered from this "silver-bullet-itis" as well but it is no more a cure-all than card number encryption. Payments security is about layers of defense because many are required to block criminal hackers. For example, the best e-commerce merchants, the Merchant Risk Council's Platinum members, use on average 7.9 tools to manage their fraud risk. Weaker performers use fewer tools. At point of sale terminals and ATMs, EMV protects by eliminating the counterfeit and transaction replay risks, a pair of big holes.

Exhibit 3: EMV Deployment Options by Country and Customer Verification Method

Chip-and-Offline PIN Countries		Chip-and-Signature / Online PIN Countries	
Europe	Norway	Spain	Australia
Belgium	Poland	Portugal	New Zealand
Estonia	Slovakia	Mexico	China
France	Sweden	Italy	India
Finland	UK	Turkey	Malaysia (until 2015)
France	Japan	Germany	Russia
Ireland	Malaysia (after 2015)		*Rest of Asia is signature*
Netherlands	Canada		
Rest of Europe is Signature	Brazil		
	Chile		

Source: Mercator Advisory Group, 2012

Why Now

The venerable magstripe card has served the payment card well for decades, enabling untold numbers of electronic transactions. But the magstripe is no longer able to fend off fraudsters armed with low cost magstripe readers, card duplication gear and Internet-sourced card data. As those fraudsters have proven over and over, it is simply too easy to create counterfeit payment cards.

The result has been an outbreak of card skimming that has cost credit unions, merchants, other card issuers, and consumers millions. With most of the developed world now using EMV to prevent counterfeit card fraud, increasingly card fraud is migrating to the United States, affecting both point of sale and card not present e-commerce security. From a payment security point of view, the U.S. is a sitting duck, especially exposed to cross border fraud.

As card-generated revenues have fallen due to regulation and a weaker economy, fraud losses are playing a larger role in issuer calculations. With debit, in particular, becoming a cost-based activity, the use of an EMV card, along with a PIN to limit lost and stolen losses, becomes a stronger means to limit risk.

For international travelers, magstripe-only cards sometimes cause confusion at the checkout when the clerk does not know what to do with them. Magstripe cards, especially in France, do not work at some unattended locations. For U.S. issuers, this is causing some customer satisfaction concerns.

When is EMV Coming?

While it has been anticipated for years, the U.S. is beginning to adopt smartcard-based payment security in earnest. On August 9, 2011, Visa announced the beginning of what will be a long process to move the United States toward a broad deployment of EMV. Visa's avowed purpose was to pave the way for contactless and NFC-based mobile payments, all taking advantage of EMV's dynamic data to improve security. On January 31, 2012 MasterCard answered with its own announcement in support of the U.S. EMV rollout. With both major card networks behind the initiative, EMV's arrival in the U.S. finally has some dates behind it. To nudge the payments ecosystem –acquirers and merchants in particular – Visa announced three separate programs with dates:

1. **Technology Innovation Program (TIP)**. The TIP program allows merchants to skip their annual Visa PCI compliance validation once 75 percent of their Visa transactions are originated on chip-enabled (EMV compliant) POS terminals. The U.S. TIP program goes into effect October 1, 2012. Qualifying POS terminals must accept both contact and contactless chip cards and contactless transactions from NFC-equipped mobile devices. Visa's TIP program does not eliminate a merchant's PCI requirements, just the validation once three quarters of Visa transactions originate from EMV capable terminals.
2. **Merchant Acquirers Get Ready**. By April 1, 2013, acquirers must be ready to process the cryptographically generated dynamic data associated with each EMV transaction.
3. **Merchant Get Ready - Liability Shift**. After October 15, 2015, if a cardholder with an EMV card must use the magstripe on that EMV card because the merchant does not have an EMV capable POS terminal, the merchant acquirer will be responsible for any counterfeit fraud associated with that transaction. The merchant acquirer is likely to, in turn, make the merchant responsible for the fraud on that transaction. This liability shift will be in effect for both domestic and cross border POS transactions. Gasoline retailers have another two years to prepare, given the high cost of upgrading their automatic fuel dispensers. The phrase "liability shift" is frequently used in discussions over EMV rollout. The purpose of the liability shift is to encourage the transition to chip cards. With chip-to-chip transactions, there is no concern regarding liability shift.

MasterCard's dates are equally aggressive. Both networks are pushing for a comparatively swift EMV rollout in the United States with that October 15, 2015 date. Of course, U.S. issuers have to get behind a massive EMV card rollout for that to happen and that is hardly a done deal. With U.S. as the largest card market in the world with 1.2 billion payment cards, the return on investment, especially for credit card issuers, is not entirely clear.

Besides issuers, merchants have to upgrade over ten million devices because EMV requires new security hardware and software in the point of sale terminal. That is another huge change. While the card brands have scheduled a 2015 liability shift for magstripe transactions onto the merchant (the merchant takes the risk for the transaction), this schedule will be challenging to meet. Large merchants typically refresh their

payment terminals every five to seven years. Small merchants can keep them for far longer. For those reasons alone, despite the liability shift, Mercator's forecast for EMV terminal deployment is 50% in 2016.

EMV issuance in the United States is getting underway, but the numbers are modest to date. A few large banks have begun to issue EMV cards to their corporate and high net worth customers. Several credit unions have issued EMV cards as well. More broad-based issuance is still months, if not a year or two, away. Reaching meaningful deployment rates, where chip-to-chip transactions predominate, is five years away. At least. Getting out well in advance of any domestic need, the State Employees' Credit Union of North Carolina has already started issuing the new smartcard format to its portfolio of 1.6 million debit cardholders.

Issuer Recommendations

To get ready for EMV *and* mobile payments, credit unions are wise to undertake these steps in preparation for an EMV roll-out. To be clear, the roadmap may be very different between credit unions. There is no single map to follow.

Begin the Planning Process. There are many moving parts to an EMV deployment. You must build an EMV roadmap that meets the needs of your members and your organization. As you consider how you will deploy EMV, here are key issues for your review:

- **Evaluate Member Needs**. Those US issuers who have already released an EMV card to date have done so, for the most part, to address the needs of their traveling card holders, largely higher net worth customers. Of the U.S. 311 million population, only 62 million (20 percent) are passport holders. That's a good place to start. So, evaluate your members needs based on travel patterns. Issue EMV cards to these individuals. As a number of larger U.S. issuers have chosen to do, you may wish to issue cards that are offline PIN capable. While more expensive, they work at every EMV terminal in the world provided, of course, that your member remembers his PIN.
- **Choose Your Card Verification Method**. You have decisions to make regarding the capabilities of the card you issue. For credit cards, what cardholder verification methods do you wish to support? Signature only or do you want a PIN? Do you want to make sure the card works absolutely everywhere (In France, there are bicycle rental kiosks, ticket machines, and after hours fuel pumps that accept only offline PIN capable cards) or are you OK with operation in online markets?
- **Issue Both Debit and Credit**. Protecting both credit and debit card portfolios requires issuance of EMV cards for both types. While credit transactions will generally be run as signature transactions in the US (that choice is, however, up to you as a card issuer) PIN debit as we know it will be an option that has the added security strength of a nearly counterfeit-proof smartcard. Given the PIN's strength in lowering lost, stolen, and friendly fraud losses and today's cost sensitive debit operations, an EMV debit card with online PIN authentication is a good option.
- **Provide Dual Interfaces**. Almost 100% of MasterCard-branded cards issued today in Canada are dual interface, containing both the standard contact chip interface and the upgraded, EMV-compatible

contactless interface. Because both Visa and MasterCard are encouraging POS terminal upgrades to support both contactless card and NFC-based smartphone transactions, the number of merchant locations capable of taking a contactless transaction will begin to grow, at last, in the next couple of years. The contactless feature is one to plan for, particularly as contactless payments will become more prevalent via the smartphone phone factor. As general merchants, as well as transit systems, adopt contactless payments, usage will increase.

- **Plan an ATM Update Process**. Your ATMs will require new card readers to take advantage of EMV smartcard security. ATM software must also be upgraded and, for older ATM models, that may have an impact on your ATM replacement plans. Make sure ATMs you are planning to purchase are EMV-ready. While you are at it, ask your supplier about transaction capabilities including mobile top-up, virtual card support and other features. Another area for consideration with your supplier is cash advance.
- **Processor Readiness**. Your card processor must be ready, of course, to handle EMV transactions. Now that Visa and MasterCard are actively encouraging issuers to move to EMV, it is prudent to make sure your processor can handle the new format. Ask your processor what EMV services are available or in their plan.
- **Prepare Staff and Member Training**. EMV will require training for both your staff and your members. At the very least, members will have to learn not to swipe the card but insert it into the card reader. Your staff may need to answer questions regarding the liability shift for non-chip transactions (it affects the merchant, not the member). And your staff will be able to point out the advantages during international travel (no acceptance concerns, higher security), whether to Canada, Mexico, or somewhere more distant.

Other Considerations

- **Not Your Plain Old Plastic Card.** Production of EMV cards is very different from the process issuers are accustomed to with magstripe cards. The card itself, as a small computer, is far more complex. Every card product requires its own script – a program that defines its capabilities – and each script requires testing. Personalization of EMV cards requires a different process as well. These services, as well as the cards themselves, will cost more than today's offerings. Obviously, instant issuance will be impacted, requiring new equipment capable of programming an EMV card.
- **Interchange.** At this time, the card brands have not announced any upcoming changes to interchange rates as a result of their EMV rollout plans. EMV is a security measure that replaces today's magstripe infrastructure and its economics are tied to improved fraud and risk performance. For example, PIN debit EMV cards will offer improved performance over magstripe PIN debit cards. At this time, it would be wise not to factor higher interchange into your plans to fund the higher cost of EMV card issuance.
- **Other Factors.** EMV cards offer a higher level of flexibility than magstripe cards. Transaction size and velocity limits may be written to the card itself. PIN changes are practical. And there is some evidence that the contact interface is more reliable than the magstripe. These features, along with the fraud loss mitigation from EMV's strong counterfeit card protection, should help drive ROI as well as ease operational concerns.

Begin the Transition. Based specifically on your evaluation on the number of the travelers among your members and in general on the support for EMV in the USA by Visa and MasterCard, put an EMV pilot card issuance program on your schedule. Once you've performed an analysis of your cardholder's travel patterns and consulted with your processor, issue EMV cards to those traveling members who will appreciate the convenience and security EMV cards offer while traveling.

By starting out with a limited portion of your card portfolio, you can gain the experience and supply chain familiarity you will need to complete the transition of your entire card portfolio once issuance and acceptance trends in the U.S. become clearer. There is no pressing need to consider a mass reissuance of your entire portfolio at this time. An EMV issuance plan that fits your normal card replacement schedule makes sense.

Platform for the Future

EMV does a lot to improve the counterfeit card problem at the point of sale and the ATM. Skimming card data gets much harder. By reducing the availability of static data, it also helps decrease card not present fraud during e-commerce and mobile commerce transactions. But it will take nearly a decade to achieve 100% EMV deployment in the U.S. Magstripe cards, and magstripe risk, will be with us for some time.

In the meantime, as NFC-equipped smartphones rollout in 2012 and beyond, the EMV shift will be used to increase payment security for mobile payments using NFC. EMV provides an important part of the security infrastructure needed for a wide range of mobile transactions. POS payments and e-commerce payments can also leverage, with the appropriate hardware, EMV and, in the case of mobile handsets, the hardware is there.

There continues to be speculation that the U.S. will skip over the EMV card form factor and move right to NFC-equipped smartphones for contactless transactions. While a phone-based payment approach is foreseeable a decade or more from now, the card form factor will be with us for a very long time. With both EMV and NFC payment technologies arriving at the same time, the smart credit union will plan to support both and take advantage of the security and marketing advantages each offers.

Copyright Notice

External publication terms for Mercator Advisory Group information and data: Any Mercator Advisory Group information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Mercator Advisory Group research director. A draft of the proposed document should accompany any such request. Mercator Advisory Group reserves the right to deny approval of external usage for any reason.

8 Clock Tower Place, Suite 420 | Maynard, MA 01754
phone: 1(781) 419-1700 | e-mail: info@mercatoradvisorygroup.com
www.mercatoradvisorygroup.com

White Paper by:

Sponsored by:

CSCU
CARD SERVICES FOR CREDIT UNIONS

3031 N Rocky Point Dr W, Suite 750, Tampa, FL 33607 813.289.2728 www.CSCU.net