DEPTH. FOCUS. SERVICE.

MERCATOR ADVISORY GROUP

EMV ESSENTIALS FOR THE U.S. MERCHANT

A Mercator Advisory Group Research Brief Sponsored by Heartland Payment Systems

January 2012

About Heartland Payment Systems

Heartland Payment Systems, Inc. (NYSE: HPY), the fifth largest payments processor in the United States, delivers credit/debit/prepaid card processing, gift marketing and loyalty programs, payroll, check management and related business solutions to more than 250,000 business locations nationwide. A *FORTUNE* 1000 company, Heartland is the founding supporter of The Merchant Bill of Rights, a public advocacy initiative that educates merchants about fair credit and debit card processing practices. The company is also a leader in the development of end-to-end encryption technology designed to protect cardholder data, rendering it useless to cybercriminals. For more information, please visit HeartlandPaymentSystems.com and MerchantBillOfRights.org.

www.heartlandpaymentsystems.com

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. One called NFC (near field communications) is getting plenty of buzz because it is all about smartphones and mobile marketing. The other, the smartcard standard EMV for secure payments, may be less well known in the U.S., but it is well known and broadly deployed elsewhere around the world.

As these two approaches come forward at the same time, they have caused considerable concern and confusion among merchants and issuers. 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 have committed 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 critical element of that overall experience. Of course, layered into the customer experience is concern for payment security and PCI compliance.

EMV alone is a significant upgrade to the U.S. payments system. To accommodate EMV, every POS terminal and every ATM's card acceptance sub-system will require either replacement or enhancement. EMV presents an opportunity for retailers to upgrade POS terminals and ATMs to support both EMV and contactless payment and other transactions from both cards 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 payment processors and other service providers may further ease message decryption and other concerns.

This Payments Trends update answers key questions around EMV's arrival in the U.S., why merchants should care, and suggests the next steps for a merchant to consider.

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 contains its own microprocessor chip (that's why it is called a smartcard), EMV cards are impossible to counterfeit economically.

While improvements to magstripe security exist, EMV is the technology that the payment card brands 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. Canada is nearing completion of its EMV roll-out and Mexico is well underway.

An EMV card is exactly the same size and thickness as a standard magstripe card (see Exhibit 1). 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 connects the card to the terminal and the two devices can communicate. Of course, almost all EMV cards also have a magstripe for use at terminals that haven't been upgraded to EMV.

Exhibit 1: Contact EMV Card

Source: Mercator Advisory Group, 2011

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 or inserted into the EMV card reader. In Canada, nearly 100% of MasterCard-branded cards are dual interface. The contactless EMV interface is the same one that smartphones equipped with NFC chips use so a POS terminal that supports both contact and contactless EMV is ready to accept mobile payments from smartphones.

EMV cards can be deployed for online and offline authorization. Online authorization uses a process similar to our magstripe authorization process today where the transaction is verified immediately via an online connection to the card issuer. Offline authorization is authorization between the card and the acceptance device, without online authorization. Offline authorization is called chip and PIN. The PIN unlocks the card. In many markets, a PIN is used for credit transactions as well. The choice of whether to use offline authorization generally runs on a national basis. Depending on the issuer and/or the merchant's preferences based on transaction type and size, the cardholder may or may not need to enter a PIN.

Given that virtually 100% of U.S. transactions are authorized online, the need for offline authorization, also known as chip and PIN, is negligible for domestic transactions. In the U.S. we expect the vast majority of credit cards issued to be "chip and signature" cards that will not require a PIN. Online authorization will be used as it is today with the chief EMV benefit being the elimination of counterfeit cards. As a result of the Durbin amendment and the greater need by issuers to manage the cost of debit processing, we expect debit cards to employ EMV online PIN verification, just as we do today.

EMV is a global standard. The U.S. is the major laggard and the last major EMV holdout (see Exhibit 2).

Exhibit 2: Online and Offline PIN Countries

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

Source: Mercator Advisory Group, 2011

Why is EMV the Right Choice?

The venerable magstripe 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 merchants, card issuers, and consumers millions. With most of the developed world now using EMV to prevent counterfeit card fraud, card fraud is migrating more and more 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.

EMV will protect against three issues when compared to magstripe:

1. Counterfeit cards. EMV cards are virtually impossible to copy.
2. Skimming. Because each transaction is unique and cards cannot be economically counterfeited, skimming an EMV card is not worthwhile.
3. Offline interceptions – "man in the middle" attacks – are thwarted because each transaction contains unique, encrypted data that is of no use to the fraudster.

When is EMV Coming?

While it has been anticipated for years, it appears that the U.S. is beginning to adopt smartcard-based payment security. 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 on dynamic data. To date, none of its major competitors have made similarly wide-ranging pronouncements, although they are expected to. Issuer reluctance, given the costs and regulatory environment, is not surprising.

To move the payments ecosystem – issuers, acquirers and merchants – Visa announced three separate programs:

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 on 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, merchant acquirers will be responsible for any counterfeit or fraud losses on a transaction 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 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.

Visa's pushing for a comparatively swift EMV rollout in the United States with that October 15, 2015 date. Of course, in order for that to happen U.S. issuers have to support a massive EMV card rollout.

What is MasterCard Doing? To date, the second largest card network is encouraging the EMV transition only on its ATM business. It is targeting inter-regional Maestro ATM transactions. But it hasn't announced any endorsement for a U.S. EMV rollout.

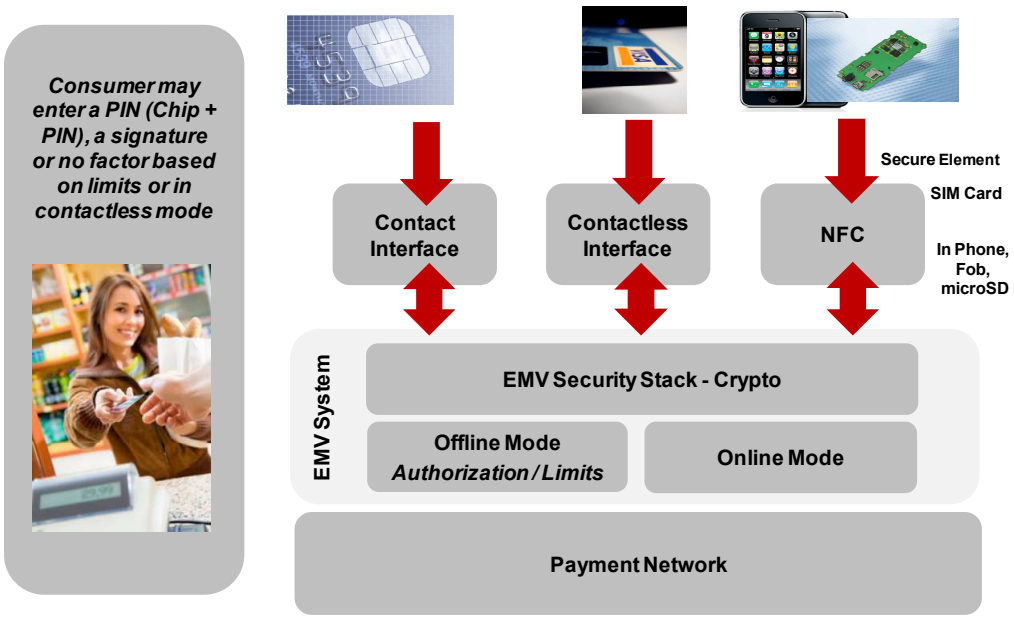
EMV issuance in the United States is getting underway. A few credit unions and a few large banks have begun to issue EMV cards to their corporate and high net worth customers. But there are plans to bring the security of EMV to more and more U.S. cardholders. Because debit issuance is now a cost-based activity, Mercator anticipates that

debit card issuers in the U.S. will opt for EMV cards to take advantage of the lost, stolen and friendly fraud protections that a PIN confers.

EMV is not One Thing

For many U.S. readers, the term "EMV" has been synonymous with a contact-only, PIN-only technology. The "chip-and-PIN" approach used in the UK and elsewhere, however, is simply an implementation decision. Signature EMV based on a contact transaction exists, as does (*and this is important*) contactless EMV. EMV can be used for any transaction type: credit, debit, and prepaid. And it can be built into smartphones armed with NFC chips (see Exhibit 3).

Exhibit 3: EMV - Multiple Form Factors, Multiple Communications Links



Source: Mercator Advisory Group, 2011

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 multiple layers work better. 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. For point of sale payments, EMV creates a secure environment by eliminating the counterfeit and transaction replay risks, a pair of big holes.

Merchant Recommendations

To prepare for EMV *and* mobile payments, merchants of almost any size are wise to follow the following recommendations:

- ✓ If you're refreshing your terminal estate, buy EMV capable terminals. Spend the extra $10. Make sure you're ready to take "chip and PIN" payments.
- ✓ If mobile commerce and payments are on your mind, and they should be. Purchase terminals that support contact *and* contactless EMV. Look for terminals where the contactless capability is built into the terminal directly, not via an add-on card or external device. That will keep the cost lower. Buy contactless payment capability if you plan to get more than two years (and you do) out of your POS terminals. This positions you for both today's contactless card payments and for the coming era of NFC-based transactions.
- ✓ If you haven't already, consider PIN debit acceptance. Because EMV does support PIN, nearly 100% of EMV terminals include PIN pads. So put those pads, and the lower cost of debit acceptance, to work.
- ✓ Drive a hard bargain. There is going to be heavy competition for the POS upgrade business.

Platform for the Future

EMV does a lot to improve the counterfeit card problem at the point of sale. By reducing the availability of static data, it will decrease, in the long run, card-not-present fraud during e-commerce and mobile commerce transactions. The ability to skim cards goes away. In the short to medium term, as card present fraud becomes more difficult, card not present fraud will increase as fraud migrates to the less secure channel.

As NFC-equipped smartphones roll out in 2012 and beyond, the EMV shift can 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.

With both of these payment technologies arriving at the same time, the smart merchant will plan to support both and take advantage of the security and marketing advantages each offers.

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

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