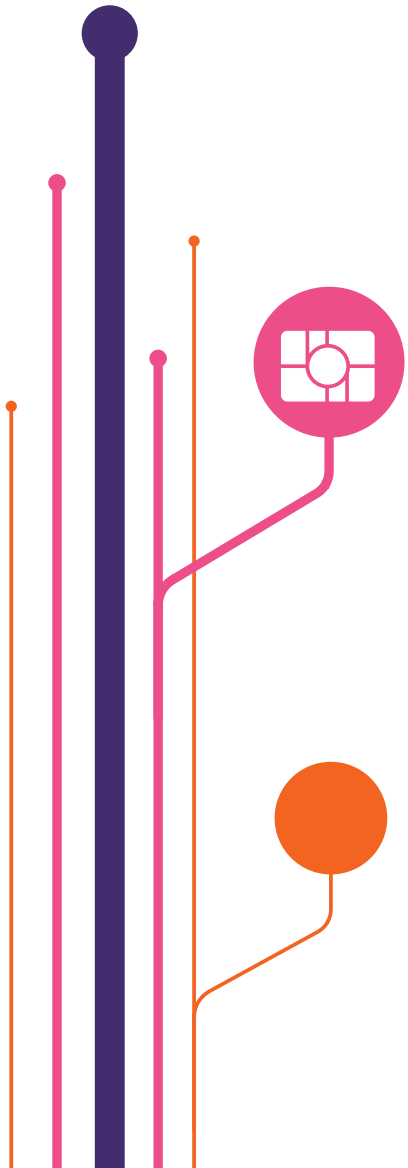
creditcall
The Heart of Payments



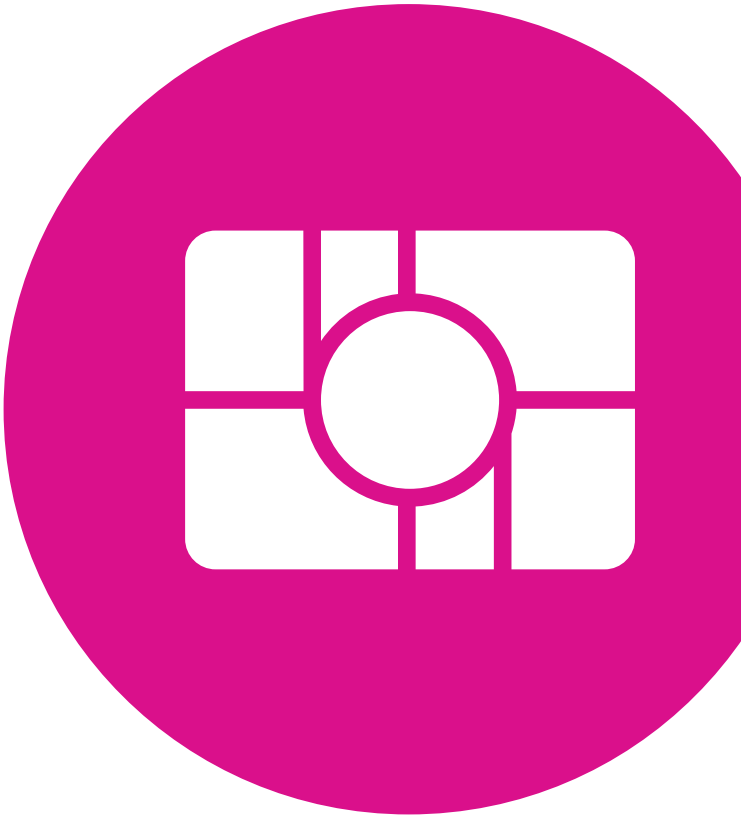
The Ultimate EMV Cheat Sheet:
Everything ISVs, Integrators and VARs Need to Know About EMV Migration

July 2014

“...more than $11 billion was reported stolen due to credit and debit card fraud in 2013, up from $8 billion in 2012.”

Javelin Strategy & Research: 2014 Identity Fraud Report

Contents



Case Study: Target Corporation

On December 18, 2013, security blogger and former journalist for The Washington Post, Brian Krebs, of *Krebs on Security* broke the story that Target had experienced what has since been identified as the largest breach of personal consumer data to date. The news of the breach in payment security swept the nation, and according to Target, some 70 million customers were affected by the breach.

Consumers and merchants alike began to see the security vulnerabilities in magnetic stripe cards and many called for change. In a *recent survey* of 1,011 American adults conducted by Vision Critical 2014, 64 percent were more likely to pay in cash due to recent security breaches and approximately the same number of respondents believed that a credit or debit card with an EMV chip would result in more secure financial transactions.

While the Target breach put the spotlight on payments security in the news and across major retailers throughout America, the breaches did not stop. Krebs *continued uncovering* and reporting on numerous other card breaches in the next nine months, including:

January 11
Neiman Marcus announces that a cybersecurity firm has found a card payment breach, but does not confirm the scale of the breach.

January 16
In light of the **Target** security breach, federal investigators warn retailers and other companies that accept card payments about an advanced piece of malicious software that could be affecting many more stores.

January 23
Neiman Marcus confirms cyber-criminals stole card information for 1.1 million customers who shopped there between July 16 and October 30, 2013.

January 26
Michaels, the country's largest crafts chain and its art and framing subsidiary chain **Aaron Brothers** report "possible fraudulent activity" on some customers' payment cards.

February 2
White Lodging (the manager of 14 hotels, including Marriott, Radisson, Renaissance, Sheraton, Westin and Holiday Inn locations) announces it is investigating a breach involving bars and restaurants at its hotels between March 20 and December 16, 2013.

March 14
Jam and jelly maker **Smucker's** announces a website security breach that jeopardized customers' credit card data.

March 17
Sally Beauty Supply, one of the largest cosmetics retailers, announces a breach of credit card data involving less than 25,000 cards.

March 22
The **California DMV** announces a breach of its online payments system which compromised transactions from August 2, 2013 to January 31, 2014.

April 14
Michaels, Inc. confirms that three million customer credit, debit cards were stolen in Michaels and **Aaron Brothers** breaches between May 2013 and February 2014.

May 14
The **U.S. Postal Service** confirms it is investigating reports of fraudsters installing skimming devices on automated stamp vending machines at Post Office locations across the United States.

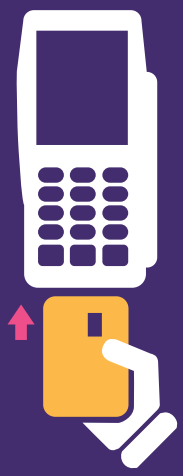
June 12
National food chain, **P.F. Chang's** confirms a security compromise that involves credit and debit card data stolen from some of its restaurants.

Swiping vs. Inserting

How consumer behavior will change

Mag-Stripe Transaction

Chip Card Transaction



While the exact cause of the plethora of breaches is not all exactly the same, they are all illustrations that the U.S. is not only behind the rest of the world in payments technology and security – but is in dire need to upgrade its technology to protect consumer data. To date, many financial institutions have begun laying the framework for issuing Chip cards.

As a result of its very public breach, Target announced it would put copious resources toward migrating its systems to EMV in the coming year. It recently announced its in-store credit/debit card "REDCard" will soon be Chip-enabled. Sam's Club, a Walmart-owned wholesale club, has already begun issuing Chip cards in the U.S., and many speculate that Walmart will continue to invest significant resources in migrating its chains to the EMV standard, in an effort to protect its consumers from similar breaches.

Setting a secure environment:

Security is of utmost importance when dealing with sensitive consumer data. While adopting new security technologies should be a no brainer, it's not always as clear cut as it seems. The widespread adoption of any new technology that affects the interaction between a consumer and a merchant, particularly where there is a financial transaction at stake, must first overcome the 'chicken and egg' scenario – it must be made an option before consumers know they want it, yet some merchants are reluctant to invest until they are sure the market demand will be there.

To ensure a watertight data security and the highest levels of data protection, hardware-based encryption is a must. This takes the PINpad out of the equation, creating a Point-to-Point Encryption (P2PE) zone between the card acceptance point and the payment gateway. Cardholder information is uniquely encrypted from the moment the card is inserted and transmitted, and remains protected as it flows through the rest of the payment processing chain. The information is not decrypted until it reaches the small and highly secured area within a hardware security module (HSM), which means that sensitive data is never visible in its clear text, non-encrypted form outside of the security boundaries of a payment gateway. As the cardholder data is securely encrypted with a key not known to the merchant, the PCI DSS scope of the merchant is significantly reduced.

With a clear, easy way to protect consumer data combined with the persistence of cyber criminals today, being able to secure valuable consumer information is invaluable for merchants.

Introduction

In *"2014 Identity Fraud Report" from Javelin Strategy & Research*, more than $11 billion was reported stolen due to credit and debit card fraud in 2013, up from $8 billion in 2012. While there is not one root cause for concern, the discussion around credit card fraud often ties back to the cards themselves.

Around the globe, countries have adopted EMV technology to combat against fraud. A *report from Europol says 80 percent of fraud outside the European Union*, using EU payment cards, occurs in the U.S.

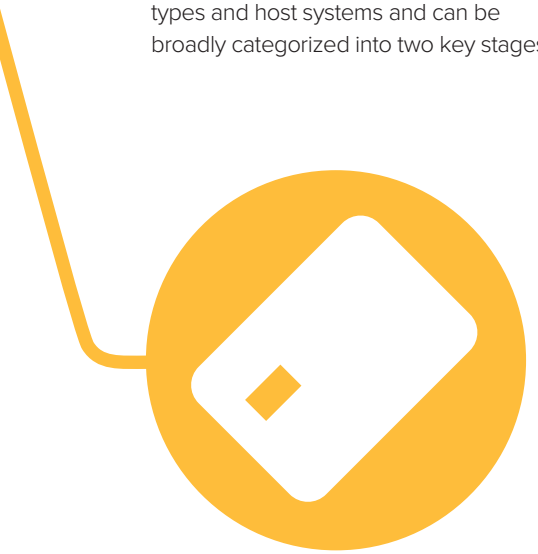
With all eyes turning to the U.S., considering a future where credit card technology leads to the promise of a secure payment environment around the globe, it's surprising that the U.S. hasn't jumped on the EMV bandwagon sooner. The main driver behind this migration is the central goal of worldwide fraud reduction that has been put into place. In order to reach this goal, the migration to EMV must permeate a significant percentage of credit cards in the U.S. in the next two years. This gives the U.S. market a long way to go, sitting at *only 1-5 percent chip card ready in Jan. 2014.*

Despite the low numbers of EMV cards currently in circulation in the U.S., the Oct. 2015 deadline isn't likely to change. President of North America of MasterCard, Chris McWilton, *wrote a letter* to U.S. banks on January 8, 2014. In it, he states, "In the wake of the recent reported merchant data breach, chip technology has gained even greater interest and rightfully so. MasterCard continues to believe that now is the time to migrate to EMV in the U.S." He went on to say, "MasterCard will be keeping its 2015 liability shift dates in place."

Comparing the traditional mag-stripe system to EMV Chip-card technology, the benefits of EMV are exponentially greater; however, these benefits come at a cost. For processors, issuers, merchants and others involved, the massive extent of the U.S. payments ecosystem makes this undertaking a painstakingly time-intensive process.

> **"...MasterCard will be keeping its 2015 liability shift dates in place."**

With the global move from mag-stripe to Chip-enabled cards, the payments industry must tackle multiple moving parts at the same time. These range from hardware and software to transaction types and host systems and can be broadly categorized into two key stages:



Point-of-sale (POS) or payment device hardware and applications:

These require contact and contactless devices and their applications to be implemented and behave correctly according to the EMV specifications. This also extends to mobile POS devices. Where application developers or VARs are developing or integrating EMV Kernels, the application must be implemented according to the EMV functional specifications. The integration of the POS or terminal to the acquirer host system must also be validated.

Acquirer processors:

Organizations must test the integration of the terminal and acquirer processor. This covers the terminal application, user interface, the connection to the acquirer host and the acquirer host system. This is often the most contended and time consuming part of the process which in optimal conditions can take 10-16 weeks. A first certification can take considerably longer.

On the frontline of payments, merchants are looking to their device manufacturers and integrators for the necessary EMV-ready technology. They will face penalties from the fraud liability shift if they do not comply, so many are prioritizing rapid, low-cost solutions that they can easily implement within the timeframes available.

Payment Brand Milestones for U.S. EMV Migration

August 2011
Visa announces its plan to address faster EMV migration in the U.S. via retailer incentives, processing infrastructure acceptance requirements and a counterfeit card liability shift

January 2012
MasterCard announces its U.S. EMV roadmap

March 2012
Discover announces a 2013 mandate to support EMV for acquirers and direct-connect merchants in the U.S., Canada and Mexico

June 2012
American Express announces its U.S. EMV roadmap

October 2012
PCI Audit Relief
If more than 75% of merchant **MasterCard** and **Visa** transactions originate from EMV-compliant contact and contactless POS terminals, the merchant is relieved of audit requirements for PCI compliance (but is still mandated to be PCI compliant)

April 2013
Acquirer Compliance
Acquirers and processors must be enabled to handle full EMV chip data in contact, contactless and mobile transactions

Cross-Border ATM Liability Shift
The existing **MasterCard** EMV liability shift program now applies to inter-regional/cross-border Maestro ATM transactions taking place in the U.S.

October 2013
Account Data Compromise (ADC) Relief
If at least 75% of **MasterCard** transactions originate from EMV-compliant contact and contactless POS terminals, the merchant is relieved of 50% of account data compromise penalties.

PCI DSS Reporting Relief
If more than 75% of merchant **American Express** transactions originate from EMV-compliant contact and contactless POS terminals, the merchant is relieved of PCI Data Security Standard (DSS) reporting requirements

October 2015
Counterfeit Card Liability Shift
Financial institutions and merchants that have made the investment in EMV migration are protected from financial liability for card-present counterfeit fraud losses. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today.

Account Data Compromise Relief
If at least 95% of **MasterCard** transactions originate from EMV-compliant POS terminals, merchants are relieved of 100% of account data compromise penalties

October 2017
Counterfeit Card Liability Shift, Automated Fuel Dispensers
This extends the card-present counterfeit card liability shift to transactions from automated fuel dispensers

12.7m
U.S. EMV enabled cards by Visa

Out with the old, and in with the new, improved, and more secure

The U.S. is quickly approaching an important deadline in the payments landscape. By Oct. 2015 the least compliant party, whether it be card issuers or merchants, will be affected by what is known as the "liability shift". *According to Visa's Counterfeit Liability Shift Policies* "...the party that is the cause of a chip-on-chip transaction not occurring (i.e., either the issuer or the merchant's acquirer) will be financially liable for any resulting card-present counterfeit fraud losses. When a transaction occurs using chip technology, any liability for counterfeit fraud, though unlikely, would follow current Visa Operating Regulations." The liability shift simply means that the least EMV compliant party will be responsible for covering the full cost of any fraudulent transactions experienced as of October 2015. The responsible party could be the merchant, who hasn't upgraded their POS terminal to EMV or it might be the financial institution, who hasn't issued EMV cards.

EMV Ecosystem

Aite Group has predicted that by Oct. 2015, 70 percent of U.S. credit cards, and 41 percent of U.S.-issued debit cards, will be enabled for EMV. Other forecasts slightly contradict this. *Javelin Research* has forecasted that 166 million EMV credit cards will be in circulation in the country by the end of 2015 – which is only about 29 percent of all credit cards they have forecasted that will be in circulation at that time. Javelin forecasts that 105 million debit and prepaid EMV cards will be in circulation – only 17 percent of the expected total. We can use these forecasts to make an educated guess that the reality is likely somewhere in the middle.

Visa and MasterCard have both released recent chip-enabled card information. Simon Hurry, a Senior Business Leader at Visa Inc, responsible for global contactless and contact chip card programs presented at an EMV Migration Forum meeting in May 2014. He announced that Visa has issued 12.7 million EMV cards to date. While MasterCard does not release its card circulation numbers, it has noted that 0.9 percent of its cards in the U.S. are chip-enabled as of Dec. 2013.

Despite what the adoption rates will be by the end of 2015, payments technology in the U.S. is outdated and leaving many consumers at serious risk for card fraud. As we saw in late 2013 and early 2014 with major retailers such as Target, Neiman Marcus and Michaels reporting large scale security breaches, the old way of doing things creates risks for vulnerability. Magnetic stripe cards are easily replicated and used for fraudulent purchases and the current POS systems leave too much room for hackers to steal associated sensitive cardholder data which could open the door for identity theft.

0.9%
U.S. EMV enabled cards by MasterCard

EMV Adoption Across the Globe

According to the latest figures from *EMVCo*, there are 80 countries across the globe in the process of migrating to the EMV standard, many of which are at different stages of their migrations.

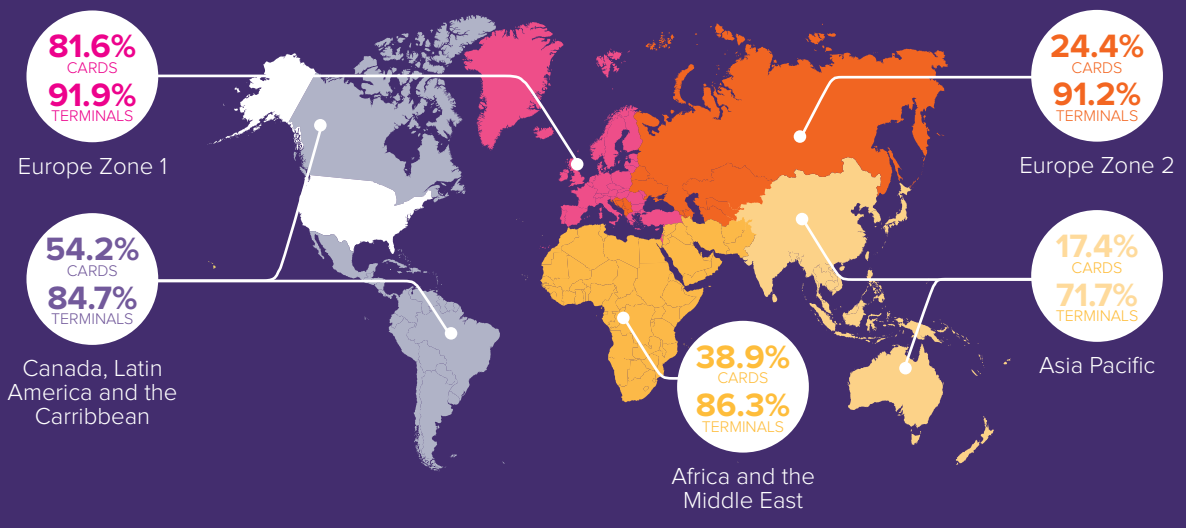
According to EMVCo (Dec. 2013):

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America and the Carribbean	471M	54.2%	7.1M	84.7%
Asia Pacific	942M	17.4%	15.6M	71.7%
Africa & the Middle East	77M	38.9%	699k	86.3%
Europe Zone 1	794M	81.6%	12.2M	99.9%
Europe Zone 2	84M	24.4%	1.4M	91.2%

* Figures reported in Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member institutions globally.

EMV Deployment Map

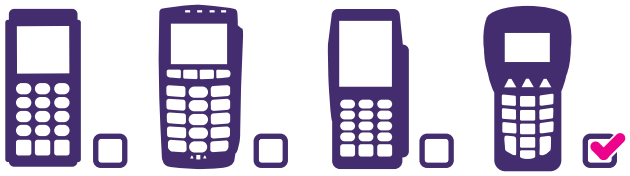


Source: *EMV deployment figures as of Q4 2013*

The Five Steps of Migrating to EMV

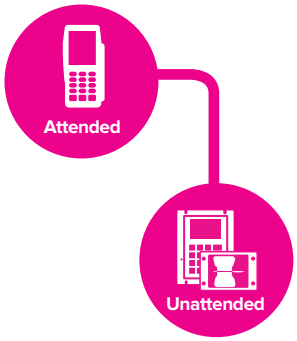
Processors, ISVs, Integrators and VARs often voice five key pain points that they experience when facing the task of migrating their payment systems to EMV for the first time. However, learning from the EMV migrations of other countries and partnering with an EMV-ready payment gateway are two great ways parties involved can be better prepared for an efficient and successful migration to the standard. Most often, these are five key steps that Processors, ISVs, Integrators and VARs voice when getting ready to migrate to the standard:

1 Picking a PINpad and creating a robust driver



Time frame: 3 months

One of the first steps in EMV migration requires selecting a PINpad and creating a reliable and robust driver. But this creates several variables to consider within the decision-making process. For example, what is the environment of the sale—attended or unattended?



If the environment is unattended, there are a few questions merchants will need to answer:

- **What CVMs (Cardholder Verification Methods) should be supported?**
  - Should there be support for foreign CVMs so that foreign visitors feel at home?
- **How important is PIN Debit?**
  - In environments where debit cards are prevalent, PIN will need to be supported, which means PINpads will need to be selected.
  - When deciding on a PINpad, merchants have to consider whether to support Chip and PIN, Chip and Signature or both.

Other variables are to be considered such as cost, form factor and aesthetics. Once those variables are addressed, attention then turns to the driver. Although there are a number of EMV capable PINpads available from the major manufacturers they are often complicated to integrate despite there being huge amounts of documentation and SDKs. The worst case scenario is that the manufacturers will provide a specification of the protocol the PINpad uses to communicate to the outside world. It is then the responsibility of the integrator to implement this protocol in its entirety. To do this effectively, the integrator must invest time in learning about EMV (for example Application Selection, Data Authentication, Online

> **In mature EMV markets, a typical certification cycle can take between 10-16 weeks.**

Processing and Issuer Script Processing), transaction flows, transaction logic and of course exception handling when an inevitable error occurs in the transaction. This is further complicated by typically poor support from the manufacturer, inconsistencies in the documentation and undocumented PINpad behavior.

The more enlightened PINpad manufacturers provide an SDK rather than a protocol document. This is definitely a step forward. However these SDKs are often over-complicated by the bloated number of functions that the PINpad supports that are often unrelated to EMV. They also require a deeper understanding of EMV, so while they solve some of the integration issues, they do not solve the time investment in understanding EMV. Another problem with this approach is that often the SDKs are not always updated frequently so bugs can go unaddressed for some time.

Manufacturers often suffer from inconsistent support which will be further exacerbated by the sheer volume of integrators who will be asking the same integration and support questions. Most manufacturers are also not set up to support developers and are unfamiliar with the diverse range of development environments and methodologies that exist today.

2 Updating processor interfaces to support EMV messaging

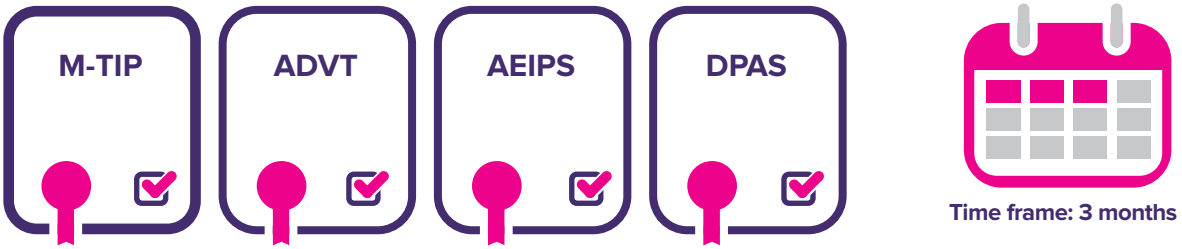
Time frame: 6 months

In the U.S., most merchants and ISVs have a magnetic stripe interface to their processing partners. Each of these interfaces need to be individually updated to support the different transaction flows of EMV and the additional data fields required by EMV. This complicated task is a significantly more difficult undertaking than creating a magnetic stripe interface, let alone creating multiple interfaces for different processors.

As these interfaces were often created some time ago, a common scenario is that the original developer who developed the interface has left the organization. A decision to develop a new interface from scratch or even to update an existing one is no small undertaking. It is also likely that many different parties will be attempting the same exercise which will place strain on the ability of the Processor to support the endeavor. Developing these interfaces is further complicated by the significant differences between magnetic stripe vs. EMV terminology and process flow. Updating a processor interface also assumes that the integrator has a deep understanding of EMV and EMV transaction flows. It is also questionable whether the processors will have scaled their integration support sufficiently to cope with the mass of other integrators who will be following the same path. Therefore, as creating and testing the interfaces is an iterative process, it is crucial to secure timely support from the processor.

“Pre-certified solutions significantly reduce the amount of time and effort to get up and running.”

3 M-TIP/ADVT/AEIPS/DPAS certifications



Time frame: 3 months

Once an integrator has updated their processor interface, they face the complex task of end to end testing and certification. Most merchants underestimate the time required to compete the layers of brand certification required before an EMV solution can go live. In mature EMV markets, a typical certification cycle can take between 10-16 weeks and it often requires expensive test tools and cards. If merchants are amply prepared and budget enough time for M-TIP, ADVT, D-PAS and AEIPS certifications, the migration process is made much easier.

Certification is not a one-off process: it must be repeated every three years when the EMV Kernel certification on the PINpad expires. The process involves every single PINpad and Processor combination. For example, if an integrator needs to support three different PINpads and three different Processors, then it will take 144 weeks to certify these combinations every three years. Processors are looking at truncating these timescales, but it is unclear at this time how this will be achieved. There are also a number of factors that may require additional rounds of certification in the future on the same solution beyond repeating the process every time the EMV Level 2 certification expires.

Additionally, it is advisable to allow extra time for a first certification for various reasons - documentation interpretation errors, unforeseen technical issues and availability of test hosts. As many merchants migrate to EMV simultaneously, Processors may not have as much time to support the myriad of different certifications. It is unclear at the moment whether the Processors in the U.S. will be able to cope with the volume of certifications before the Oct. 2015 Liability Shift.

4 Terminal Management System

Once a merchant has successfully updated their application to support EMV, they must address how they plan to manage the data elements required by EMV, particularly the firmware on their new PINpads. Whereas regular manual updates can be quite tricky, Terminal Management Systems can consistently check for updates and automatically install them. This is particularly helpful for large estates of PINpads.

Time frame: 3 months

A PINpad is essentially an embedded platform that runs its own complex software stack. As with any software stack, it requires updates to keep the stack compliant with current versions of the EMV standard. Security vulnerability patches or general bug fixes also need to find their way to the PINpad. Therefore, all EMV-enabled solutions will require frequent data updates to cover off new data elements such as CA Public Keys and Data Object Lists which can change periodically. Having the correct CA Public Key is critical to the cryptographic operations of EMV. This is often an overlooked part of a successful migration, even in countries where EMV is well-established.

Without a TMS platform, an integrator runs the real risk of PINpads that do not have current software or the latest configuration. Regardless, the certification status of the core EMV software that resides on the PINpad will expire every three years. While this effectively ensures all PINpads are updated on a regular schedule, three years is a significant gap in the exploitative hacker world. When vulnerabilities are exploited in cases where updates have not been regularly made, it will lead to compliance issues and ultimately card brand fines that will be passed down to Merchants by the Processors. It is essential that any EMV solution has access to a TMS platform for efficient and timely deployment of updates.

5 Certifying for PCI P2PE

Although not directly related to EMV, strong transaction security is a prudent security counter measure. PCI point-to-point encryption (P2PE) protects sensitive credit and debit card data from the point in time it is inserted into a card reader or PINpad, while in transit, and all the way to the payment processor. Most PINpads provide the basic functionality to support P2PE, but to implement it fully requires significant effort. P2PE ensures solutions meet requirements for card data protection and de-scopes some of the problematic areas of PCI DSS. Some of the benefits P2PE offers include:

- A considerable reduction of merchant PCI DSS scope,
- Protection of card data in transit and at rest,
- Terminal (PED) and PSP (Gateway) combinations can be P2PE pre-certified and are listed as a pre-certified solution by PCI SCC on its website.

As with many PCI standards, PCI P2PE is detailed, security-focused and requires a significant effort to become compliant. To implement P2PE correctly requires extensive knowledge of cryptography and how it is applied to transactions. It also requires a significant investment of time and money in dedicated hardware (Hardware Security Modules) that serve to decrypt cardholder data that has been encrypted within the PINpad. It also requires new policies and procedures to manage the cryptographic keys that are injected into each and every PINpad. Pre-certified solutions significantly reduce the amount of time and effort to get up and running.

Time frame: 6 months

Solutions

The five most common pain points that Processors, ISVs, Integrators and VARs have voiced are essential to consider and develop an understanding of, when evaluating the options available for an effective EMV migration to take place. When considering all of the changes outlined earlier, the following solutions are viable:

In-house development

The in-house approach is highly desirable for many brands who want to build their own EMV technology stack. However, this approach requires a significant amount of expertise and time. Considering the entire process can take anywhere between 12 to 24 months, in-house development may not be the best approach for some. Once built, PINpad updates and certification maintenance requires ongoing time and budget resource.

Pre-certified solution

Elsewhere in the world, pre-certified solutions have offered an easier route to EMV migration. The two common technology solutions are:

- **Fat tech stack on PINpad** which is a limited embedded device,
- **Shared tech stack between POS and PINpad**, a scenario that *Creditcall's ChipDNA* supports.

Creditcall's solution for adding EMV transaction processing to Windows or a Linux-based POS is called ChipDNA. The ChipDNA API provides a simple and rapid way to remove the complexities of EMV compliance and the arduous, lengthy EMV certification regime.

ChipDNA manages the PINpad, PINpad User Interface, EMV compliant transaction flow and secure communication to the Creditcall EMV Ready Payment Gateway. Once the transaction is complete, ChipDNA provides an approved, declined or error state plus any receipting information required.

ChipDNA solves the EMV migration dilemma faced by ISVs and integrators by addressing the five major steps of EMV:

1. Developing a robust PINpad driver that works time after time.
2. Re-engineering existing processor protocols to support EMV commands and binary data.
3. The time consuming and costly M-TIP, ADVT, AEIPS and DPAS certifications that are mandated by card brands.
4. The creation of a Terminal Management System (TMS) to keep PINpad firmware and EMV configuration up to date.
5. Strong transaction and cardholder data security using Point-to-Point Encryption (P2PE) and tokenization.

With ChipDNA, you can be EMV-ready without the expensive and complicated EMV test tools or cards, without time-consuming, complicated processor certifications and with strong transaction security and cardholder data protection by utilizing P2PE and Tokenization.

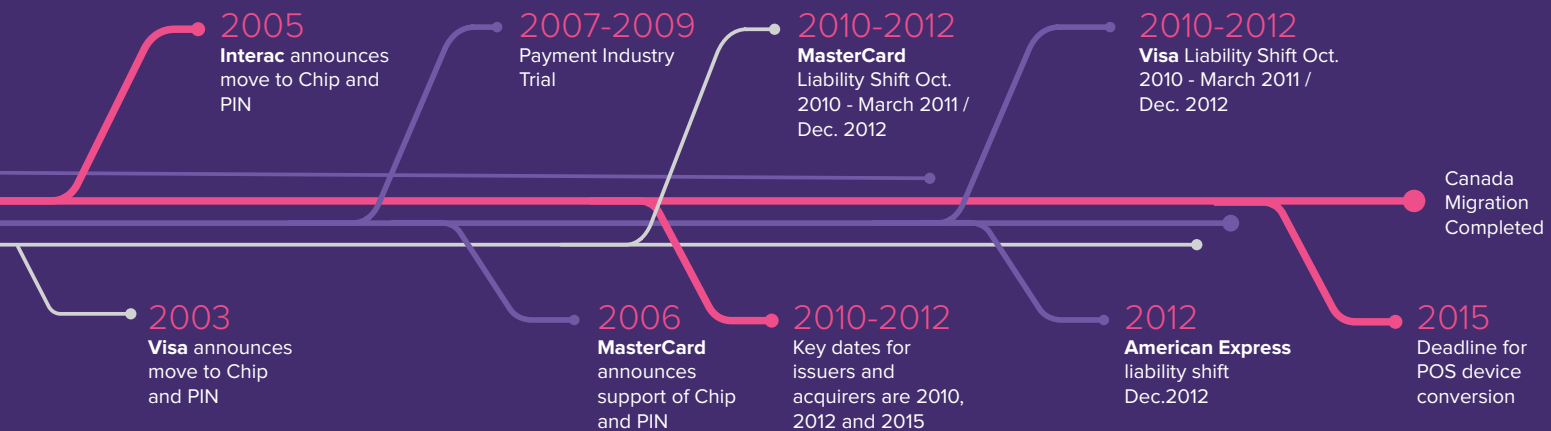
For more information visit
www.creditcall.com/ChipDNA

Case Study: Canada's EMV Migration

As the U.S. is in the primary phases of migrating to EMV, it benefits from being able to look to other countries that have adopted the technology. Canada is on its way to completing its EMV migration by next year and as it nears the end of its migration, it offers some great insights on fraud reduction.

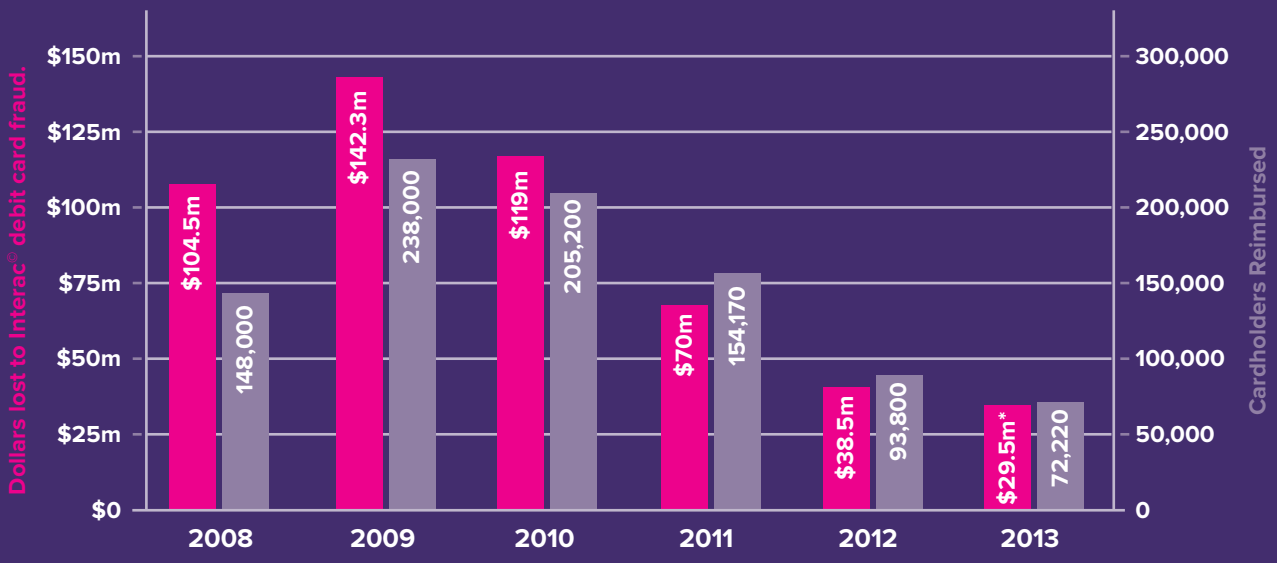
In June of 2003, Visa Canada announced that it would begin migrating all Visa Cards to EMV Chip Cards starting in October 2004. That announcement spurred Canada's payment body, Interac Canada, in 2005 to make the migration from magnetic stripe credit and debit cards to EMV standards. While countries in many parts of the world were migrating to EMV at that time, EMV standards were essentially non-existent in North America. Interac made the decision to pursue a migration after a fraud trend analysis suggested significant vulnerabilities in Canada's payment infrastructure. Much like how the U.S. has put together its timetable for EMV migration, so did Canada:

Chip Migration Timeline in Canada



With Canada's EMV migration in its last year, Interac's goal is for all POS devices to accept Chip and PIN by 2015. However, Canada is already seeing a significant benefit from the majority of its merchants who have migrated to EMV. Interac recently released updates on the reduction in credit and debit card fraud losses due to EMV in Canada. *According to Interac*, Debit card fraud losses are at a record low, decreasing to $29.5 million in 2013 from a high of $142 million in 2009. Notably, only 25 percent of losses in 2013, or $7.3 million, are the result of fraud exploitation within Canada.

Interac Fraud Data 2008-2013



*** Only 25% of losses in 2013, or $7.3 million, are the result of fraud exploitation within Canada.**
Source: *http://www.interac.ca/en/stat-fraud*

Canada's large decline in the skimming of credit card data is owed to the country's adoption of EMV chip cards and a continued investment in fraud detection.

The U.S. can also look forward to reduced fraud throughout the course of its own migration to EMV. Because EMV is already prevalent worldwide, most countries that Americans travel to will be able to accept their new EMV cards. Heightened security and more convenient payments on a global scale are just a few of the reasons why the U.S. has so much to gain from its migration to EMV.

Useful Links

EMVCo
http://www.emvco.com

EMV Connection
http://www.emv-connection.com

EMV Canada
http://www.emvcanada.com

EMV USA
http://www.emv-usa.com

Interac Canada
http://www.interac.ca

MasterCard EMV
http://www.mastercard.us/mchip-emv.html

PCI Security Standards
https://www.pcisecuritystandards.org

Smart Card Alliance
http://www.smartcardalliance.org/pages/activities-emv-migration-forum

The UK Cards Association
http://www.theukcardsassociation.org.uk/welcome/index.asp

UK Payments Administration
http://www.ukpayments.org.uk

UK Chip and PIN
http://www.chipandpin.co.uk

About Creditcall

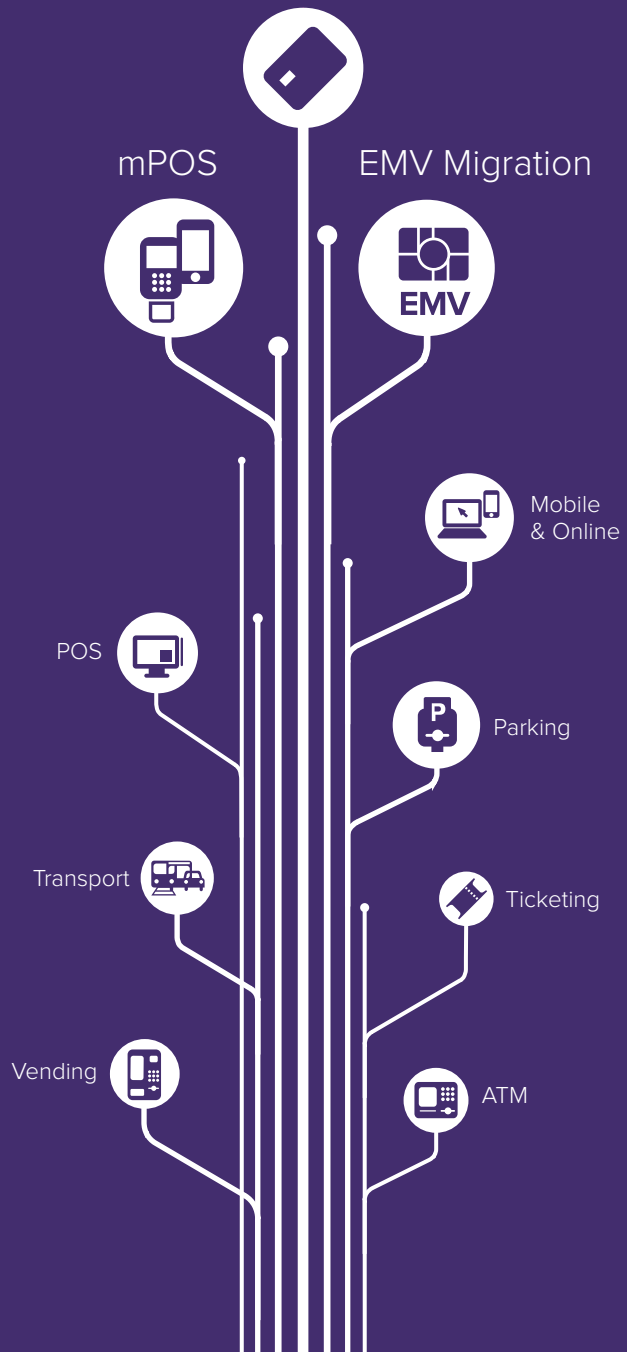
Creditcall makes card acceptance simple from any device, anywhere. Whether attended, unattended, online or mobile payments, our award-winning EMV-ready payment gateway and EMV Migration solutions are at the very heart of our clients' businesses, ensuring payments flow – all day, every day.

Founded in 1996 and with over 14 years of EMV experience, Creditcall has a proven track record in providing payment gateway services and offers EMV Migration solutions that are tried and tested.

- Our EMV Migration solution, ChipDNA, is a rapid EMV Migration SDK for Windows, Linux, iOS and Android. It greatly helps ISVs transition from older magnetic stripe technology to EMV and Chip technology. ChipDNA is the easiest and most cost effective way of adding EMV payment functionality into an attended or unattended Point of Sale (POS) application.
- We were the first EMV-ready Payment Gateway in the U.S., and completed our EMV certification in April 2014.
- Our Chip-based EMV Level 1 and EMV Level 2 Kernel software is used globally in contact and contactless environments such as ATMs, mPOS, card readers, PINpads and other POS devices.
- We are the first EMV-compliant mPOS solution to allow businesses accept Chip and PIN cards 'on the go' via smartphones and tablets.

Millions of users and billions of transactions depend on Creditcall EMV technology each and every day. Creditcall works collaboratively with companies across Europe, North and South America, South Africa and Asia-Pacific to deliver business-critical payment solutions. Clients include ATOS, DHL, Elavon, Hilton Hotels & Resorts, Toyota, Wayne (a GE Company) and Westfield.

Creditcall – The Heart of Payments.



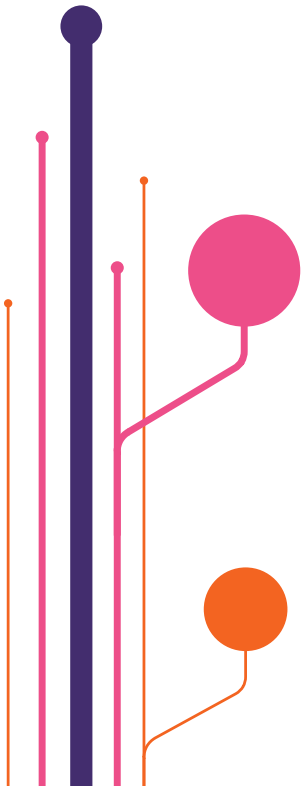
Regional Offices

Creditcall Europe
Merchants House North, Wapping Road, Bristol, BS1 4RW, United Kingdom
T: +44 (0)117 930 4455
E: *hello@creditcall.com*
W: *www.creditcall.com*

Registered No: 3295353.
VAT Registered No: 713 0076 80.

Creditcall North America
1133 Broadway, Suite 706, New York, NY 10010, USA
T: +1 (800) 868 1832
E: *hello@creditcall.com*
W: *www.creditcall.com*

For more white papers from Creditcall, visit *www.creditcall.com/white-papers*



creditcall
The Heart of Payments