EMV | THE NEXT TWELVE MONTHS

INDUSTRY PERSPECTIVES AND IMPLEMENTATION IMPERATIVES

AN EBOOK EDITED BY PYMNTS.COM

CONTRIBUTORS

- GEMALTO
- OBERTHUR
- DATACARD
- CREDITCALL

PYMNTS.com

CONTENTS

OF BLACK SWANS, EMV AND THE LIABILITY SHIFT EBOOK INTRODUCTION

We talk a lot about "black swans" in payments – those events that seem to come out of nowhere yet change everything. Most people in payments spoke of Apple as being the industry's "black swan" - whose entre into payments could change the landscape permanently.

I disagree. While the launch of Apple Pay has the potential to change everything in payments – or at least become the catalyst for change - everyone knew that Apple would get into payments eventually. And, although given Apple's penchant for secrecy, no one knew just when or how they'd do it, it was not unexpected.

So, that brings us to the real black swan in payments – and perhaps the most significant one we've seen in recent memory: The Target breach.

Until that happened, most merchants in the US remained unconvinced that EMV was a priority that needed their attention. Fraud at the physical point of sale wasn't their biggest concern, and the move to mobile and cloud-based mobile payments schemes, seemed a much higher deal and more worthy of their time and investment.

That all changed when word got out about the Target breach and the fact that the compromise happened at the physical point of sale. As everyone knows well in payments, their sales plummeted, their reputational losses mounted, their core customers left them in droves and sales plummeted. What we learned about the Target breach, and we've studied the consumer data, is that consumers really didn't change their payments habits post-breach, but they did change their merchant preferences. They stopped going to Target.

So, quite naturally, embracing EMV was one of the first things that Target did to try to rebuild consumer confidence, despite the fact that everyone in the business knew that EMV would have not prevented the breach. But it was something that Target could show to its consumers and its Board that it was taking steps to make the point of sale - and cardholder data – more secure.

And, that was all that was needed to get CEOs and Boards of major retailers to follow suit, a move that was made that much easier – and even accelerated - in the wake of the succession of POS breaches that followed in the subsequent months.

So, now here we are in the US, about a year away from the date when merchants will either be EMV compliant or risk the liability shift that makes them responsible for losses in the event of a compromise at the point of sale.

Merchants, large and small, are now scrambling to put those plans in place.

This eBook is a collection of writings on the topic of EMV from those who have been on the forefront of implementing EMV in other parts of the world. As one of the contributors stated, the delay on the part of the US isn't a bad thing – it provides a rich set of learnings and best practices for merchants in this market to follow. We are sharing them with you in this volume.

One of those learnings is that EMV is not the lone tactic in the fight against the fraudsters, who always seem one step ahead. As every other country has experienced, a move to EMV means a move to online for the fraudsters. Just as famed bank robber, Willie Sutton said, when asked why he robbed banks ("it's where the money is,") the cyber criminals, follow the money, too. Cybercrime, unfortunately, is a huge global business – simply shutting down one channel is a sure way to get them focused on others where there could be vulnerabilities. EMV is the first step to a multi-layered approach to protecting cardholder data at the moment it is swiped and as it is processed. We have some thoughts on what those layers should be and the sequence for getting them deployed.

The shift to EMV also raises a lot of questions. Are small merchants at risk – and should they really bother to deploy EMV, especially when some sectors, like restaurants, might want to leapfrog it entirely and go right to mobile? How does the move to mobile impact EMV and vice versa? Does it delay it or it is an on ramp? What is the relationship between EMV and Apple Pay and its contactless/NFC protocol – are they mutually exclusive? Will the deployment of EMV accelerate the move to NFC? And, suppose a merchant hasn't started the migration to EMV yet – is it too late to make the deadline given the constraints on the processors to certify the backlog of merchants now building in the queue?

These are all questions that are what will keep all of us in payments pretty busy, and pretty busy debating over the next year. We're proud to bring you this collection of insights from those who know it best.

If you have something to add, or, after reading this, have more questions than answers, we hope you'll drop us a **note**. We'll do our best to get you the answers you need on what has become a mission-critical topic for our industry.

Thank you, as always for your support - and happy reading!

Kind regards,

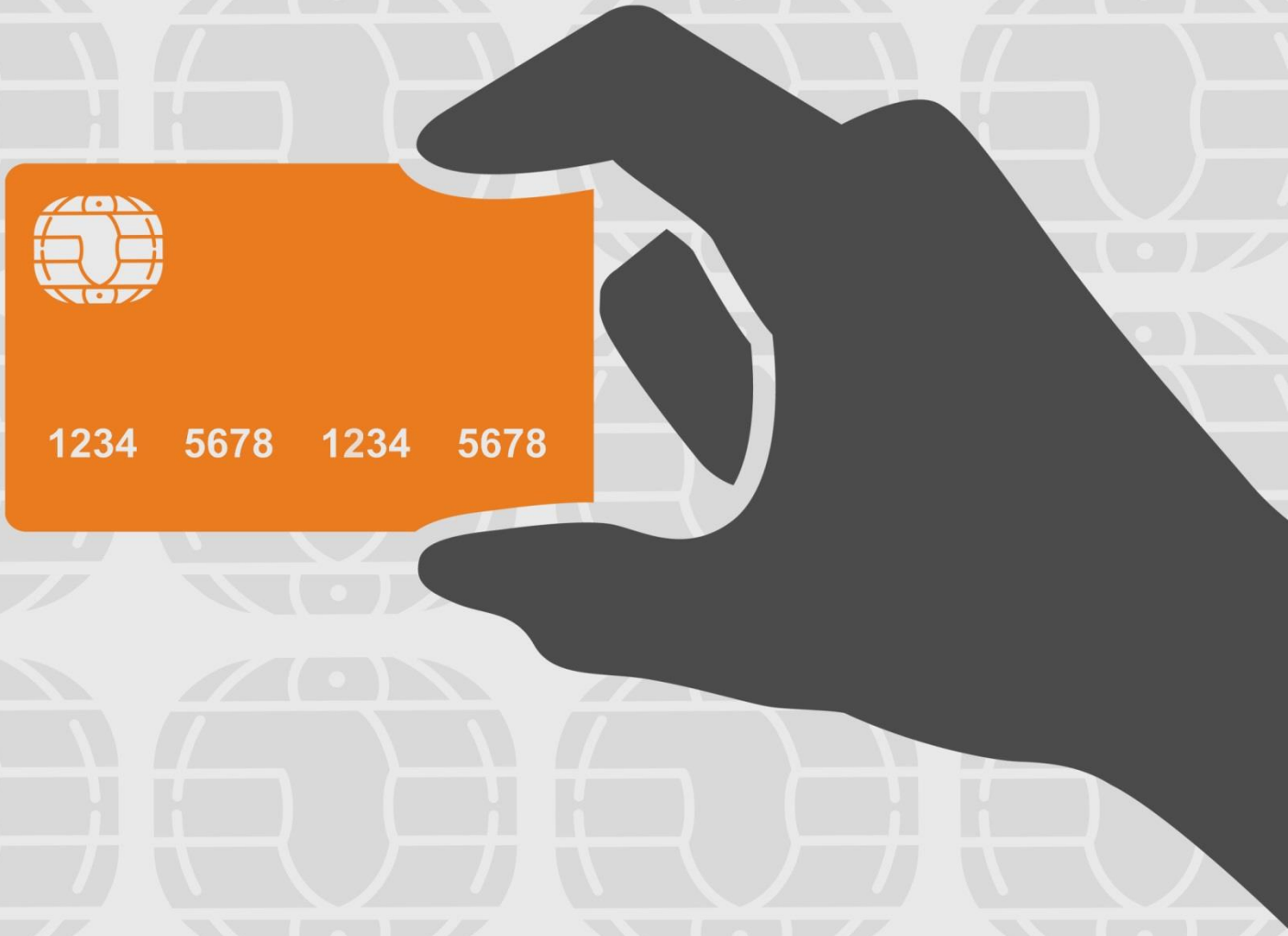
Karen Webster

Karen Webster
CEO | Market Platform Dynamics
President | PYMNTS.com

THE COUNTDOWN TO EMV

WHAT TO EXPECT FROM EMV UBIQUITY, THE UPSIDE FOR CONTACTLESS PAYMENTS, AND BEST PRACTICES

BY PHILIPPE BENITEZ, VP MARKETING, MOBILE FINANCIAL SERVICES, NORTH AMERICA



gemalto
security to be free

INTRODUCTION

The U.S. is one of the last holdouts, where magnetic stripe remains king. With less than a year remaining to migrate from magnetic stripe to chip technology, the industry is in a busy transition. Fraudsters are also busy. Large scale breaches are a weekly occurrence in the news. According to Aite Group, over the past several years credit and debit card fraud has been on the rise reaching roughly 10 cents out of every $100 transacted. Partially due to the lag in the adoption of EMV, the United States has had a 70% increase in credit card fraud since 2007 while the U.K has seen an 80% decrease after migrating to EMV.

Credit card fraud increased in the U.S. by 70% since 2007 while the U.K. decreased by 80%

Source: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Payments-Transformation-EMV.pdf

EMV MITIGATES THE RISK OF FRAUD

Using the example of the recent merchant breaches, EMV technology would have made the data worthless on the counterfeit card market. Reducing the monetary value of the stolen information minimizes the incentives for fraudsters to attempt such complex attacks. EMV also provides better protection for cardholders at the point-of-sale by eliminating the opportunity for card skimming, where a magnetic stripe is scanned without the cardholder's consent. As the U.S. is one of the last countries to migrate, there has been a higher rate of card transplant fraud, where stolen card information from EMV markets is printed onto a magnetic stripe card and used in non-EMV markets. The U.S. has a lot to look forward to since other regions in the world have been tremendously successful in preventing fraud as well as maintaining the reduction ratios.

EMV IS THE DRIVING FORCE FOR MOBILE, CONTACTLESS AND WEARABLES

As EMV becomes ubiquitous in the U.S., the timing has never been better for contactless payments because issuers can now leverage two important benefits of the EMV migration: The momentum of consumers changing their payment experience at the point-of-sale (POS), and the new infrastructure that merchants are currently installing. For the first time in U.S. history, contactless POS terminals are becoming standard, which means inevitably all forms of contactless payments can be accepted.

FOUNDATION FOR FUTURE ADVANCED PAYMENTS AND MOBILE CONVERGENCE

Javelin Strategy estimates that by the end of 2015, more than half (60%) of retail locations will be EMV capable. Almost all POS terminals sold in America today are equipped to accept contactless, wearable and mobile EMV payments. It takes a small, incremental investment to load the software needed to support the contactless technology, but can reap large rewards for merchants and issuers. In other words, the U.S. migrating to EMV devices supporting EMV contact and contactless would bring mobile payment acceptance as a bonus.

Contactless payments already have proven benefits: shorter time at checkout, convenience and less cash on hand. According to Deloitte, contactless transactions can be up to 25% faster than paying with cash. The speed and ease of the transaction can reduce time spent at the POS by 77%, while merchants benefit from a higher turnover rate. The move to contactless in the U.K is estimated to have driven almost £1.4 billion in additional revenue for merchants.

Source: http://www.simon-kucher.com/sites/default/files/Contactless%20payments%20worth%20more%20than%201bn%20GPB%20to%20retailers.pdf

EMV IS THE DRIVING FORCE FOR MOBILE, CONTACTLESS AND WEARABLES

A recent Kelton survey found that 9 out of 10 consumers are concerned about security making it a significant barrier to widespread adoption. Using the underlying technology of EMV, consumers will be able to securely pay with plastic, mobile and even wearables bringing not only benefits to users but to merchants and issuers too. While the contactless and mobile market is already growing, the new wearable trend is poised to take off. Recent Markets to Markets research estimates the value of wearables to reach $11.61 billion by 2020.

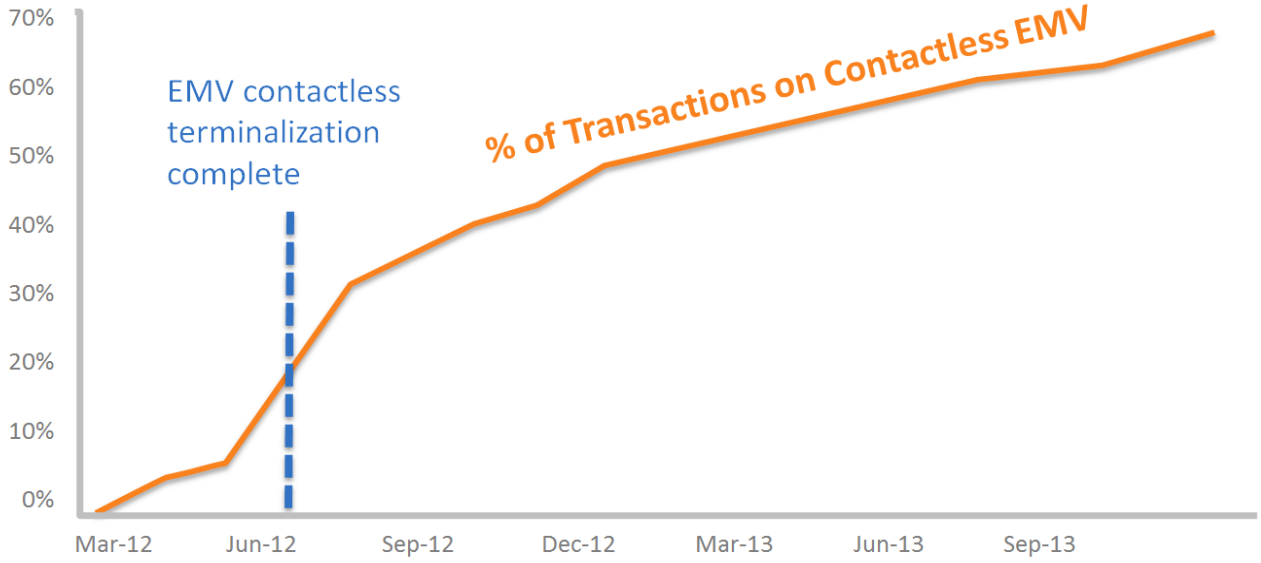
The timing has never been better for contactless payments because issuers can now leverage two important benefits of EMV migration: The momentum of consumers changing their payment card experiences at the POS, and the new infrastructure that merchants are currently installing.

Leading financial institutions like CaixaBank and Barclays both recently announced they are already issuing wearable gadgets to their customers. These novel wearable banking devices, certified by the international payment schemes, give customers the freedom and security to pay everywhere they go, without the need to carry a purse or wallet. In fast-track environments, merchants, festival goers and transport users handle less cash for fluidity and a digital trail of the transaction. Barclays, for example, is seeing continuous growth in their number of contactless transactions, which currently stands at 300,000 a month. The momentum is going to carry over to the U.S. as other EMV-markets transition from standard contact payments towards more innovative and faster ways to pay.

At the bottom of the following chart is a list of countries in which contactless has become “mainstream,” or accounts for more than 10 percent of all transactions. Those in white are countries that started EMV on contact and then moved contactless, and those in orange are countries that leapfrogged contact EMV and went primarily contactless.

Source: http://www.thatsemv.com/downloads/Gemalto_EMV_Success_Stories.pdf

CONSUMERS WOULD RATHER TAP AND GO THAN DIP AND WAIT



More than 10% of transactions are contactless in:

Australia	**Canada**	Poland	**Singapore**
Hong Kong	New Zealand	**Taiwan**	Czech Republic

% of Visa & MasterCard transactions using contactless Source: Visa, MasterCard

BEST PRACTICES FOR MIGRATION

Gemalto has collected best practices for migrating to EMV from hundreds of deployments worldwide.

1) Consult with EMV experts

When building a house it is standard to consult with an architect, builder, or plumber. Deploying EMV is similar; understanding the process, certifications and necessary resources before launching the program is vital. Doing so brings financial benefits and faster time-to-market by helping issuers avoid common pitfalls.

2) Plan a timeline

After consulting with EMV experts, planning out the deployment timeline will help address all the moving parts. Depending on your various card portfolios and reissuance cycles, we recommend a full six months for the card migration. Based on its security features, the personalization of EMV cards is much more complex than that of magnetic stripe. The certified, mandatory process to personalize card data for EMV covers the entire supply chain from the infrastructure, organization, equipment and even the operators. As billions of cards are being migrated in the U.S., it is best to consider additional time for personalization and issuance in your timeline.

BEST PRACTICES FOR MIGRATION

3) Collaboration is key
EMV brings together different roles within a financial institution that previously may not have overlapped. We have seen that opening up dialogue between experts from innovation to marketing within a company makes deployment a much smoother one.

4) Consider the artwork
While a lot of focus and attention is given to technical requirement, card graphics can be an afterthought. Introducing a chip onto the front of a card changes the existing artwork layout. It is important to reconfigure your branding, positioning and graphics to adapt to the changing real estate on the new EMV card.

5) Communicate with your customers
We have seen an EMV migration as the perfect opportunity for the issuer to connect with their customers by providing awareness and education on how to use their secure chip card as well as the security benefits the cardholder will have in the future. One example is the "Do you speak EMV" approach which informs the cardholder on the new terminology and what will change at the point-of-sale.

Do you speak EMV?

Dip/Dipping – Instead of swiping a card, customers insert an EMV card into the POS terminal, much like an ATM. Inserting the card and removing it is called "dipping."

"Tap & Pay" or Wave – When using a contactless card, there is no dipping. The card is "tapped" or "waved" against the POS terminal. One quick tap establishes connection and verifies authorization.

Chip & PIN or Chip & Signature– EMV payment cards are commonly referred to as "chip & pin" cards because the chip card is often coupled with a PIN code for advanced security. However, not all cards need to be associated with a pin number. It's possible to have "chip & signature" cards, too.

Dynamic Data or Dynamic code – EMV cards generate a "dynamic code," a security code that changes for each transaction. That way, if a card is copied or compromised, the data cannot be used to make multiple transactions. In contrast, the data transmitted by magnetic stripe cards never changes and, once compromised, can be used over and over for countless fraudulent transactions.

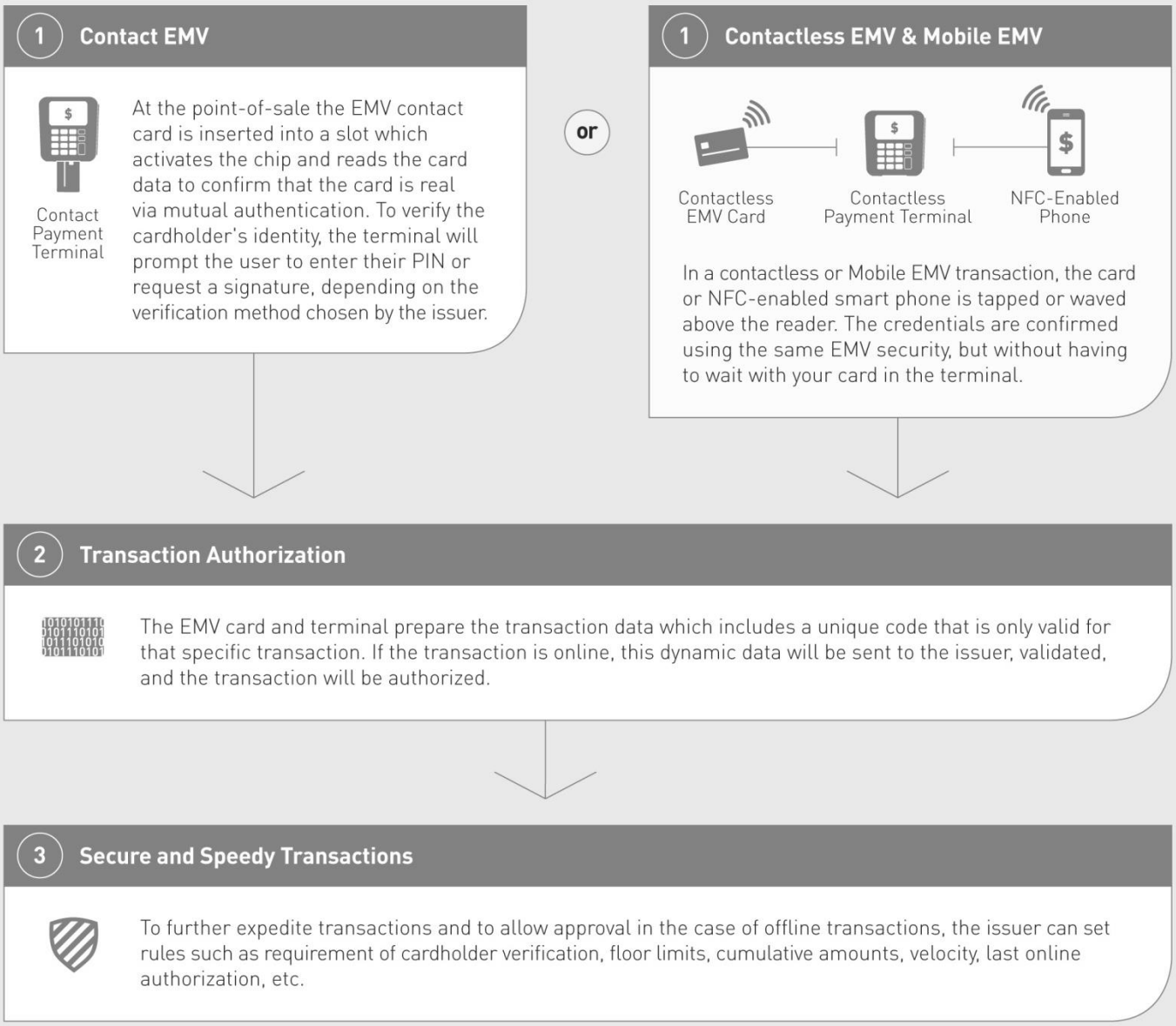
6) Technology considerations
Technology considerations are arguably one of the most crucial discussions for issuers and merchants moving forward with their EMV implementations. The foundation of EMV brings the highest level of security to innovative payment options such as mobile, contactless and wearables. We have worked with customers around the globe to determine their next steps in providing users with the full EMV experience. In the majority of previous migrations basic EMV cards are issued and as consumers understand the benefits they begin looking for the same type of technology for faster payment experiences. For example, Commonwealth Bank provided contactless EMV options to its customers and has since seen higher usage rates in addition to increased sales.

CONCLUSION

The ubiquity of EMV chip cards in the U.S. will dramatically decrease the options fraudsters will have to use stolen account data and it will enable cardholders to embrace contactless and mobile payment at the POS

SECURING TRANSACTIONS AT THE RETAIL POINT-OF-SALE

No matter which payment method is used, EMV affords the added security of credit cards remaining in the possession of the cardholder throughout the entire transaction. With EMV, the computer chip inside the bankcard is an active part of the transaction; unlike the magstripe, which is passive.



ABOUT GEMALTO, YOUR TRUSTED EMV PARTNER

A Trusted, Experienced Partner

We understand the needs of card issuers because we have supported banks through decades of EMV issuance, working with more than 3,000 financial institutions and issuing 4 billion payment cards.

Customer Service for the Entire Journey

Our support doesn't end with the first wave of EMV issuance. We're ready to support you through the entire lifecycle of managing your EMV program. With deep expertise in mobile payment solutions, we'll help to ensure you're getting the most out of your mobile program for the road ahead.

Capacity and Time to Market

As the world's largest provider of EMV solutions, we have the capacity to scale with your EMV needs better than any other card provider, which means you can achieve your time to market goals.

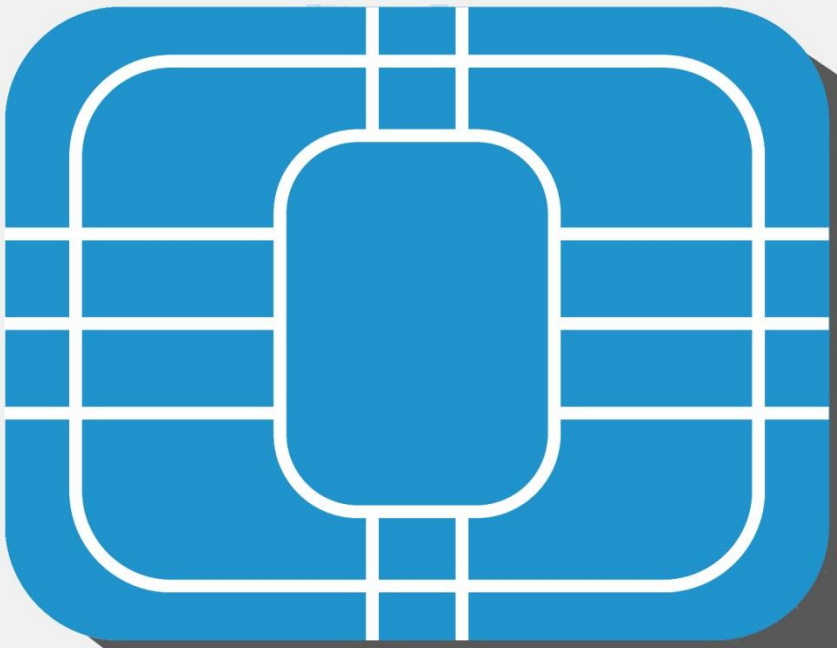
To begin your EMV journey visit: www.gemalto.com/emv

For more information on EMV visit: www.thatsemv.com

Connect with Gemalto on Twitter: @Gemalto_NA

WHY EMV AND WHY NOW?

BY PHILIP ANDREAE , VICE PRESIDENT FIELD MARKETING AT OBERTHUR TECHNOLOGIES



oberthur TECHNOLOGIES
THE M COMPANY

INTRODUCTION AND HISTORY

EMV is actually younger than we all may think as it only became available, as a specification that could be implemented, in 1996. The evolution of EMV can be seen in the development of Integrated Circuit Cards or ICCs which have been around since 1978 when Bull successfully created the self contained computer all within one piece of Silicon. Then a much less robust payment solution was developed in 1984 by Carte Bancaire, the French domestic payment system, and helped to establish the basic principles for what EMV ultimately developed.

EMV as a specification was designed to replace the magnetic stripe, hologram and other security features present on a physical payment card.

The Goal: replace the physical features with a digital mechanism capable of authenticating the card presented at the point of sale.

The founders of EMV wanted to create something that was future proof and could be dematerialized as technology evolved and the phone emerged as a means of merging our leather wallet with the future smart phone. Such early smart phone examples included in the Nokia 9000, which in 1996 offered Internet Browsing on the mobile phone and the Palm Pilot held our music, pictures, calendars and address books.

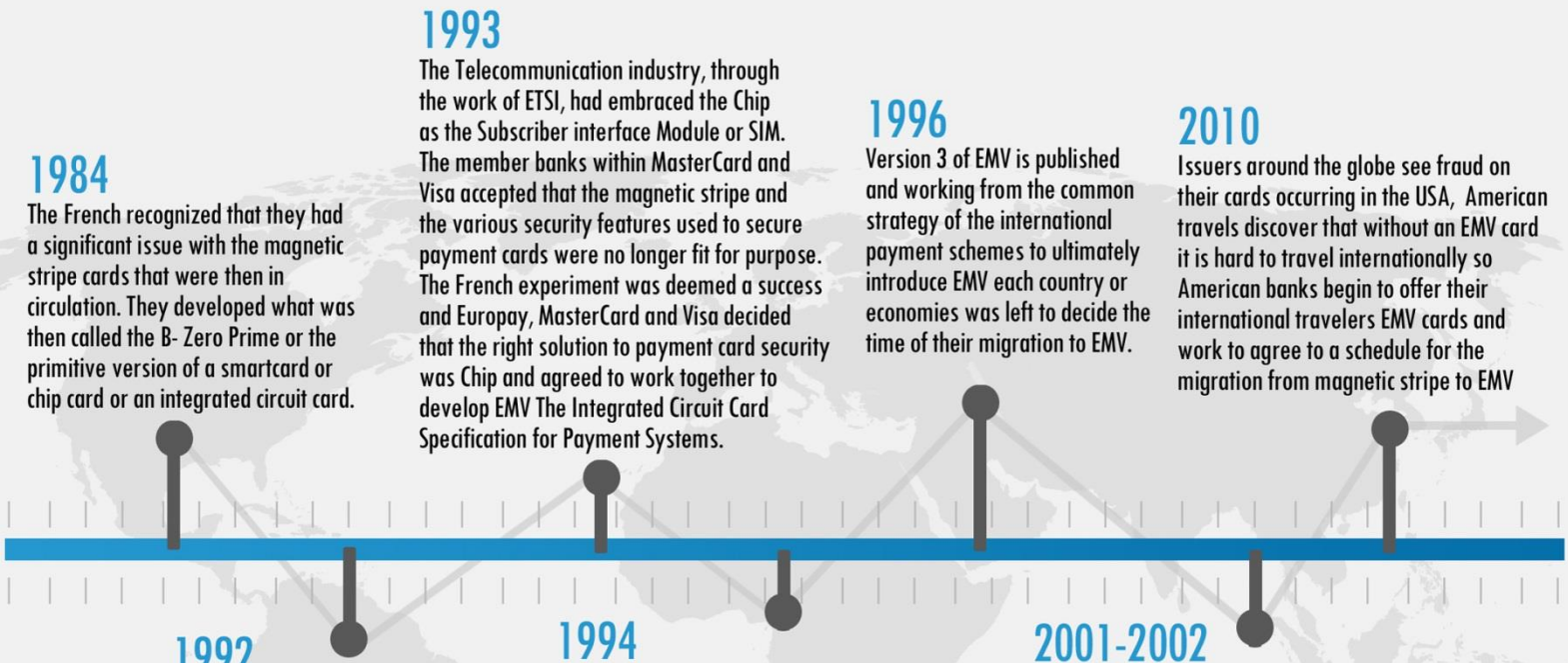
From 1996 until the present day EMVCo continues to update the EMV Contact Card Specification to enhance the security, improve performance and assure interoperability. The most recent release Version 4.3 was published in November of 2011. They have even begun work on an architecture designed to assure the security of payments well into this century.

INTRODUCTION AND HISTORY

Additionally, Based on the finalization of the ISO 14443, the International standard for near field communications, the various payment schemes created their own proprietary specifications for the use of NFC, all based on the EMV tool kit. In 2009 the owners of EMV contributed their contactless specifications (PayPass, PayWave and Express Pay) to EMVCO and worked together incorporate them into the EMV Contactless specifications. These specifications were last updated in February of 2014 as version 2.4. These specifications now incorporate the necessary enhancements to support Mobile Wallets, and specific requirements emerging from Transit.

Today Apple Pay, SoftCard, Google Wallet and a myriad of other interoperable mobile wallet initiatives around the world conform to the EMVCo specifications.

EMV MILESTONES *FROM THE PERSPECTIVE OF PHILIP E ANDREAE*



1984
The French recognized that they had a significant issue with the magnetic stripe cards that were then in circulation. They developed what was then called the B- Zero Prime or the primitive version of a smartcard or chip card or an integrated circuit card.

1992
In France fraud goes from the teens in basis points to somewhere less that 02 basis points. Simultaneously, the number of online transactions goes from 25 percent online to 10 percent. It is proven that: chip can be used to authorize transactions offline using issuer- controlled parameters in the card. There was no need to pay the telecommunication agents for online requests and there is a radical drop in counterfeit fraud.

1993
The Telecommunication industry, through the work of ETSI, had embraced the Chip as the Subscriber interface Module or SIM. The member banks within MasterCard and Visa accepted that the magnetic stripe and the various security features used to secure payment cards were no longer fit for purpose. The French experiment was deemed a success and Europay, MasterCard and Visa decided that the right solution to payment card security was Chip and agreed to work together to develop EMV The Integrated Circuit Card Specification for Payment Systems.

1994
In Parallel with the Boards of MasterCard and Visa (then dominated by the USA) agreeing to the global migration to EMV for the physical world, the Internet emerged. Merchants saw the internet as a way to extend their market from being local to being global. The payment systems extended the Mail Order Telephone order rules and related liability allowing the merchants to only capture the information clearly printed on the face of the card and began work to develop SET the specification for Secure Electronic Payments

1996
Version 3 of EMV is published and working from the common strategy of the international payment schemes to ultimately introduce EMV each country or economies was left to decide the time of their migration to EMV.

2001-2002
Starting in the UK and extending around the globe the migration to EMV progresses. The United States deploys contactless cards using EMV standard and figuring out a way to support a minimal level of dynamic data without a need to upgrade the various authorization and clearing systems Simultaneously the international payment s chemes replace SET with 3D-Secure and push merchants and Issuers to adopt this new standard for securing internet payments. Unfortunately consumers rebel and merchant have to decide, lose the sale -8 % or accept the cost of fraud 0.30 %.

2010
Issuers around the globe see fraud on their cards occurring in the USA, American travels discover that without an EMV card it is hard to travel internationally so American banks begin to offer their international travelers EMV cards and work to agree to a schedule for the migration from magnetic stripe to EMV

THE ROLE OF EMV IN SUPPORTING DIGITAL PAYMENT INNOVATIONS

Ever since the telephone and telex machines where introduced as mechanisms that would digitize payments; we have been actively involved in driving innovation thorough enhanced method of supporting digital payments.

Today and into the future EMV is and will enable face to face secure payments utilizing cards, fobs, dongles, smart phones and the cloud. It will secure payments in the shops and malls of this great land. It is the standard that is enabling the growth of Mobile wallets (Apple Pay, SoftCard and Google Wallet) and the ability to Identify, Authenticate, Verify and ultimately Authorize payment transactions in a secure and transparent way. That was and remains the goal of EMV and is what it continues to assure.

Recognizing the internet will continue to see double digit growth and continues to offer all of us access to an every expanding global shopping mall. Fully aware of how consumers are using phones, tablets, kiosks, ATM and personal computers to find and purchase what they desire; we are developing enhanced security solutions such as our cards capable of generating and displaying one time passwords or offering the ability to display a dynamic Card Verification Value. We see opportunities to merge EMV with 3D-Secure EMV as a method of secure the internet. We see cards and digital credentials inside mobile phones, issued by Financial Institution potentially becoming an integral part of the emerging use of federated credentials designed to replace user names and passwords and secure cyberspace.

In addition EMV brings enormous advantages to token and tokenization. Here is how: The PAN or Personal Account Number, the 15 or 16 digits printed on the face of the card, is a token or unique number connecting the card to the account the Financial Institution manages for the cardholder. Unfortunately back in 1994 and even now when the Internet emerged we did not found a convenient and acceptable method to protect the card not present environment from stolen data being used to commit fraud.

THE ROLE OF EMV IN SUPPORTING DIGITAL PAYMENT INNOVATIONS

We the consumers, merchants and financial institutions allowed "Convenience to TRUMP Security". We collectively drove the payments networks to simply expand the scope of the rules and merchant liability associated with mail order and telephone order catalog sales. We allowed the merchant to simply ask the consumer to enter the data on the face of their payment cards If we had come up with an effective and convenient way to authenticate that the consumer was who they claimed to be we would not be talking about tokenizing a token (the Personal Account Number). Unfortunately we are where we are and now must figure out how to protect the Card Not Present (Internet / eCommerce) space.

What people are talking about doing is segregating the account numbers or tokens we use in the physical world from those that we use in the virtual or mobile world.

Whenever EMV is employed there is a need to create a set of credentials for each "PAN". This process is called Data Preparation and is when the Secrets and certificates that allow EMV to create the Unique and Dynamic Signature associated with each transaction are created. This is exactly what is happening when Apple described the process when the PAN is mapped to the DAN and the Secure Element is enabled to support that particular card.

The interesting reality is that in the physical world, through the use of these secrets and credentials EMV, will restore the Personal Account Number back to what it was, a unique number that links the card to the line of credit or deposit account a financial institution manages for the cardholder

CONCLUSION

EMV is a security protocol built on International standards and evolving cryptographically enabled computer technologies. The technology that EMV employs evolves, just like all computer technologies, and is specifically enhanced to add additional security features designed to assure the integrity of the cryptographic processes and secrets that underline all forms of hardware based security in use today.

EMV is only about payments. The techniques and technologies EMV utilizes are the technologies that will secure cyber space. Not EMV but standards like EMV will provide the means of assuring that our identity in cyberspace can be secured. Efforts now underway in the FIDO alliance and W3C are looking to methods of eliminating the use of Single factor Authentication or User Name password and replace them with Multi-factor authentication based on Cards, Fobs, Phones, Fingerprints, Voice prints, facial recognition and a myriad of other techniques to make sure only the rightful consumer or citizen is presenting themselves in cyberspace.

We spend time educating our clients and the industry on the power and capabilities of EMV. OT also participates in or is monitoring the activities of various standards bodies such as FIDO, X9, W3C O we are engaging with our competitors, clients and suppliers to enhance and develop security solutions to our connected world.

OBERTHUR'S CORE EMV STRENGTHS

OT is a key historical player in the U.S. market, having established its U.S. footprint in 1996 and rapidly started business with the largest banks in the industry.

OT's EMV partnerships include trusted global brands American Express, China Union Pay, Discover, MasterCard and Visa. OT has delivered EMV cards to four of the top five card issuers in the U.S. Further, OT provides magstripe cards for seven of the top ten U.S. card issuers.

OT is an EMV pioneer in the U.S. and current market leader with 65% share of this still burgeoning market. OT currently produces 20+ million EMV cards for 25 different U.S. issuers annually.
To support the EMV migration, OT invested in its U.S. production capacity in order to produce 400 million EMV cards and 100+ million chips annually.

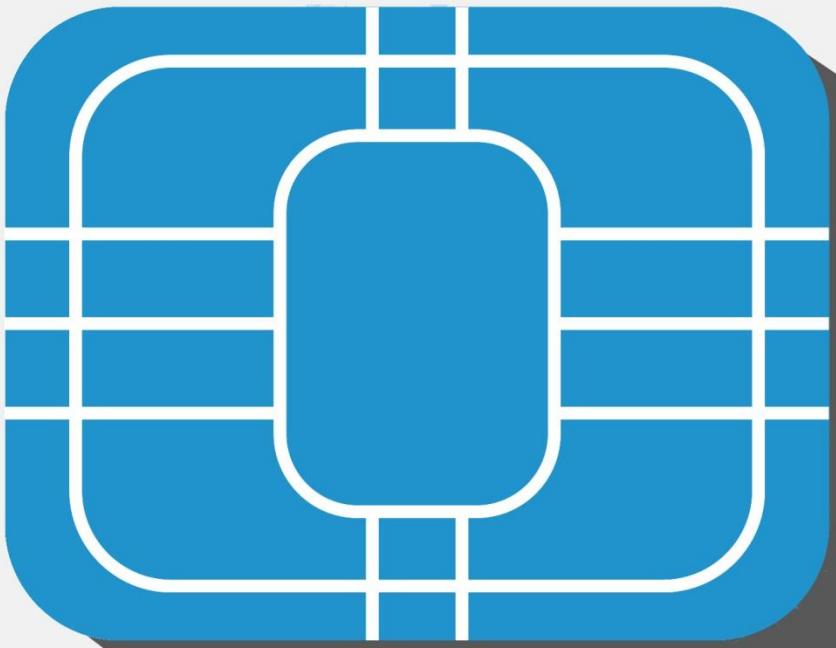
To mitigate the complexity of EMV, OT offers EMV-In-A-Box, allowing a smoother, faster issuance of EMV cards. EMV-In-A-Box's proven methodology has been executed for 250+ EMV migration projects.

EMV-In-A-Box effectively addresses issuers interested in both initial migration from magnetic stripe cards to EMV contact or dual interface cards, supporting multiple cardholder verification methods (CVM), or reissuing cards on a similar card platform due to chip lifecycle expirations, a new card platform or extending their portfolios from contact to dual. Thus, EMV-In-A-Box provides full lifecycle management of your EMV card issuance programs, which allows for complete flexibility today and tomorrow.

ABOUT OBERTHUR TECHNOLOGIES

OT is a world leader in digital security solutions for the mobility space. OT has always been at the heart of mobility, from the first smart cards to the latest contactless payment technologies which equip millions of smartphones. Present in the Payment, Telecommunications and Identity markets, OT offers end-to-end solutions in the Smart Transactions, Mobile Financial Services, Machine-to-Machine, Digital Identity and Transport & Access Control. OT employs over 6 000 employees, including 600 R&D people. With more than 50 sales offices across 5 continents and 10 facilities, OT's international network serves clients in 140 countries.

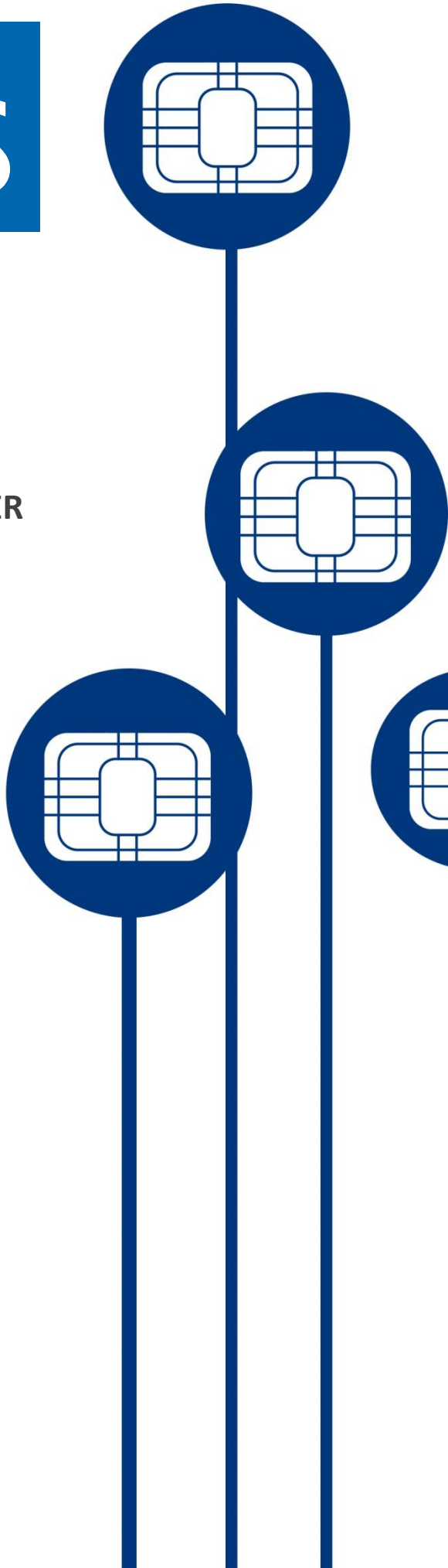
For more information: **www.oberthur.com**



THE FIVE Ws OF EMV

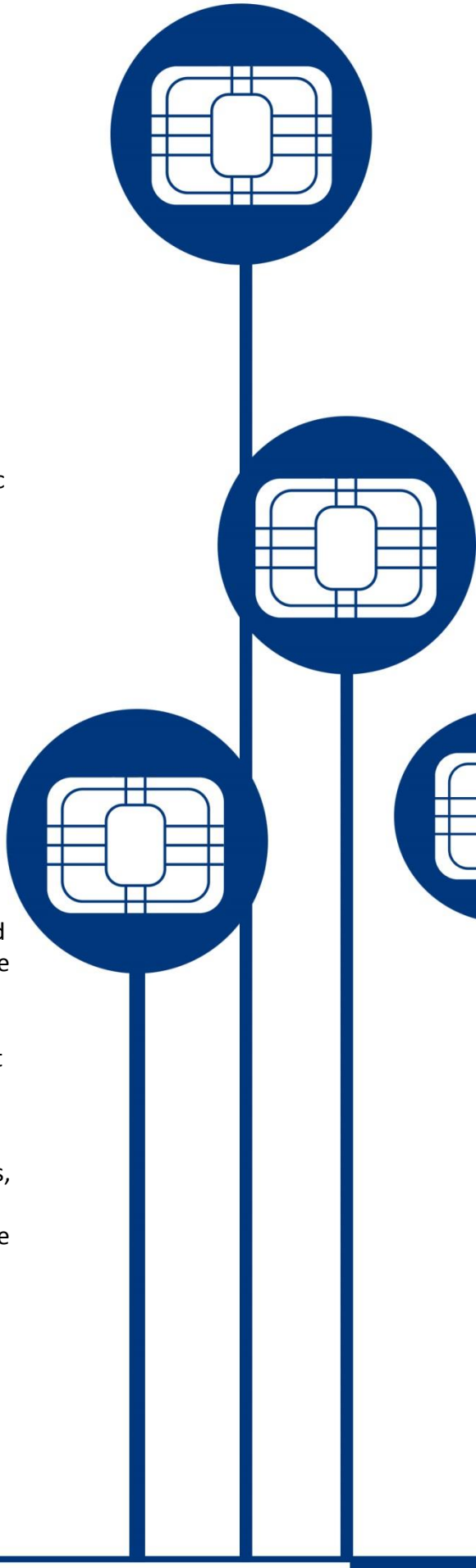
BY DAVE EWALD

GLOBAL EMV CONSULTANT AND MANAGER
DATACARD GROUP



DatacardGroup

WHERE IS THE U.S. PAYMENT CARD INDUSTRY NOW? WHERE IS IT GOING?



Today, payment and identification cards of all types (credit cards, gift cards, loyalty cards, membership cards, security IDs, etc.) are encoded with the cardholder's information on the back of the card using a strip of magnetic tape, also known as the magnetic stripe.

When a consumer swipes a standard magnetic stripe card at a retailer's point of sale (POS) terminal, or inserts it at an ATM, the data on the magnetic stripe is captured for transmission to an authorization system. Fraudsters have been able to put skimmers at these locations to capture the data from the magnetic stripe, and in more sophisticated attacks, install malware on computers connected to the POS terminal to capture the data. The prevalence of magnetic stripe cards in the US makes card skimming and card copying easy and lucrative. In 2012, the US accounted for 47% of global credit card fraud while only being responsible for 23% of total global credit card use.

Chip cards are different from traditional magnetic stripe cards in the way they communicate with card reader devices. Rather than the classic swipe-to-scan method, chip cards have an embedded integrated circuit chip which connects to the POS terminal's chip card reader. This chip is a microprocessor with the capability to encrypt transaction data dynamically for each purchase. With over 1 billion cards in use, EMV is already a burgeoning global reality.

Contact Chip Cards can be distinguished by their square metallic contact pads. These cards are inserted into a POS terminal which has an integrated chip card reader; much like a microSD card or flash drive is inserted into a computer. The card stays inserted in the POS terminal until the transaction is complete. Chip cards are only activated when connected to a reader, which provides the power source for communication. Chip cards do not have batteries and do not need to be charged.

Contactless Chip Cards also do not require an internal power source. Embedded in the plastic of a contactless card is an antenna. Using radio waves, the card communicates with a reader that emits a specific radio frequency. This frequency is harnessed to power the electronic chip. Contactless cards are especially advantageous for use as payment cards because they need only a moment to tap or wave the card near a reader to complete the communication. Recent pilots and rollouts indicate contactless chip cards will be widely utilized for transit payments.

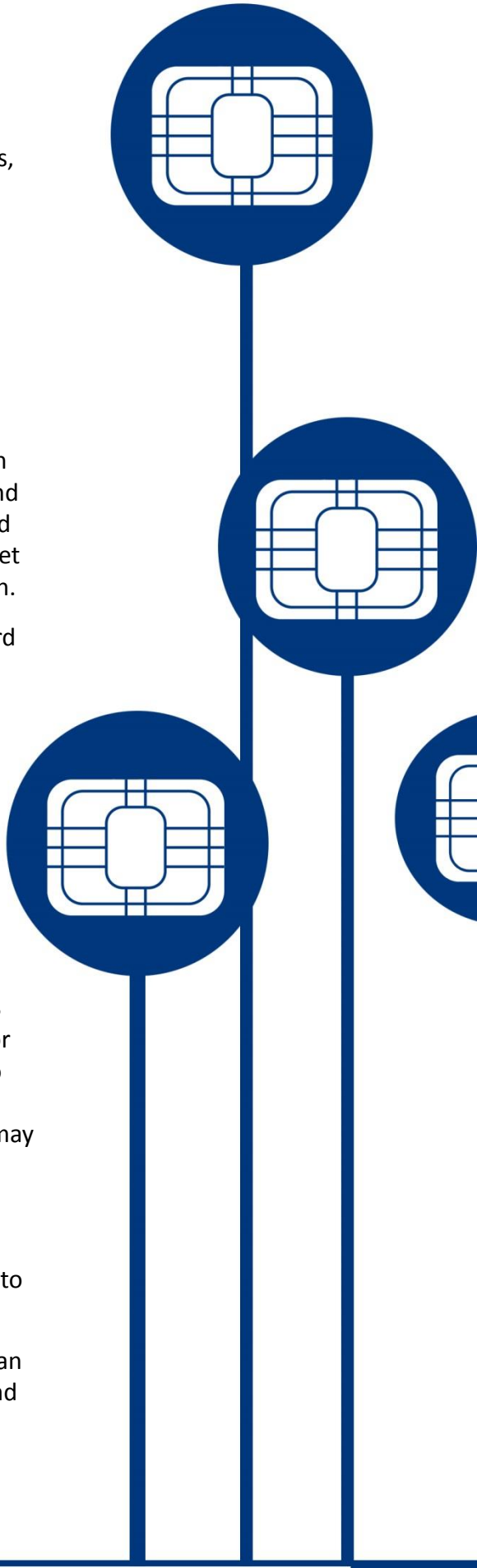
Hybrid or dual interface cards include both a contact pad and an internal antenna. They can be tapped, waved or inserted into many different chip card readers.

WHAT IS EMV?

EMV refers to the specifications administered by EMVCo using international standards to champion global interoperability for payment cards. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Today there are EMV Specifications based on contact chip, contactless chip, common payment application (CPA), card personalization, and tokenization.

These specifications and requirements were developed with a mission to increase payment security and efficiency, and to ensure global interoperability amid payment ecosystems. A globally accepted EMV card empowers cardholders to take out cash from an ATM in Hong Kong, buy lunch at a deli in New York, or buy a train ticket from a Deutsche Bahn kiosk in Munich—all with the same card. EMV regulations regarding chip size, card size, electrical use, and security features all help make this possible. Chip cards are already widely used in Europe, Asia and other regions. The transition of the US payment card market from magnetic stripe cards to chip cards is referred to as the US EMV migration.

EMVCo is the association that manages, maintains and enhances EMV chip card specifications. EMVCo is comprised of six member organizations—American Express, Discover, JCB, MasterCard, UnionPay, and Visa—and supported by dozens of banks, merchants, processors, vendors and other industry stakeholders who participate as EMVCo Associates.



WHO WILL BE AFFECTED BY EMV MIGRATION?

Cardholders will have to adapt to new ways of interacting with ATMs and POS terminals. Consumers using contact chip cards will have to insert their card for the duration of the transaction, and those using contactless cards will have to tap or wave their card over the designated area. Also, depending on how the chip card is configured and the capabilities of the POS terminal, cardholders may have to verify they are the actual cardholder by entering a PIN instead of verifying by signature.

Card Issuers will have their operation costs go up, as the new cards are more expensive to produce and replace. They will also have to work with acquirers to update their payment processing and authentication infrastructures.

Merchants will have to upgrade and certify their POS terminals so that they can communicate with chip cards. As mobile payments rise in popularity, more and more apps will adapt to enable mobile phones to communicate with POS terminals. Today, there are many apps and mobile phones which can communicate with POS terminals.

WHEN IS MIGRATION HAPPENING?

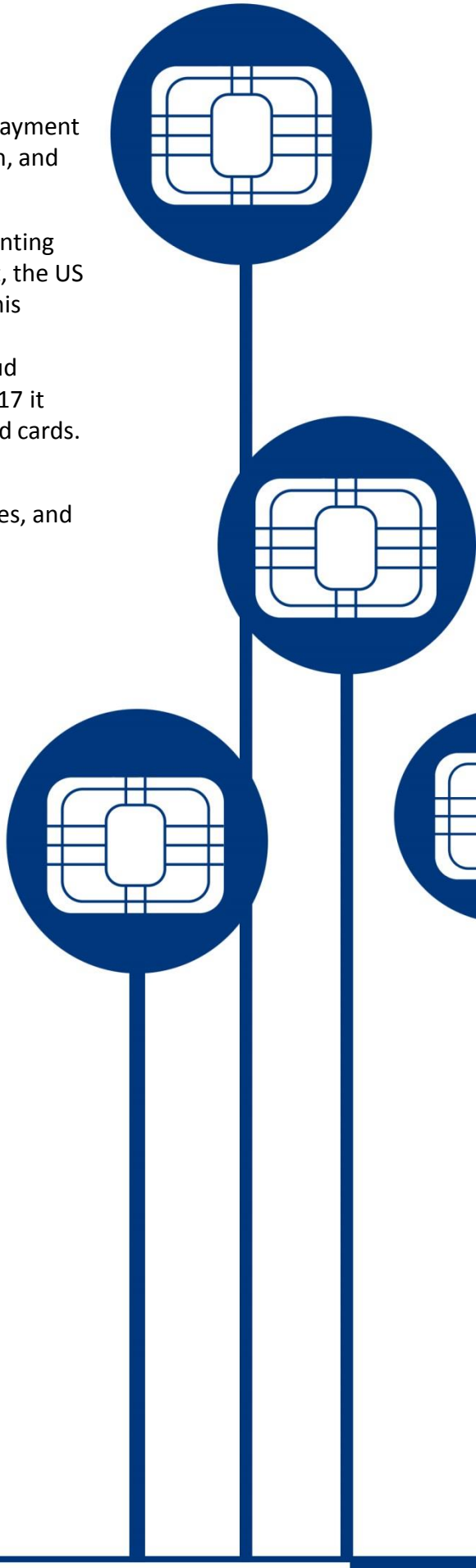
Now. Slowly but surely, major card providers in the US are beginning to offer payment cards with chips. Some cards are requiring PIN entry for cardholder verification, and others are requiring signature for cardholder verification.

The US is currently behind many parts of the world when it comes to implementing chip card payment technology, and in an effort to encourage EMV deployment, the US card brands have instituted a fraud liability shift beginning October of 2015. This means that after October 2015, all parties that make an investment in EMV technology will be protected from being financially liable for any potential fraud losses. In 2016 this will include ATMs for MasterCard branded cards, and in 2017 it extends to automated fuel dispensers, and ATM transactions with Visa branded cards. The liability shift is NOT a mandate.

Merchant Migration requires upgrading and certifying their point of sale devices, and training their cashiers to use the new payment method.

Card Issuer Migration requires providing their cardholders with chip cards and educating the issuer's employees and their customers about the chip cards, what they are capable of, and how to use them.

Cardholder Migration requires consumers to apply for chip cards, or request chip cards from their current card provider. Over time, cardholders will receive chip cards as part of new card issuance or through the normal renewal process. Cardholders will also have to adjust to new methods of using their card with card readers.

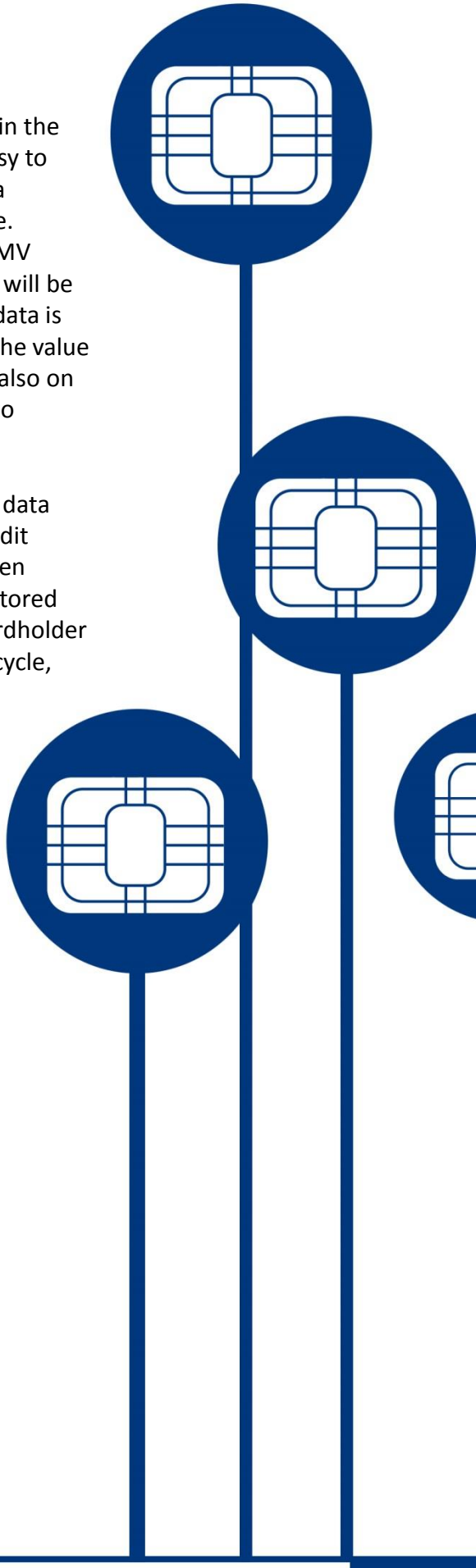


WHY MIGRATE NOW?

EMV provides better protection for cardholders. Card fraud is a huge problem in the US, largely due to the prevalence of magnetic stripe swipe cards, which are easy to counterfeit. EMV cards remove most opportunities for card skimming, where a magnetic stripe is scanned without the cardholder's consent for fraudulent use. Opportunities for card transplant fraud, where stolen card information from EMV markets is printed onto a magnetic stripe card and used in non- EMV markets, will be greatly reduced as more markets embrace EMV technology. In the event that data is stolen from an EMV card, or during a transaction initiated from an EMV card, the value of that data for counterfeiting purposes is greatly limited. Mobile markets are also on the rise, and the current transition to chip cards will make the next transition to mobile payments safer and easier by protecting and enabling consumers.

Today, fraud risk is making headlines like never before. Recent notable retailer data breaches have affected millions of American consumers, and have brought credit security issues to the forefront of public debate. Thieves have successfully stolen customer card information by observing and taking advantage of how data is stored and moved between different areas of the payment environment. Valuable cardholder information can be compromised not due to one weak link in the transaction cycle, but due to joint weaknesses in the current payment system as a whole.

EMV chip card ubiquity in the US will dramatically decrease the options fraudsters will have to use stolen account data, and it will enable cardholders to embrace new ways of making payments by protecting and informing them. Updating the US payment system infrastructure to support EMV will take time, investment, and careful planning. It will require merchants, issuers, acquirers and processors to evaluate and update their current security precautions. EMV Migration will not correct every weakness within the US payment system, but it is the first clear step in a long process of ushering the payment business into the digital age.



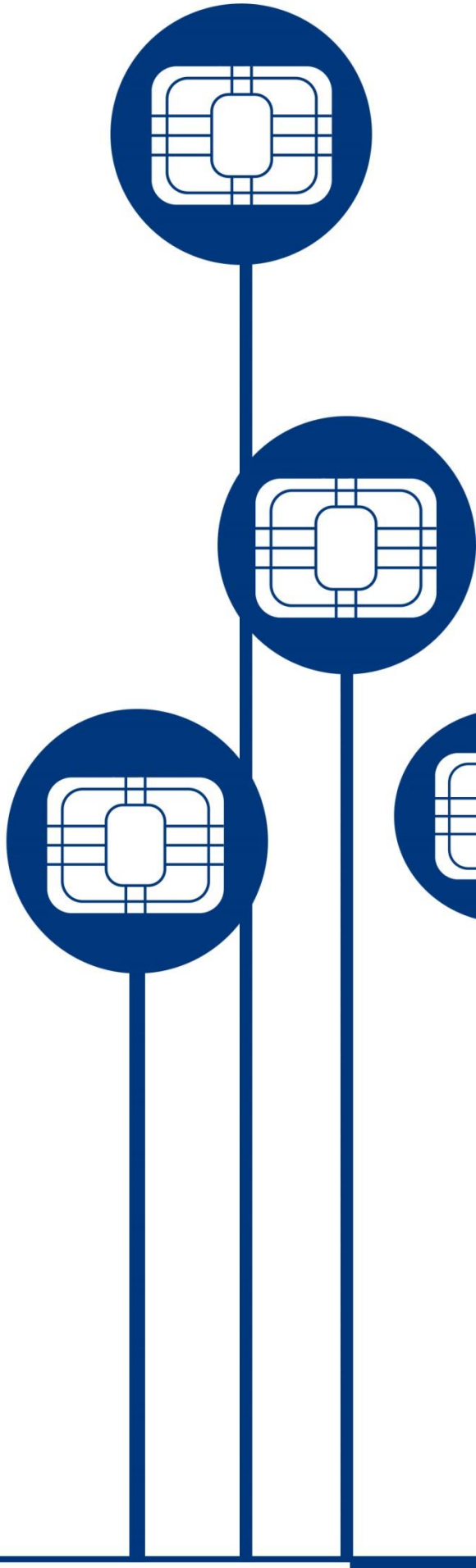
ABOUT DATACARD

Datacard Group offers technologies for securing identities and safeguarding transactions in physical and digital environments. The company's innovative portfolio now includes , bringing important new capabilities to tens of thousands of government agencies, financial institutions and other enterprises in more than 150 countries. Together, Datacard Group and Entrust issue 10M+ secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards.

Each of us is a consumer and a citizen. At different times, we're also employees, students, patients and members. In these roles, we conduct transactions, use information, enter facilities, cross borders and access government services. Datacard Group brings trust and security to each of those interactions for millions of people every day – across both physical and digital domains.

Security-minded enterprises rely on Datacard Group and use our solutions as a foundation for their identity and transaction infrastructures. We work closely with hundreds of financial institutions, including the world's 20 largest banks. Our instant issuance solutions and mobile payment solutions are creating new opportunities for banks, retailers and other consumer marketers. We're engaged in high-profile government identity programs around the world. We also serve customers in telecommunications, aerospace, pharmaceutical, education, healthcare and petroleum markets.

Learn more by visiting: **www.Datacard.com**



CUTTING THROUGH EMV HYPE AND CONFUSION IN THE U.S.

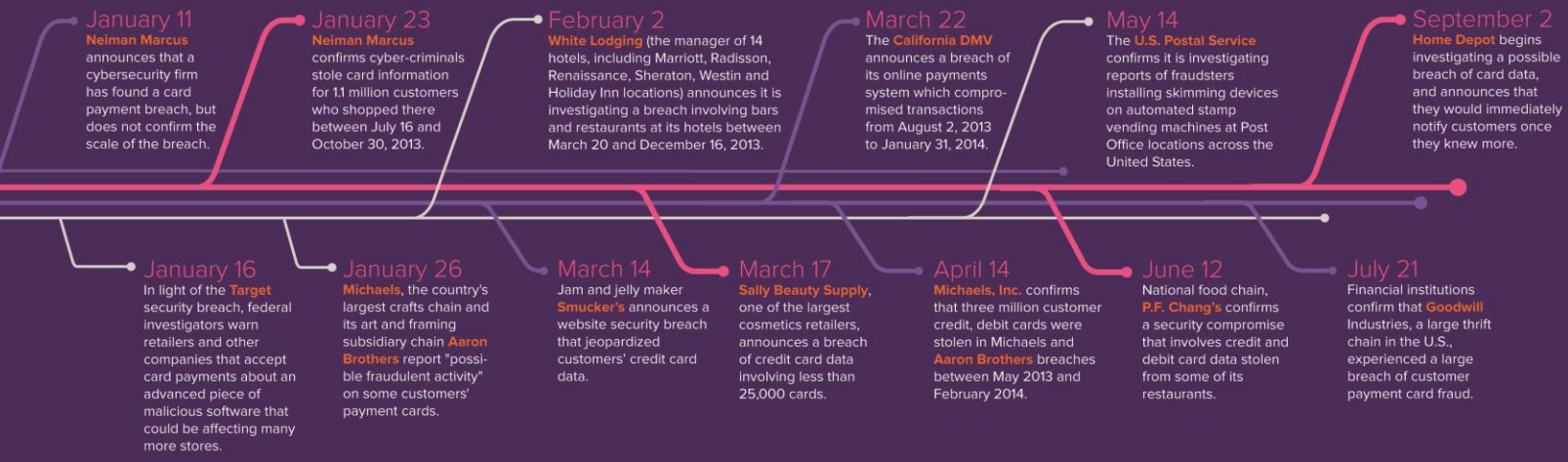
Where We Are, Where We Should Be, and How to Become EMV Compliant

By Jeremy Gumbley, CTO, Creditcall

creditcall

INTRODUCTION

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 was the largest breach of consumer data on record. The news swept the nation, and the spotlight was on Target to fix the problem. Unfortunately, Target was not the only retailer in the U.S. that was targeted by hackers in the months to come.



Home Depot's breach of sensitive customer data, which may have trumped Target's payment systems breach in total number of customers (which affected close to 70 million consumers) as the largest data theft to date, has elevated the discussion regarding data security.

These breaches have created a domino effect across the U.S. market, generating heightened consumer and political awareness around unresolved credit card payment systems security issues. Acknowledging these concerns, President Obama recently signed an executive order to speed the adoption of EMV chip cards in the U.S. (on October 17, 2014) as, the U.S. has been in the spotlight for a while, for how far behind the market it is by global comparison in adopting the EMV chip card standard – a much more secure form of payment processing.

Target's data breach cost shareholders $148 million, according to *Forbes*, which does not include monumental and disruptive fees associated with legal counseling, losing consumer trust, organizational costs that came as a result of CEO Gregg Steinhafel stepping down, and implementing new security processes.

One benefit to the U.S. slow adoption of EMV as compared to the rest of the world, is that there are many lessons learned, best practices and proven success from other nations already embracing EMV.

Take Canada for example; since Canada's EMV Migration last year, major merchants have already experienced substantial benefits. 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.

WHY DO HACKERS INCREASINGLY STEAL U.S. CARD DATA?

The consistent onslaught of consumer data breaches among major businesses immediately following Target, and most recently Home Depot, clearly illustrates some of the main vulnerabilities in magnetic stripe cards – an outdated system that is still used across the U.S. While the rest of the world* has embraced EMV to mitigate risk, the U.S. remains a laggard in such adoption. This has made the U.S. an easier target for potential hackers and resulted in both a shift in consumer's perception and confidence.

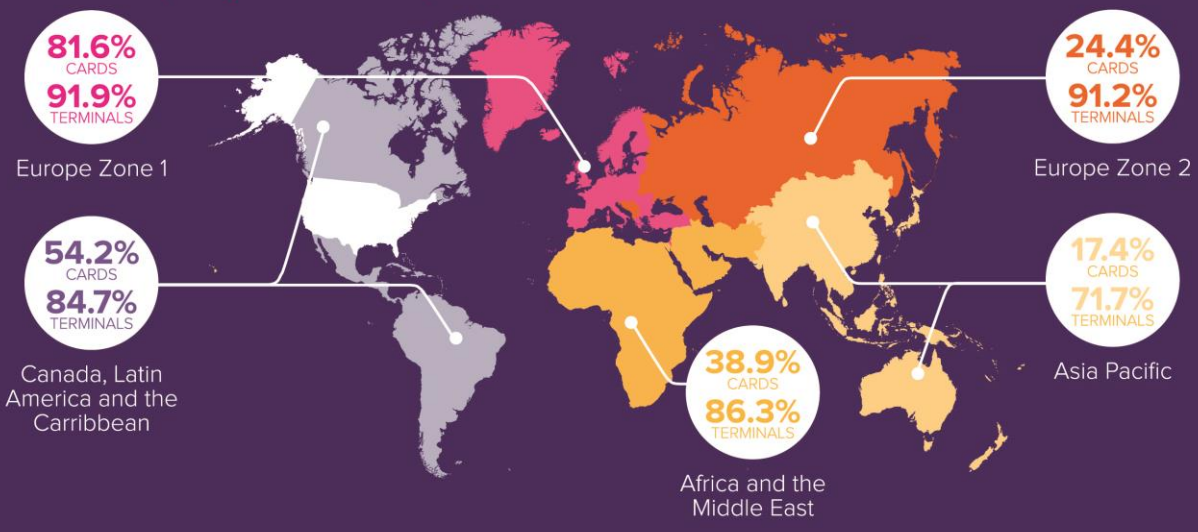
In a recent survey of 1,011 American adults conducted by Vision Critical 2014, 64% were more likely to pay in cash due to recent security breaches and approximately the same number of respondents believed that a credit or debit card with an EMV chip would result in more secure financial transactions.

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*

HOW DO HACKERS STEAL CARD DATA?

Anyone connecting to the Internet is vulnerable to being hacked. Financial gain is often a hacker's primary motivation. Many make money by setting up fake e-commerce sites to collect credit card data, or gain entry to servers that contain credit card details. There is no shortage of examples. In the case of Home Depot the hacking lasted from April through September 13. Stolen data was soon available in the black market with the cheapest cards selling for $2.26.

Criminals also skim information from legitimate cards to manufacture fake or counterfeit cards, and use them for fraudulent purposes. In fact the manufacturing of counterfeit cards, has become a cottage industry as it is a lot easier to hack a magnetic swipe card than it is an EMV chip card no matter if the authentication is made via Chip and PIN or Chip and Signature. Chip and PIN, however does introduce a second level of authentication making it even more secure, forcing hackers to obtain both pieces of information to successfully use the card in a face to face environment.

EMV makes stealing card data less attractive because it is very difficult to create a counterfeit EMV card.

EMV chip cards would not have prevented the Target data breach, but wider adoption of the technology could have dramatically narrowed the reuse of the stolen data.

WHY NOW IS THE RIGHT TIME

Although the liability shift deadline, October 2015, is important, the surge in consumer demand is a clear indicator to businesses that the cost and repercussions of not embracing EMV can easily outweigh the upfront costs of compliance. A recent MasterCard survey says that 57 percent of Americans are now expecting to receive their EMV chip cards in the mail within six months.

EMV is real but it will take many years before all merchants are able to accept chip cards and all consumers carry them. However, this is no longer the chicken and egg scenario, where merchants want to see consumer demand before they invest in EMV technologies. Many consumers already know they want the security benefits of EMV.

As with any technology shift there are varying degrees of misconceptions. These will be outlined in the next section and how to approach them.

UNDERSTANDING SCALE AND COMPLEXITY OF EMV MIGRATION

Albeit a cliché, the phrase, "you don't know what you don't know," may currently be true, as the U.S. is widely unaware of the scale, scope and complexity required to upgrade a payment system to the EMV standard.

Creditcall has served as a trusted EMV payment-gateway partner and EMV Level 1 and Level 2 Kernel provider for many international merchants and PINpad manufacturers migrating to EMV. In over 14 years of EMV Migration experience, Creditcall most often hears of customers experiencing the following five pain points when upgrading a payment system to the EMV standard. With the quickly approaching October 2015 liability shift, these steps can help direct merchants, ISVs, VARs and integrators through the complex process and put them on the right track to meet the deadline.

THE FIVE PAIN POINTS OF EMV MIGRATION

1) PINPADS AND DRIVERS

A PINpad is where a large part of an EMV transaction takes place through a complex dialogue between the chip card and the PINpad. Although there are a number of EMV capable PINpads available from major manufacturers, they are often complicated to integrate and manage, despite integration guides and Software Development Kits (SDKs). In a worst case scenario, manufacturers will provide a PINpad protocol or API specification to interface with 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 (e.g. Application Selection, Data Authentication, Online 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, bugs in the PINpad software, inconsistencies in the documentation and undocumented PINpad behavior. The more experienced 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 the PINpad supports, which are often unrelated to EMV. SDKs also require a deeper understanding of EMV. So while SDKs solve some of the integration issues, they do not solve the time investment in understanding EMV. Another problem with this approach, is that SDKs are not frequently updated so bugs can go unaddressed for some time.

Furthermore, manufacturers suffer from often inconsistent support, which is further exacerbated by the sheer volume of integrators who will ask the same integration and support questions. Most manufacturers are also not setup to support large volumes of developers, and are unfamiliar with the diverse range of development environments and methodologies that exist today.

> ***"Although there are a number of EMV capable PINpads available from major manufacturers, they are often complicated to integrate and manage, despite integration guides and SDKs."***

2) PROCESSOR INTERFACES AND EMV MESSAGING

Many integrators support a multitude of different Processors, and each and every interface will need to be modified to support the new EMV data fields and process flows. This is already a complicated undertaking with a single interface, let alone multiple interfaces. When combined with the fact that most interfaces are based on legacy code developed many years ago, the addition of new features such as EMV becomes an increasingly difficult task, especially if the original developers are not available. 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.

> ***"Many integrators support a multitude of different Processors, and each and every interface will need to be modified to support the new EMV data fields and process flows."***

3) CARD SCHEME CERTIFICATIONS

(M-TIP/ADVT/AEIPS/DPAS)

Once an integrator has updated their Processor interfaces, they face the complex task of end-to-end testing and certification. In markets where EMV is mature, this process can take up to 16 weeks and often requires expensive test tools and cards. It is unclear at this time if Processors will be able to cope with the volume of certifications required before the October 2015 liability shift. This is not a one-time process; it must be repeated every three years when the EMV Kernel certification on the PINpad expires. It must also be repeated for every PINpad and Processor combination. If an integrator needs to support three different PINpads and three different Processors, then it might take 144 weeks (3 x 3 x 16) to certify these combinations. This will of course have to be repeated every three years. Although the Processors are looking at truncating these timescales, it is currently unclear how this will be achieved. In our experience this is the part of EMV Migration that is often vastly underestimated in terms of complexity and time needed.

4) TERMINAL MANAGEMENT SYSTEM (TMS)

Once an integrator has completed the first three steps, they then need to consider how to manage a potentially large estate of PINpads. A PINpad is essentially an embedded platform that runs its own software stack and as with any software stack, it requires updates to keep it compliant with current versions of the EMV standard. Security vulnerability patches or general bug fixes also need to find their way to the PINpad. Regardless, the certification status of the core EMV Kernel software that resides on the PINpad will expire every three years. In addition to the software on the PINpad, EMV also requires certain configuration items such as CA Public Keys that are used in cryptographic operations. Without a TMS platform, an integrator runs the risk of having PINpads without current software or the latest configuration. This 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 deployed has access to a TMS platform for efficient and timely deployment of updates.

5) PCI POINT TO POINT ENCRYPTION (P2PE)

Although not directly related to EMV, strong transaction security via P2PE is a prudent security counter measure. Most PINpads provide the basic functionality to support Point-to-Point Encryption, but to implement it requires significant effort. P2PE is a system where cardholder data is encrypted, within a highly secure area of the PINpad, before it is sent to the outside world – in this case the integrator's application. To implement P2PE correctly, working knowledge of cryptography, and how it is applied to transactions, is paramount. It also requires a significant investment of time and money in dedicated hardware such as HSMs (Hardware Security Modules) that serve to decrypt the 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. The formal PCI P2PE certification is a large and complex undertaking.

Although not directly related to EMV, strong transaction security via P2PE is a prudent security counter measure.

EMV MIGRATION CONSIDERATION

Protect your business reputation:

$61 million- The amount of money Target has spent, according to *The Washington Post* to pay for legal fees, software updates, customer reimbursement and credit monitoring due to failure in cyber security. However, there is no amount of money that can pay for consumer confidence; Consumers are the merchants' greatest assets and Target is still struggling to regain their confidence.

Cost efficiency:

$188 - The dollar amount for each record lost according to the 2013 Data Breach Study conducted by Ponemon Institute and Symantec. For a small, single-location merchant processing 6,000 unique transactions a year, the data breach risk is $1,128,000, enough to bankrupt the merchant. Thus, businesses should focus on P2PE with EMV technology which is exponentially more cost effective in the wake of a breach.

CONCLUSION

From start to finish, upgrading a payment system to the EMV standard can take up to 22 months. In order to be ready for the October 2015 deadline, anyone migrating to EMV should have started with their EMV transition back in January 2014. However, that does not mean that merchants, ISVs, VARs and integrators are too late to meet the October 2015 deadline – regardless of where they are in the process.

Given the monumental risk, costs and uncertainty associated with being the least EMV-compliant party by October 2015, many payment solution providers are determining the best approach to accomplish the migration to EMV. On one hand, organizations may navigate the inexplicably complicated process alone, using in-house expertise. The alternative is to partner with an EMV-ready payments solution provider with experience and track record in delivering EMV solutions, such as Creditcall. The benefit in leveraging the latter is that an EMV-ready solution provider will accelerate the EMV Migration process by reducing risk, operational resources and necessary skill requirements.

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

Merchants need to realize the responsibility that they have to their customers – their greatest asset – to not be the next Home Depot or Target and have to reactively update data security. They proactively need to protect customers' valuable data while ISVs, VARs and integrators need to develop EMV-ready POS solutions. Home Depot and Target are among well-known brands who have since signed on to a plan to activate EMV support in their point-of-sale devices by January 2015 as part of the BuySecure Initiative that Obama enacted.

The takeaway on the road to EMV adoption is to:

1. Start NOW – EMV Migration can take up to 22 months, it won't happen at the push of a button
2. Ensure the safest payment system possible by combining EMV with P2PE
3. Don't reinvent the wheel – partner with an experienced EMV solution provider

While the woolly world of EMV Migration will come with expected growing pains, there are experienced EMV-ready partners, like Creditcall, available to help ease the burden. Experts in the field can ensure that organizations are set to complete an EMV Migration in the most efficient and effective manner.

Given the monumental risk, an EMV-ready solution provider will accelerate the EMV Migration process by reducing risk, operational resources and necessary skill requirements.

ABOUT CREDITCALL

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

Need to get your POS or mPOS solution EMV-ready? Creditcall can help with ChipDNA - a rapid EMV Migration SDK for Windows, Linux, iOS and Android, enabling ISVs and VARs to transition from magnetic stripe technology to EMV. ChipDNA is the easiest and most cost effective way of adding EMV payment functionality into your POS or mPOS application now!

Get your POS and mPOS solution EMV ready:

Call: (800) 868-1832

Learn more at: www.creditcall.com/ChipDNA

For the latest EMV news, follow us on Twitter @Creditcall

Creditcall – The Heart of Payments.