FUTURE PROOF YOUR BUSINESS

WHITEPAPER

SWIPE

CHIP CARDS

TAP

MOBILE WALLETS

EMV: The New Way To Pay

Future Proof Terminal

CHASE Paymentech

The global payments landscape is constantly evolving and so is the way your customers pay for their purchases. With everything from smart phones to smart cards offering a myriad of payment options, merchants now have to be prepared for today's smart consumer. Technologically savvy and constantly on the go, today's smart consumer is more likely to tap and go than to swipe and sign – and they expect the most advanced options when it comes to protecting their cardholder data. With all these emerging technologies, your point of sale can often become a point of contention without the capability to offer your customers the payment options they want.

Europay®, MasterCard® and Visa® (EMV), commonly referred to as chip technology, is captivating the industry as both a security upgrade and, more recently, a BAU recommendation. And with such a large portion of the international payments landscape already offering this technology, U.S. merchants are taking a proactive approach to understand what EMV is and what it means to their business.

Table of Contents

What is EMV and How Does it Work? *A Technical Perspective*

Already prevalent in Europe, Canada and other high-commerce locations, EMV is the latest technology for point-of-sale terminals that offers you and your customers more security when it comes to proactive prevention of card skimming, counterfeit replication and other types of card-present fraudulent attacks. Each EMV card contains a built-in security chip that utilizes a form of cryptography to authenticate the card, card issuer and the data stored on the card. The chip itself provides three key elements: It can store information, perform processing and provide cryptographic authentication that helps to protect sensitive data. The ability to verify the card's authenticity during each transaction, combined with a PIN or signature requirement to verify the cardholder, results in a higher degree of certainty that the transaction is not a fraudulent one.

Once the transaction has been initiated, there are many steps taken that involve both the card and the terminal before a decision to authorize the transaction can be performed. This includes:

Application Processing

The terminal sends a request to the card, which the card responds to with a list of functions that need to be performed before processing the transaction. When the terminal receives the information from the card, it identifies any processing restrictions that need to be considered. Application usage control ("is the card only permitted for domestic use?") is one example.

When all of the processing checks are complete, the terminal will log the results of the validation, which is then subsequently used by the terminal to form its transaction authorization decision later in the transaction flow.

Offline Data Authentication

Following the previous application processing checks, the terminal also performs data authentication offline, at the terminal level. This is done using secure data that is configured in the chip itself to validate the EMV card. Offline data authentication is one of the benefits that EMV has over magnetic stripe technology, as it allows the terminal to authenticate the card with every transaction and without the need to go online to the issuer for approval.

Cardholder Verification Methods (CVM)

This is a method already in use today whereby both the cardholder and the cardholder's acceptance of a transaction are verified using a signature or PIN.

continued on next page

FUTURE PROOF YOUR BUSINESS

Chase Paymentech's Future Proof terminal enables you to accept EMV and more.

SWIPE Let them swipe. And keep business as usual. Your customers currently pay with debit and credit cards, and that's not going to change anytime soon. You need a terminal that accepts payments as quickly and securely as it always has – and one with the built-in technology to accept any new payments on the horizon.

CHIP CARDS Let them use chip cards. And fight fraud. Referred to under many different names, the chip-enabled payment card has successfully driven down face-to-face fraud around the world – and is making its way into customers' wallets in the U.S. The Future Proof terminal accepts chip cards and significantly reduces your chance of accepting counterfeit cards.

TAP Let them tap. And keep the lines moving. Contactless readers enable customers to wave or tap their bank cards at the point of sale, bypass the signature and go. Behind the scenes, the technology works just like a swipe. This means speedier checkouts and safe, secure transactions for you and your customer.

MOBILE WALLET Let them use their mobile wallets. And keep customers coming back. Contactless readers enable customers to pay with many of the mobile wallets that are becoming available. This technology allows them to pay with a simple wave of their smart phone at the point of sale and will eventually allow you to offer coupons, loyalty discounts and more. This two-way communication is the next step in payments and with the Future Proof terminal, you will be ready for it.

continued from previous page

The CVM that is used to validate a cardholder during an EMV transaction instance is dependent on the CVM(s) the card issuer has configured on their card products and the CVM(s) that the terminal has been configured to support by the acquirer. When a chip card is presented for transaction processing, the card and the terminal will compare mutually supported CVMs. If more than one CVM is mutually supported between the card and the terminal, it is the highest priority mutually supported method that will be used to verify the cardholder for that transaction instance.

Terminal Risk Management

Once the card data has been successfully authenticated, the terminal will initiate various risk analysis functions that include checking the transaction amount against the floor limit defined by the card and the terminal. If the transaction amount exceeds either or both of those floor limits, the transaction will be required to go online for authorization.

Terminal Action Analysis

This is where the terminal evaluates all of the previous validation steps to determine whether the transaction should be approved offline, sent online for issuer authorization or simply declined offline.

If the terminal decides that a transaction should be approved offline, sent online for issuer authorization or declined offline at the terminal level, it will send one of the following requests to the card based on its decision:

- Approve Offline
- Approve Online
- Decline Offline

Card Action Analysis

When the card receives one of the above requests from the terminal, it can respond by accommodating the request, declining the recommended offline approval and returning a decline offline response, or overriding the recommended offline approval request and returning a response to send the transaction online for issuer authorization. Transactions will always go online when either the terminal requests, or the card responds, with a need for online approval.

Transaction Authorization

Depending on the card's decision, the transaction will then be declined offline, approved offline or sent online for issuer approval/decline. When transactions are sent online for issuer authorization, the issuer will respond with a approved/declined message and may optionally include issuer scripts to update the parameters configured on the chip card.

Once authorization is complete, the terminal passes along the issuer online approval to the card so that it can make the final decision to accept the approval or decline the transaction. At this point, if the issuer sent scripts in the transaction response, the card will process the updates to the necessary chip parameters for use in all subsequent transactions.

It is this advanced functionality that makes EMV a more secure alternative to its magnetic stripe counterpart. The drive for a more secure way to pay, however, is what first launched chip technology into the payments landscape and predates the arrival of chip cards in the U.S. by more than 20 years.

The History of EMV

Chip technology actually precedes the delivery of the EMV specifications by more than a decade. According to EMVCo (a separate entity comprised of Visa®, MasterCard®, JCB® and American Express® that is responsible for the management, maintenance and ongoing enhancement of the EMV specifications), the first mass deployment of chip cards for payment by the banking industry was in France. In response to the need to reduce fraud resulting from counterfeit and lost/stolen magnetic stripe cards, the French banks conducted field trials of microprocessor chip cards embedded in plastic bank cards as early as 1984.

Just ten years later, all French credit and debit bank cards carried a chip using a French-developed specification. And as a result of issuing chip cards with PINs, the French were able to reduce fraud due to lost, stolen and counterfeit cards.

Based on the success of the French pilot, the 1990s saw the spread of chip card issuance throughout a number of different markets in Europe. However, due to the fact that these programs were based on domestic market specifications only, the problem soon became the inability to offer anything but magnetic stripe acceptance when the cardholder traveled outside their local market.

The United Kingdom and Japan were considering the migration to chip technology in the early 1990s but both markets were reluctant to continue promoting this new standard when the functionality existed in the local markets only – and thus initiated the global standard for chip acceptance.[1]

EMV versus Magnetic Stripe

While EMV continues its steady migration into the global payments landscape, magnetic stripe cards have been the standard in the U.S. marketplace for some time now. How does EMV technology differ from its predecessor?

There is a significant difference between a magnetic stripe read and an EMV chip transaction. During a magnetic stripe transaction, the card itself functions as no more than a static data storage device that is read by the terminal. The terminal then performs all the processing and applies the rules for payment. More important than this, however, is that magnetic stripe technology does not possess the capability to verify the authenticity of the card itself – is it a counterfeit card being used for fraudulent purchases? This weakens the value of both the PIN or signature cardholder verification methods. This being the case, some merchants will require further proof of identity by asking for the customer's passport or driver's license – predominately with high-volume transactions. But this method, while potentially helpful, is not foolproof as the card may be in the name of the fraudster.

In fact, since the adoption of EMV in the UK alone, counterfeit fraud losses have dropped significantly – by more than 63 percent since 2004.[2] The same study attributes the steep decline to the broader acceptance and usage of chip and PIN cards in the country. And it goes on to say that, when using counterfeit magnetic stripe cards, criminals prefer to transact in the U.S. For the past five years, the U.S. has earned the distinction of the number one country for card fraud committed.[3]

Unlike their magnetic stripe counterparts, EMV cards contain an embedded microprocessor chip that has the ability to encrypt transaction data dynamically for each purchase. And because the transaction information is encoded differently every time, it's harder for criminals to skim or copy useful payment data and use it again for another fraudulent purchase. The technology on the card's chip, in conjunction with a PIN or signature cardholder verification method, provides the type of two-factor authentication necessary to combat the unauthorized use of lost or stolen card data. In this scenario, the cryptogram housed in the chip itself is used to authenticate the card's value (that it is the original card and not a replication), while the PIN required for point-of-sale purchase helps to validate that the person using the card is the actual cardholder.

During an EMV transaction, the chip itself interacts with the terminal and is actually capable of processing information and determining many of the rules for the payment. The terminal then helps to enforce the rules set by the issuer on the chip. It is a mutual decision between the chip and the terminal to determine whether the PIN is prompted or a signature is required to successfully initiate the authorization. If the terminal is unable to provide the services requested by the chip, the issuer has the capability to set rules that will result in the chip declining the transaction request.

The Danger of Skimming – A Business Case for EMV

In the payments industry, the fraudulent practice of duplicating account data by reading the information from the magnetic stripe of one card and replicating a secondary card is called skimming. In a skimming scenario, the fraudster uses a card reader to capture the static account data from the magnetic stripe of one card for later exploitation. Many times, the cardholder is not even aware that any fraudulent activity has occurred until after it is too late and the unauthorized purchases have already shown up on their account statement.

For the most part, skimming devices are undetectable to the untrained eye and fairly cheap to obtain. They can range from simple handheld devices to intrinsic attachments that may include digital cameras to capture PINs. They can also use wireless technology to transmit the captured information (along with other card details) to the attacker remotely. This is one of the most common forms of fraudulent compromise committed at card-present merchants.

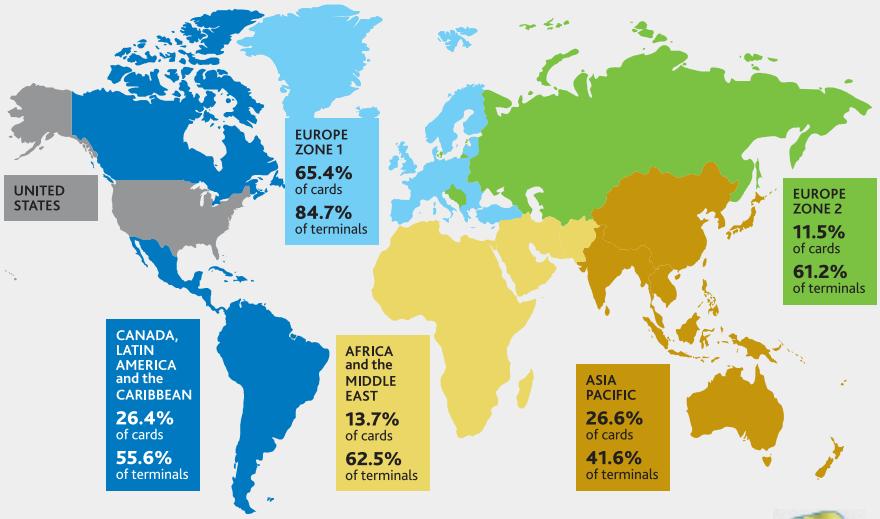
The intention behind this type of fraud is to duplicate the card data in the form of an identical card that can then be used for fraudulent activity such as withdrawing cash directly or initiating high-dollar ecommerce purchases. In fact, Canadian-based Interac Association just recently announced that Canadian dollar losses due to card skimming declined by nearly 40 percent last year when compared to 2010 numbers. The organization credited chip technology for the impressive statistics.

At the forefront of the imminent migration to chip technology is a decrease in chargebacks and lost revenue for merchants. As it stands now, nearly 50 percent of U.S. cardholders have experienced problems in the last four years when using their payment card in Europe.[4] This results in monetary loss, customer frustration and brand compromise. Chargeback reduction is another key benefit of chip payments. The chip itself captures and transmits so much data – including the Customer Verification Method (PIN or signature) and online or offline authentication results. All of these factors combined can result in a significant decrease in chargebacks as fraudulent activity becomes less and less attractive or possible due to the security features offered by these cards.

An additional benefit, and one that makes retailers even more eager about the migration, is the terminal upgrade cycle. With the adoption of EMV chip card acceptance, the new terminal required to enable the upgrade will also foster the integration of contactless payments – a technology that enables payments to be accepted with a tap of the card or a wave of a phone. As the payments landscape has been going mobile for some time now, the addition of these two features will soon be a must for almost any merchant.

From a numbers perspective, it is estimated that the total cost of fraud losses suffered on U.S. credit, debit and prepaid cards is expected to reach $10 billion dollars by 2015.[5] Taking into account the severity of these numbers, it has also been estimated that the cost to migrate the entire U.S. payments landscape to EMV could be recovered within one year – largely attributed to the savings that could be recognized in fraud losses alone.[6]

EMV ADOPTION RATES BY REGION*



*Figures reported as of September 2010 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.

EMVCo

Chase Paymentech was a key player in the Canadian migration to chip-only card-present transactions. The company has been processing chip transactions for the Canadian merchant base since 2008 and was the first Visa and MasterCard approved acquirer to process chip and PIN credit-only transactions in the Canadian region.

The Merchant Perspective

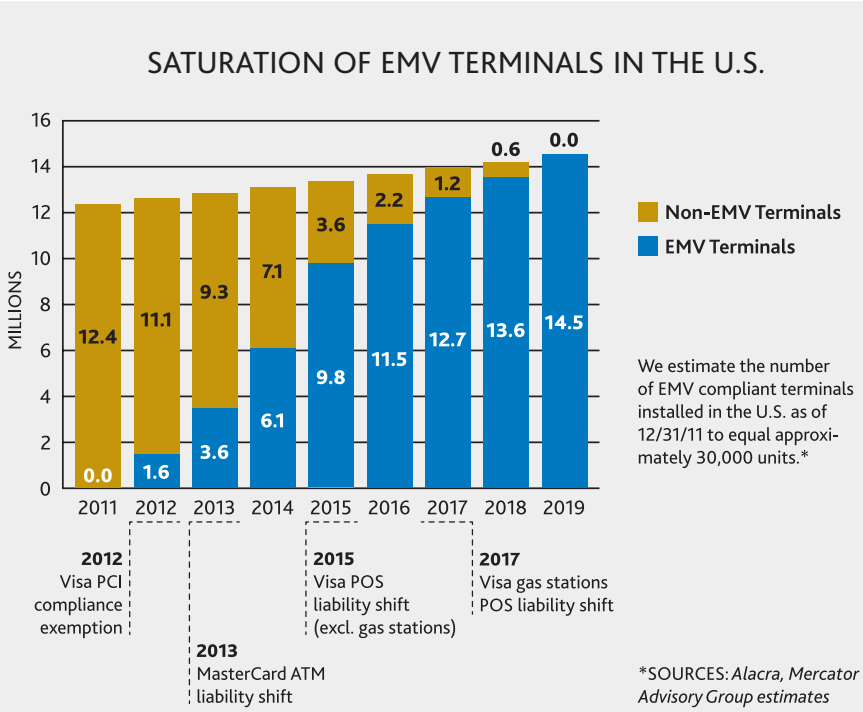
With Canada, Europe and many other surrounding payment landscapes initiating chip technology as a standard in their marketplace, a shift in card-present fraud seems directed toward the U.S. And as ongoing speculation that infiltration to the U.S. region seems imminent, stakeholders everywhere are making a proactive effort to understand what EMV migration could mean to their payments strategy and how it could protect them from this threat.

A positive factor for those U.S. retailers contemplating EMV migration is that the majority of the world has already made the transition. According to EMVCo, the adoption of EMV cards has now reached more than 40 percent around the world – excluding the U.S. – while EMV acceptance device adoption is now at more than 70 percent. The company also reports approximately 1.15 billion EMV payment cards are currently in circulation, with 21.9 million EMV terminals already active worldwide.

Another motivating factor is the liability shift and revised compliance validation requirements being offered as an incentive by Visa. As part of Visa's plan to incent merchants toward chip adoption, Visa will waive Payment Card Industry Data Security Standard (PCI DSS) compliance validation requirements to encourage merchant investment in dual chip and contactless-enabled terminals.

Effective October 1, 2012, Visa will expand their Technology Innovation Program (TIP) to the U.S. As stated by Visa, the TIP will eliminate the mandate that requires eligible merchants to annually validate their compliance with the PCI DSS for any year in which at least 75 percent of the merchant's Visa transactions originate from dual-interface (enabled to support both EMV contact and contactless chip acceptance) terminals.

Additionally, U.S. merchants must meet all of the following criteria to receive the benefits of this program:[7]



- The merchant must have validated PCI DSS compliance within the previous 12 months or provided Visa with a plan of action for achieving compliance.
- It must be verified by the merchant that no sensitive authentication data (as defined in the PCI DSS) is stored anywhere at their location.
- As mentioned previously, at least 75 percent of the merchant's total transaction count must originate from dual-interface, chip-reading device terminals.
- The merchant must not be involved in a breach of cardholder data.

Visa has also announced a liability shift effective October 1, 2015 (petroleum merchants have an effective date of October 1, 2017), for domestic and cross-border counterfeit card-present POS transactions. 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 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.[8]

MasterCard has also introduced their Point-of-Interaction (POI) Roadmap for U.S. merchants. As part of this program, similar to Visa, eligible merchants will no longer be required to annually validate compliance if at least 75 percent of their annual MasterCard and Maestro® transactions are processed through a dual-interface hybrid (enabled to support both EMV contact and contactless chip acceptance) terminal.

continued on next page

continued from previous page

Merchants will be eligible to participate in the MasterCard POI program if they meet the following criteria:[9]

- The merchant must have validated PCI DSS compliance within the previous 12 months or provided MasterCard with a plan of action for achieving compliance.
- It must be verified by the merchant that no sensitive authentication data (as defined in the PCI DSS) is stored anywhere at their location.
- The merchant must not be involved in a breach of cardholder data.
- The merchant has established and annually tests a breach incident response plan in accordance with PCI DSS requirements.
- As mentioned previously, at least 75 percent of the merchant's total transaction count must originate from dual-interface, chip-reading device terminals.

Please note: Regarding the liability shift, MasterCard has taken the same stance as Visa with their Global Chip Liability Program. Both are effective October 1, 2015.

For smaller, Level 4 merchants, a business case for EMV is just as important. As the payments landscape continues to evolve, offering your customers the payment options they want will only grow in importance and necessity when it comes to sustaining your bottom line and growing your business. Not to mention, upgrading to the dual-interface terminals required for EMV acceptance will also equip you to accept mobile payments – another payment option your customers will soon be asking for.

The Issuer Perspective

Issuers choosing to support EMV as a card option for their cardholders will also have to make enhancements to their card-issuing systems. Certain risk parameters, security elements and required chip data will be required to personalize the EMV chip for each individual card issued. And while there are additional costs associated with this, the capability to take advantage of advanced functionality such as post-issuance application loads and the ability to update the card (via the chip housed within) will help issuers justify the cost of issuance.

Functionality that supports the dynamic data within the chip will also have to be added on the issuer side – as well as authorization capability to verify the card and approve or decline the transaction.

And finally, when it comes to global inter-operability, EMV again has the advantage. With the ability to update functionality as needed and with the capability already supported to accept both contactless (RFID and NFC) and EMV chip payment options, chip-enabled terminals have the global reach necessary to both justify the cost to upgrade and promote the necessity for every merchant to have one in their storefront.

Currently in the U.S., JPMorgan Chase, Bank of America, Citibank and Wells Fargo are some of the major banks that have already initiated the EMV standard and have cards already out in the marketplace. And Visa reports that EMV chip implementation has already accelerated on a global scale – with 62 percent of cross-border transactions conducted with a chip card via a chip-enabled terminal.[10]

The Cost to Upgrade

The cost to upgrade magnetic stripe to EMV cards ultimately falls to the issuer. The traditional magnetic stripe card can commonly cost as little as 20 cents each, whereas EMV cards have the potential to cost up to $10, depending on the memory and security features offered by the chip.[11] However, due to the fact that an EMV card can be managed and updated when changes to the card become necessary, it can now be treated as an asset as opposed to an expense.[12] Magnetic stripe cards – which are cheaper to replace than update if the card becomes unusable, have historically been viewed as an expense.

From a hardware perspective, the burden of terminal replacement will typically fall to the merchant. And while these costs can vary greatly between model and supplier, the overall cost of payment and POS devices have been going down. Similarly, it will become increasingly difficult to buy a POS terminal that is not chip compliant. And, as the global population continues to find it necessary to both upgrade and replace terminal technology due to wear and tear and constant advances, many conclude that EMV terminal migration should be considered as an assumed cost of business, rather than a separate cost that needs to be budgeted for.[13] This, of course, is largely attributed to the fact that the investment far outweighs the expense as it is more secure with the capability to significantly reduce fraud resulting from counterfeit card acceptance. Not to mention, with the contactless/NFC functionality already built into the chip-enabled terminals, your checkout process will become faster and more efficient with the ability to accept both tap-and-go and mobile wallet payment options.

Final Thoughts

When building your business case for EMV acceptance, it's important to remember that it is about more than just EMV. Chip-enabled terminals also have the functionality to accept both contactless (RFID and NFC) and EMV chip payments – both of which are payment options that today's smart consumer will be looking for and expect.

As the global standard continues to migrate towards this functionality, merchants everywhere are looking to educate themselves on what this means to their business. A proactive approach to preparing your store-front to accept this new technology includes engaging your processor to determine when they will be ready for chip card processing, soliciting the help of a POS provider to begin assessing what the EMV upgrade will look like for your business and finally, speaking to any third-party software providers (if applicable) to understand their strategy when it comes to EMV compliance. For more information, please visit www.chasepaymentech.com.

1. EMVCo "A Guide to EMV" V1.0, 2011
2. Bankrate.com "US Warms up to EMV Credit Cards," 2012
3. Bankrate.com "US Warms up to EMV Credit Cards," 2012
4. Bellid "Six Myths Preventing EMV Migration in the US," 2010
5. Bellid "Six Myths Preventing EMV Migration in the US," 2010
6. Bellid "Six Myths Preventing EMV Migration in the US," 2010
7. Visa.com
8. Visa.com
9. MasterCard.com
10. Visa.com
11. Bellid "Six Myths Preventing EMV Migration in the US," 2010
12. Bellid "Six Myths Preventing EMV Migration in the US," 2010
13. Bellid "Six Myths Preventing EMV Migration in the US," 2010