Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

EMV Compliance in the U.S.

Now is the time to make the transition to EMV

People matter, results count.

Contents

1. Highlights

In 1994, Europay, Mastercard, and Visa came together to develop an Integrated Circuit Card Specification which would ensure global interoperability of smart card-based payments. What emerged was the EMV standard, which has rapidly emerged as the global standard for smart card-based payments. By 2011, 75.9% of terminals and 42.4% of cards globally were EMV-compliant[1]. EMV, with its enhanced security features, has also had a documented success[2] in reducing fraud in regions where it has been adopted.

The U.S. payments industry, however, continues to rely on magnetic stripe cards. These cards are more vulnerable to fraud than EMV-compliant cards. As a result, U.S. travelers are increasingly finding that their magnetic stripe cards are not accepted in EMV-compliant regions.

In this whitepaper, we will analyze the impact of non-compliance with EMV standards on the U.S. payments industry and will also look at the objections which have been blocking migration to EMV. We will also look at the benefits which the industry is expected to reap if it chooses to adopt EMV standards. Finally, we will propose a set of considerations relevant to different payments participants—issuers, acquirers, and merchants—which should be considered to ensure a smooth and successful migration to EMV standards in the U.S.

[1] The Migration to EMV Chip Technology, Gemalto, 2011

[2] Financial Fraud Action UK, Press Release, 7th March 2012; http://www.financialfraudaction.org.uk

2. Introduction to EMV

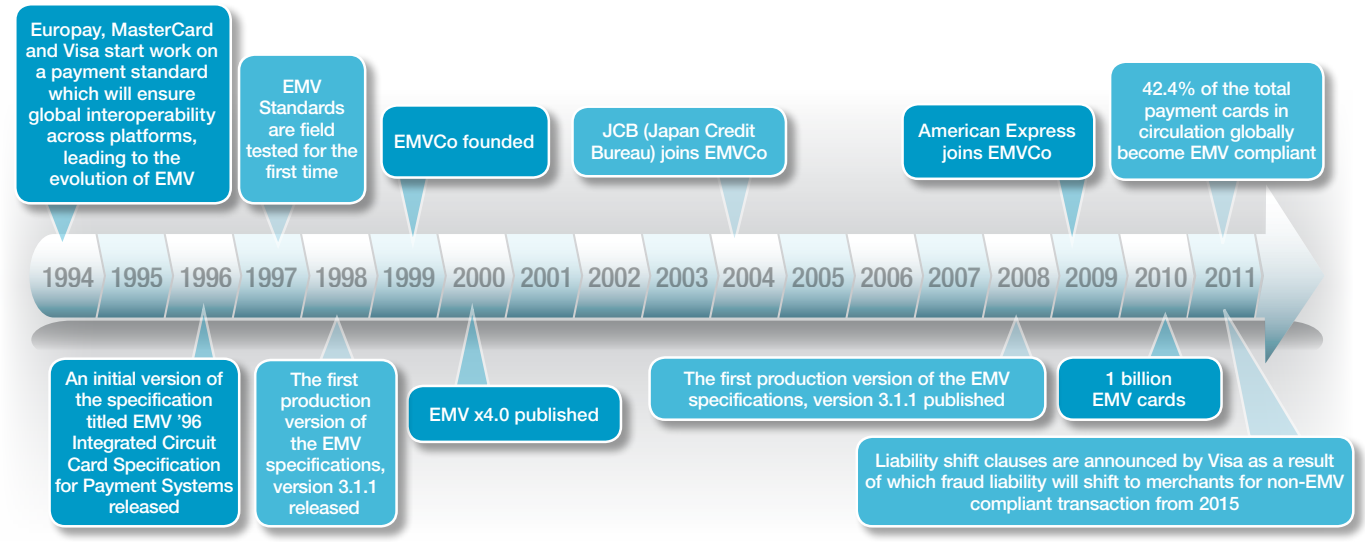
First conceptualized in 1994, EMV has rapidly emerged as the global standard for smart-card-based payments.

Europay, MasterCard, and Visa jointly developed EMV in 1994 as an Integrated Circuit Card Specification[3]. The primary objective behind the creation of EMV was to ensure global interoperability of smart card-based payments. Their goal was to ensure that all cards get accepted at all devices irrespective of their issuers, manufacturers, acquirers, or terminals.

Over the years, EMV has rapidly gained acceptance across major markets as the preferred standard for smart card-based payments, driven mainly by its ability to:

- Prevent fraud through chip authentication (thereby reducing the risk of unauthorized payments)
- Facilitate offline authentication (thereby reducing customer servicing time)
- Facilitate the implementation of customer retention programs.

Exhibit 1: The Evolution of EMV



Source: Capgemini Analysis, 2012; A Guide to EMV, EMVCo, May 2011

[3] The Integrated Circuit Card (ICC) or chip (can be either contact or contactless) stores the consumer payment application, performs cryptographic functions (thereby providing transaction security), and additional relevant information such as customer data.

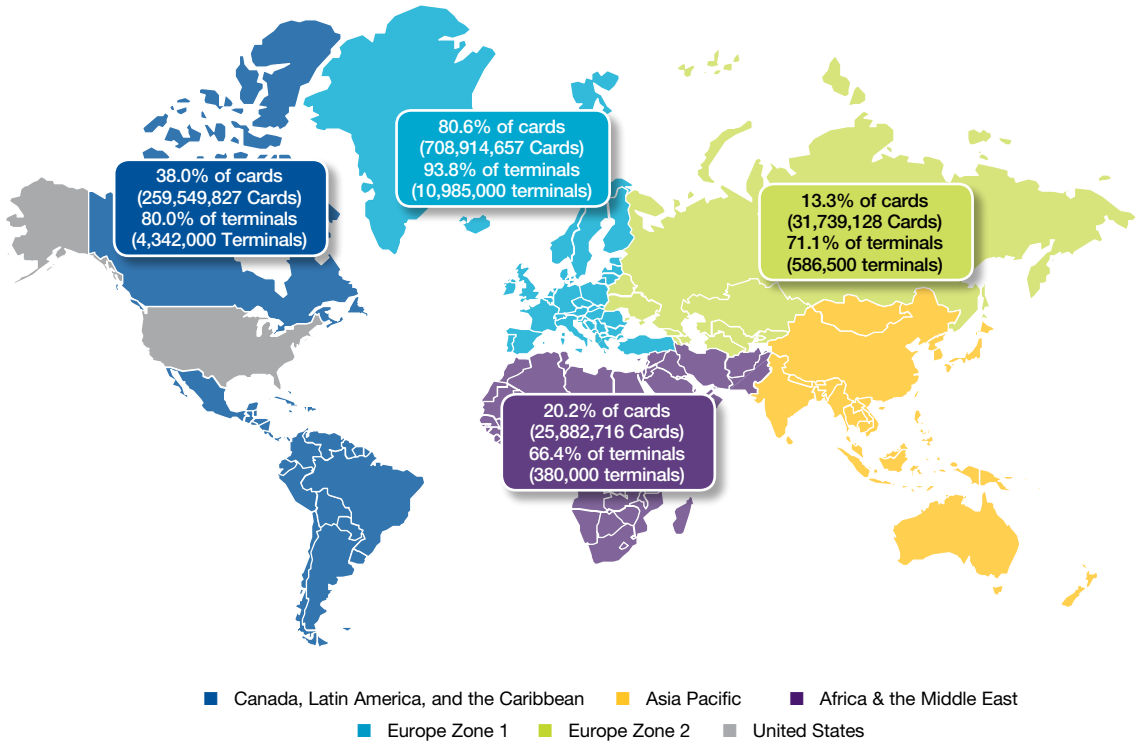
Market penetration of EMV technology deployment has been growing around the world with Compound Annual Growth Rates of 43% for cards and 48% for terminals between 2003 and 2010.

2.1. Current State of EMV Compliance Globally

EMV technology deployment has proceeded at an impressive rate across major geographical areas (with the exception of the U.S.) with Compound Annual Growth Rates of 43.0% and 48.0% being registered for cards and terminals respectively between 2003 and 2010. By the third quarter of 2011, 42.4% of the total payment cards in circulation and 75.9% of the POS terminals installed globally were EMV-compliant.

Western Europe has been at the forefront of EMV adoption with 84.7% of terminals and 65.4% of cards being EMV-compliant by the first quarter of 2011.

Exhibit 2: Extent of EMV Compliance by Geographical Region, 2011



Note: **Europe Zone 1 comprises of:** Andorra, Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Greenland, Hungary, Iceland, Ireland, Israel, Italy, Liechtenstein, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Caledonia, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, and UK

Europe Zone 2 comprises of: Albania, Armenia, Azerbaijan, Belarus, Bosnia & Herzegovina, Croatia, Georgia, Kazakhstan, Kyrgyzstan, Macedonia, Moldova, Serbia & Montenegro, Tajikistan, Turkmenistan, Russia, Ukraine, and Uzbekistan

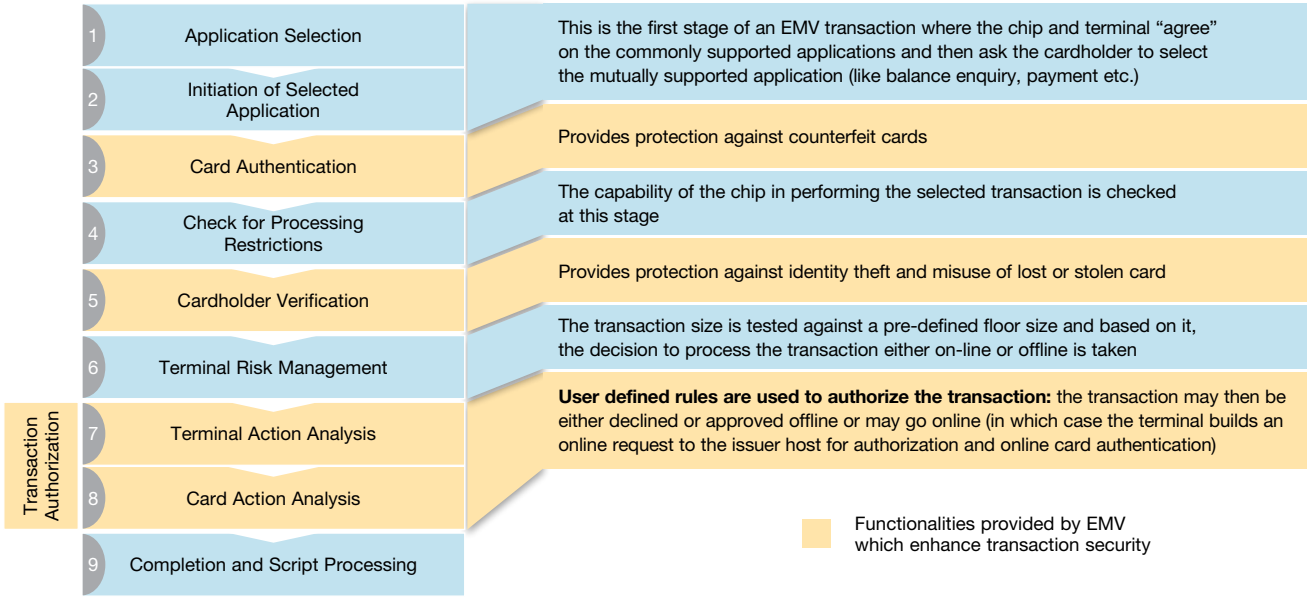
Source: Capgemini Analysis, 2012; The Migration to EMV Chip Technology, Gemalto, 2011; EMVCo, EMV Deployemnt Stats, Q3 2011

2.2. Security Features Provided By EMV

The main driver behind the rapid adoption of EMV standards globally has been the enhanced card security features it provides. These features—which help ensure greater transaction security and prevent fraud—include card authentication, cardholder verification, and transaction authorization which make it a highly secure payment standard.

The following exhibit outlines the various stages of a typical EMV transaction and briefly explains the actions which are taken at each stage.

Exhibit 3: Process Flow of An EMV Transaction



Source: Capgemini Analysis, 2012; A Guide to EMV, EMVCo, May 2011

EMV's card authentication, cardholder verification, and transaction authorization features enhance transaction security.

Card Authentication

EMV provides both online as well as offline methods of card authentication, which vary in their degree of simplicity and security.

The simplest offline card authentication method that EMV provides is **Static Data Authentication (SDA)** which relies on a public key infrastructure with the payment brands acting as the certificate authority and providing public key certificates to participating issuers. Card personalization in SDA is achieved by the issuer using his private key to sign a set of card specific data and then loading it on the card along with his public key. Authentication is achieved by the terminal validating the issuer's public key certificate using the payment brand's public root key, and then extracting the issuer's public key from the validated certificate and using it to validate the static data on the card.

Dynamic Data Authentication (DDA) is more secure than SDA and provides protection against card skimming and counterfeiting. It relies on an asymmetric key pair being generated for each card in addition to the issuer key pair. Authentication is achieved on the lines of the authentication process in SDA. The only difference is that a random number is also sent to the card for signing by its private key.

Combined DDA (CDA) is the most secure form of offline card authentication and combines the functionalities of DDA with an application cryptogram which ensures the integrity of transaction data even after its completion, preventing post-authentication fraud.

Online Authentication is the most secure form of card authentication in EMV. First, an Authorization Request Cryptogram (ARQC) is generated by the card by applying an algorithm to the device, card, and transaction data. All data is then encrypted by the card with a Triple Data Encryption Algorithm (TDEA). Finally, the cryptogram is sent online to the issuer to authenticate. Since some of the data used in the cryptogram generation varies for each transaction, the resulting cryptogram is unique for each transaction, which in turn ensures protection against card-present counterfeit fraud.

Online PIN is the most secure Card Verification Method whereas "no CVM" is the least secure.

Cardholder Verification

EMV provides four different card verification methods (CVM): offline PIN, online PIN, signature verification, and 'no CVM.'

Cardholder verification using **offline PIN** is achieved by comparing the PIN that a cardholder enters at a POS terminal with the PIN which is stored in the card, and sending the result of the comparison to the issuer host for authorization.

On the other hand, when the cardholder verification is done using an **online PIN**, the PIN is encrypted (using Triple Data Encryption Standard or TDES) and sent to the host for validation when the cardholder enters his PIN at the POS terminal. The online PIN is not stored on the card and is sent online to the issuer to validate. The decision to choose offline/online PIN is taken by the issuer based on the level of infrastructure support available.

The third form of cardholder verification is **signature verification** which requires the written signature of the customer at the POS terminal and relies on the comparison of signatures on the receipt and the back of the card for verification.

The last and least secure form of cardholder verification is "**no CVM**" which is typically used for low value transactions or for transactions at unattended POS locations.

Transaction Authentication

EMV supports both online and offline forms of transaction authentication. In **online authentication**, the transaction information and a transaction specific cryptogram are sent to the issuer who may subsequently either accept or reject them. Even magnetic stripe cards, which are prevalently used in the U.S. today, use the online form of transaction authentication.

In **offline transaction authentication**, authentication is achieved using issuer-defined risk parameters set in the card. Typically, offline authentication is used at places where terminals do not have online connectivity or where telecommunication costs are too high.

3. Current State of the U.S. Cards Market

> "The U.S. has a disproportionate percentage of the global fraud losses for two reasons . . . banks in the U.S. have been slow to adopt newer technologies such as EMV chip cards, and issuers are reluctant to decline card authorization from merchants because they don't want to alienate their cardholder"
>
> **David Robertson**
> The Nilson Report,
> November 21, 2011

The card market in the U.S. is highly developed with nearly 1.4 billion credit cards being in circulation in the U.S. currently (approximately 4.5 cards per person)[4]. Nearly 77% of the population, or roughly 181 million persons, hold a credit card. Credit cards are used more than 20 billion times a year with a total transaction volume of $1.9 trillion which is equivalent to roughly 12.9% of the country's GDP. However, overt reliance on magnetic stripe cards has made the U.S. payments industry highly susceptible to fraud, with the country accounting for nearly 47% of global fraud losses even though it accounts for only 27% of the global volume of purchases.

The following exhibit presents a comparative study of security features for EMV and magnetic stripe cards.

Exhibit 4: Security Features Comparison of EMV versus Magnetic Stripe Cards

Security Feature	EMV-compliant Card	Magnetic Stripe Card	Security Feature Flaw in Magnetic Stripe Card
Card Possession	Cardholder retains possession of contactless EMV chip cards and taps the card on a reader	Cardholders typically give their cards to a sales clerk in all other POS environments	The potential for skimming data from the card increases when the card leaves the cardholder's possession
Card Design	Card is based on highly secure smart chip technology which makes EMV chip card extremely difficult to counterfeit	Magnetic stripe data can easily be skimmed from a card or stolen from non-PCI- DSS compliant data network or storage	Skimmed card data can be used to create a counterfeit card
Transaction Security	EMV chip card transaction produces a unique transaction code that does not allow reuse or replay of transaction data	Magnetic stripe card carries static data	Static data if skimmed or stolen, can easily be used to make a counterfeit magnetic stripe card
Card Authentication	EMV chip card allows authentication of the payment card for both online and offline transactions	No card authentication is possible for ISO standard magnetic stripe cards	Lack of card authentication exposes the magnetic stripe card to counterfeit fraud

Source: Capgemini Analysis, 2012; European Payment Card Fraud Report, 2010; Six Myths Preventing EMV Migration in the U.S., Bell ID, 2011; The Migration to EMV Chip Technology, Gemalto, 2011; Top 10 Reasons the U.S. Should Consider EMV, Smart Card Alliance, 2010; Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud, Smart Card Alliance, 2009

In 2010 alone, payment fraud losses in the U.S. totaled a staggering $3.6 billion. Cost of fraud in the United States is $8.6 billion per year[5] or 0.4% of the $2.1 trillion card payment industry; these losses are rising and are expected to reach $10 billion per year by 2015. Adoption of EMV payment standards which have had a documented success in reducing fraud losses should have been the natural solution to this problem. However, a number of roadblocks impede its successful adoption in the U.S.

[4] 2011 Credit Card Facts & Statistics, Richard Barrington, Indexcreditcards.com
[5] Per estimate published by the Aite group (http://www.aitegroup.com/Reports/ReportDetail.aspx?recordItemID=625). These fraud losses may actually be dramatically underreported with estimates by Mercator Advisory Group pegging the loss estimates at $16 billion per year

3.1. Roadblocks to the Adoption of EMV in the U.S.

In this section we discuss some of the capability, business, and implementation-related issues which have hindered the adoption of EMV standards in the U.S. Strong counter arguments exist which diminish the strength of these objections.

Most of the objections to EVM's capability are unfounded and can be remedied through stakeholder education.

Capability-Related Issues

Though several issues pertaining to the capability of EMV in preventing fraud have been raised, most of them are borne of a lack of understanding of EMV's capabilities and are thus unfounded.

EMV is an outdated technology: Several payment participants consider EMV to be an outdated technology which applies only to contact chip cards. In reality, EMV specifications are continually reviewed, amended, and updated by EMVCo (which develops and maintains EMV standards) in a backward-compatible manner which prevents any interoperability issues from arising.

EMV is not secure: Recent research conducted by a group of U.K.-based researchers demonstrated the possibility of bypassing pin verification of EMV cards by routing the card to terminal communication through a fake card. This has led many to question the security of EMV standards. In actuality, the EMV card which was cracked by the researchers did not comply with current card security standards.[6] The design of EMV also allows it to adopt interchangeable encryption algorithms and variable key lengths. Even the compliance status of facilities producing EMV cards is checked on an annual basis.

EMV does not ensure fraud prevention: EMV has also been criticized for just causing fraud to migrate from a card present to a card not present (CNP) environment, and thus being ineffective in ensuring fraud prevention. However, in conjunction with measures for countering CNP fraud such as two-factor authentication techniques (3-D secure, CAP, and DPA) and Short Message Service (SMS) authorization codes, EMV has been proven to be extremely effective in preventing even CNP fraud.[6]

EMV will make transaction processing slow: Another objection against EMV adoption has been that it makes transaction processing slower when benchmarked against processing time of a magnetic stripe card transaction. However, the slight increase in transaction time for an EMV transaction needs to be weighed against the enhanced transaction security that it provides. Moreover, by using multi-threading and parallel processing, EMV-based terminals tend to be much faster than their magnetic stripe counterparts.

[6] *Six Myths Preventing EMV Migration in the U.S.,* Bell ID, 2011

Business-Related Issues

Though issuers fear loss of interchange fees and merchants believe that EMV adoption will make investments made in PCI DSS compliance a waste, they tend to overlook the fact that saving in fraud costs (which will accrue to the industry from EMV compliance) will more than compensate the firms and industry for cost incurred due to EMV adoption.

Negative impact on interchange fees: One of the greatest objections that EMV has faced in the U.S. has been the negative impact that it may have on issuers' interchange fees. Typically, an issuer derives higher interchange fees from a signature-based transaction as compared to a PIN-based transaction. It is estimated that migration to EMV may result in a loss of $1.7 billion per year for issuers in interchange fees. However, fraud losses in the U.S. amount to about $6.9 billion per year. So it actually makes good business sense to forgo some interchange revenues in exchange for the reduction in fraud losses which EMV may bring.

Absence of a Positive Business Case: It has often been argued that no positive business case exists for EMV implementation in the U.S. While this argument might have been relevant a decade ago when the cost of implementation might have seemed prohibitive, in today's context it has been rendered inapplicable. Costs of chip cards and POS terminals have declined significantly over the years while the cost of alternative measures used by the industry for detecting and mitigating fraud has increased significantly. Besides, the cost of fraud is not limited to direct fraud losses. It includes fraud management and other indirect expenses, which according to an estimate by Visa, are at least equal to the direct fraud costs. Finally, a substantial number of POS terminals in the U.S. have chip-ready hardware capabilities onto which the EMV software can simply be downloaded.

Waste of Investments Made in PCI-DSS Compliance: Many merchants are opposed to EMV adoption on the grounds that migration to EMV standards will render futile the huge investments made by them for becoming compliant with PCI-DSS. However, merchants seem to ignore the huge costs that they have to incur in order to validate their compliance with PCI-DSS standards. With Visa's new Technology Innovation Program (TIP), this requirement will be waived for merchants with at least 75% of their Visa transactions originating from EMV-complaint terminals. This could result in significant cost savings for compliant merchants.

Structural and Implementation-Related Issues

The U.S. payments industry faces the threat of global fraud gravitating towards it; thus making EMV adoption an imperative. The problems that a payment participant might face while implementing EMV standards can be easily overcome by partnering with service providers who specialize in EMV implementation.

Fraud in the U.S. does not justify EMV migration costs: There is a common misconception that fraud in the U.S. does not justify the cost of EMV migration. The fact is that physical world fraud in the U.S. is already above global average and is increasing constantly.[7] Additionally, with the rest of the world making serious efforts to migrate to EMV, the U.S. payment industry is at risk of becoming the primary target of fraudsters, resulting in even higher fraud losses.

EMV implementation is too complicated: EMV implementation requires changes to several parts of the payments infrastructure and associated process, and has thus been criticized as being too difficult to implement. The fact remains that thousands of EMV migrations have been carried out globally, and a very strong support infrastructure consisting of vendors and international payment systems exists to assist participants wishing to migrate to EMV standards.

Issuers should wait for the market to settle: Some issuers are also of the belief that they can wait for the market to settle before implementing EMV. This approach is potentially dangerous as it might lead to fraud migrating to the non-compliant issuer's portfolio from issuers who adopt EMV, leading to both financial and reputational losses.

[7] The Migration to EMV Chip Technology, by Gemalto, 2011

4. EMV Compliance in the U.S.: The Time is Now

4.1. Risks Faced by the U.S. Payment Industry in the Absence of EMV Compliance

Continued use of magnetic stripe cards has resulted in U.S. travellers being inconvenienced in EMV-compliant countries.

Difficulty Faced by U.S. Cardholders in Countries that have Migrated to Chip and PIN

When travelling abroad, U.S. cardholders face problems at many EMV-compliant terminals (especially the unattended transport ticketing terminals) which may not accept magnetic stripe cards. Even in 2009, when EMV standards were still in the implementation phase across most major markets, as many as 10 million U.S. travelers faced difficulties due to non-compatible card technology. The situation going forward is expected to worsen as more countries such as Canada and Mexico migrate to EMV, and European banks begin to completely phase out support for magnetic stripe cards. Needless to say, this trend is expected to negatively impact the card usage behavior of U.S. travelers (who may choose to rely more on cash for their overseas transactions) and consequently result in loss of revenues for payment institutions.

Exhibit 5: Results of Survey of U.S. Cardholders Who Traveled Outside of the U.S. Within the Last Three Years, 2009

Customers who paid with cash when faced with an incompatible card technology problem	72%
Customers who found the experience of incompatible card technology extremely frustrating	74%
Customers who changed their card usage behavior after facing an incompatible card technology problem	71%
Customers who ended up relying more on cash in their future foreign visits after facing an incompatible card technology problem	47%
Amount of lost spend attributed to an incompatible card technology problem (incompatible card technology was the highest contributor to lost card spend)	$1,061

Source: Capgemini Analysis, 2012; Top 10 Reasons the U.S. Should Consider EMV, Smart Card Alliance, 2010

Potential of Card Fraud Concentrating in the U.S.

Since EMV has a far higher success in preventing fraud, fraud is shifting towards regions which are not yet EMV-compliant. The U.S., with its outdated magnetic stripe technology, is thus at a risk of becoming the epicenter of global fraud.

Liability Shift of Counterfeit Fraud to Merchants

Effective October 1, 2015, Visa's liability shift will result in the liability for counterfeit fraud shifting to merchants from issuers in cases where the fraud originates from a contact chip card being used at a merchant terminal which does not support contact chip cards (globally, liability shift will come in effect in most countries by 2014).[8] Thus, merchants who have not adopted EMV standards will have to cope with the additional strain of bearing counterfeit fraud costs.[9]

Non-complying merchants will not only have to bear counterfeit fraud costs but will also lose on Visa's PCI-DSS compliance waiver.

Also, starting October 1, 2012, Visa's Technology Innovation Program (TIP) will be extended to the U.S., resulting in the PCI-DSS annual validation requirement being waived for merchants with at least 75% of their Visa transactions originating from EMV-complaint terminals. To be eligible for the program, the terminals need to be able to support both contact as well as contactless payments, including mobile contactless payments. By sticking with magnetic stripe cards, merchants in the U.S. will have to forgo the savings which would have accrued from the waiving of the PCI-DSS annual validation requirement.

4.2. Key Potential Benefits from EMV Compliance

Springboard for Growing Mobile Payments

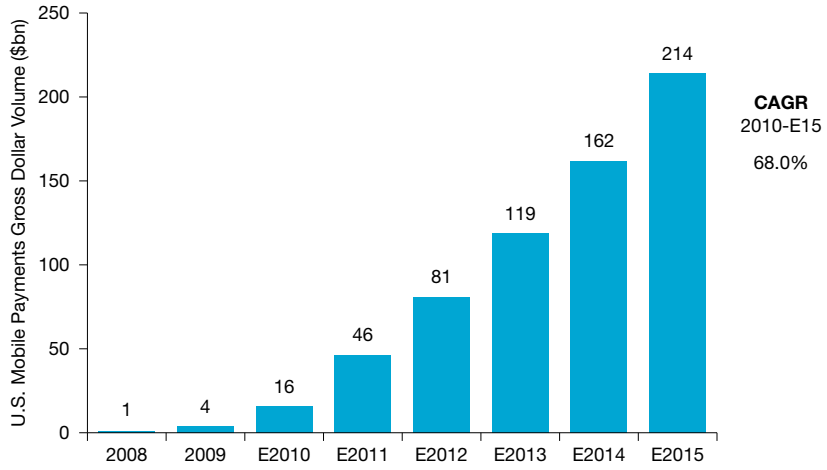
Mobile payments have been gaining rapid acceptance in the U.S. According to estimates, the gross dollar volume of U.S. mobile payments is expected to grow to $214 billion by 2015.

Both EMV and mobile payments require similar back-end infrastructure. For example, the ISO/IEC 14443 communication protocol which is used by EMV is also used for Near Field Communication (NFC)[10] payment transactions between a POS device and mobiles. Moreover, an EMV device is typically a dual contact/contactless device, which means that its installation will prepare the merchant for mobile payments too.

[8] For fuel dispensers the liability shift will apply from 2017
[9] Six Myths Preventing EMV Migration in the U.S. Fact vs. Fiction, Bell ID, 2011
[10] NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimetres apart.16 NFC-enabled mobile phones incorporate smart chips (called secure elements) that allow the phones to securely store the payment application and consumer account information and to use the information as a "virtual payment card."

A critical factor in the acceptance of mobile payments in the U.S. is that they be based on a standard infrastructure such as EMV.

Exhibit 6: The U.S. Mobile Payments Gross Dollar Volume ($B), 2008-E15



Source: Capgemini Analysis, 2012; EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions, FirstData, 2011; The Migration to EMV Chip Technology; U.S. Mobile Payments: The Time Has Come, Gwenn Bézard, Aite Group LLC, November 2010

EMV adoption can also play a critical role in increasing NFC mobile payments. Here are two examples of EMV mobile NFC trials that highlight the usability and security of EMV-based mobile NFC payments:

- **Launch of Middle East's First EMV-Chip Compliant NFC Mobile Payment Trial:** Between October 2009 and April 2010, National Bank of Kuwait, Visa, and Zain Bank partnered to launch a trial on NFC-enabled Nokia 6212 mobile phone, giving 500 selected cardholders access to their Zain credit card details on their phones. These cardholders could then use their mobile phones to make purchases across 100 merchant outlets in Kuwait's largest mall, The Avenues. This trial, which heightened flexibility and convenience to customers, was based on EMV technology. Through this trial, NBK, Visa, and Zain could gather user insight across a wide range of parameters such as customer acceptance of making contactless transactions through mobile NFC and customer response to NFC-enabled smart posters and coupon redemptions.
- **NFC Trial at Mobile World Congress, 2010:** 400 Samsung Star NFC handsets were distributed to selected Mobile World Congress attendees on February 15, 2010. The personalization of the NFC-enabled sim cards was done with a La Caixa Visa Mobile Payment application which allowed the phone to make EMV mobile payments. Using these phones, users could pay for food and drinks at 30 merchant locations across the congress in a speedier and hassle-free manner.

EMV adoption was the main driver behind a reduction in fraud losses in the U.K, which declined by 45% between 2008 and 2011.

Enhanced Bottom Line

Adoption of EMV standards boosts the bottom line of participants by reducing counterfeit fraud cost as well as by creating new revenue sources and enhancing productivity.

As discussed earlier, fraud cost in the U.S. is expected to reach $10 billion by 2015. Apart from this direct cost, issuers also have to bear reissuance cost ($25 per event), suffer reduced reactivation rates (roughly 20% of customers affected by fraud do not reactivate their accounts), make additional spending on recouping lost business ($200 per customer), and suffer from reduced transaction volumes and consequently lower realized revenue (30% of customers effected by fraud end up using their cards less frequently). Considering that EMV migration is expected to cost the industry roughly $8.6 billion[11] and that EMV has had a documented success in mitigating counterfeit fraud, the cost of EMV migration could be recovered within the first year itself.

Exhibit 7: Card Fraud on UK-issued Credit and Debit Cards, (£MM), 2007-11[12]

	2007	2008	2009	2010	2011	% +/- 10/11
Card Not Present Fraud	290.5	328.4	266.4	226.9	220.9	(3%)
Counterfeit Fraud	144.3	169.8	80.9	47.6	36.1	(24%)
Card ID Theft	34.1	47.4	38.2	38.1	22.5	(41%)
UK Retail Face to Face Transactions	73.0	98.5	71.8	67.4	43.2	(36%)
UK Card Machine Fraud	35.0	45.7	36.7	33.2	29.3	(12%)

Source: Capgemini Analysis, 2012; Financial Fraud Action UK, Press Release, 7th March 2012; http://www.financialfraudaction.org.uk

To highlight the impact that EMV has on fraud losses, consider the case of the U.K. payments industry. The U.K. migrated to EMV standards in 2004. As a result, there has been a consistent decline in fraud losses in its payments industry. Fraud losses declined by 7% between 2010 and 2011. By 2011, fraud losses in the U.K. were at their lowest since 2000. Integrated circuit card verification value (iCVV), launched on January 1, 2008, has further helped the industry tackle the type of fraud wherein fraudsters harvest card details by tampering with terminals[13].

[11] US: To EMV Or Not? by Jim Schlegel, May 1, 2010, American Banker
[12] U.K. started EMV implementation in 2004, however U.K. Card Association (which is the most authentic and oft quoted source for payments related data from the U.K. card market) provides data on fraud figures from 2007 onwards, as a result depiction of pre and post EMV implementation fraud situation is not possible here
[13] Card fraud loss rate declined 83% from 18 to 10 basis points from 2001 to 2009; http://www.financialfraudaction.org.uk/cms/assets/1/end%20of%20year%20fraud%20figures%20final.pdf

Apart from fraud reduction, EMV-compliant chip cards also facilitate the launch of additional services such as loyalty programs and marketing schemes. Merchants can also realize savings from the replacement of signed paper slips with electronic records. Finally, productivity is expected to increase because of the streamlining of the checkout process at POS, the cashier's day-end book balancing, and cash handling.

Increased Customer Satisfaction

Migration to EMV standards will ensure that U.S. travelers to EMV-compliant countries do not face the problems of non-acceptance of magnetic stripe cards which they currently face. The overall positive shopping experience of customers is expected to increase as most EMV-enabled terminals can accept contactless and mobile payments, which provide faster check-out time and greater convenience—especially for low-value transactions.

4.3. Recent Developments in the U.S. in the Field of EMV Compliance

Recent years have witnessed the U.S. payments industry moving towards migration to EMV standards. Fraud reduction and an improved experience for U.S. travelers have been the major drivers behind this trend. With several major banks such as JPMorgan Chase & Co., Citibank, and Bank of America acknowledging the benefits of EMV, the prospects of its adoption in the U.S. looks optimistic with rapid progress expected in the near future.

Exhibit 8: Recent Developments in the Field of EMV Compliance in the U.S.

October 2010	United Nations Federal Credit Union became the first the U.S. institution to offer its customers EMV cards
December 2010	Travelex introduced a pre-paid foreign currency Chip and PIN card denominated in Euros and pound sterling for U.S. travelers abroad
October 2010	State Employees Credit Union announced its plan to convert its entire 1-million-card debit portfolio to EMV chips
February 2011	Wells Fargo & Co., the U.S. bank with the most branches, began testing microchip-embedded credit cards with frequent travelers to address complaints of customers who have trouble using their cards abroad
July 2011	Silicon Valley Bank (SVB) began providing chip-enabled, or Smart, credit cards available to businesses in the U.S.
June 2011	The U.S. bank announced that it will offer its international travelers EMV cards
June 2011	JPMorgan Chase & Co. announced that it will begin issuing its J.P. Morgan Select Visa Signature card with EMV chip technology, the second in its card portfolio—following the J.P. Morgan Palladium Card—to sport the smart chip
June 2011	The Payment Processing Solutions (PPS) division of Jack Henry & Associates announced it will begin offering chip-and-signature debit and credit cards to its credit union customers
August 2011	PSCU Financial Services began offering its entire member-owner base of 680 credit unions new credit cards that carry both EMV chip-and-PIN security and traditional magnetic stripes
August 2011	Citi announced the launch of the Citi Corporate Chip and PIN card, a compliant smart card designed for the U.S. corporate cardholders traveling abroad
November 2011	Bank of America decided to roll out chip-and-pin business cards in 2012

Source: Capgemini Analysis, 2012; EMV Resources, Smart Card Alliance, http://www.smartcardalliance.org/pages/smart-cards-applications-emv

4.4. Cost of EMV Compliance in the U.S.

Divergent estimates for the cost of EMV migration are available with most pegging the cost of migration between $5 billion and $13 billion. Most of this cost is however expected to be recovered from card holders in the form of service fees.

Merchants who will have to deal with POS terminal deployment will be the hardest hit and may have to pay as much as $6.75 billion to become EMV-complaint. The silver lining for them is Visa's Technology Innovation Program, which might help them avoid spending on PCI-DSS annual validation.

Exhibit 9: Cost of EMV Compliance in the U.S.

Cost Type	Current Situation	Cost	Who Bears the Cost
POS Terminal Deployment	The U.S. currently has more than 15 million point-of-sale devices. In the U.S. merchants typically procure their own POS hardware and software, before integrating with an acquirer. Small and mid-sized merchants do not benefit from economies of scale when buying their POS terminals. Multi-lane merchants are likely to spend at least $500 per lane in the migration process.	$6.75B	Merchants
Card Issuance	The U.S. currently has 609.8 million credit cards, and 520 million debit cards. Magnetic stripe cards cost as little as $1.11 each, while EMV cards can cost between $2.25 and $10.	$1.4B	Issuers
Retrofitting or Replacing Bank-Owned ATMs	The U.S. currently has more than 360,000 automated teller machines. ATMs currently installed in the U.S. today support magnetic stripe cards only. Chip cards are used typically as part of closed campus implementations, rather than at public ATMs; contactless cards are also used for POS transactions, not at ATMs.	$0.5B	Financial Institutions
	Total Cost	**$8.6B**	**Payments Industry**

Source: Capgemini Analysis, 2012; US: To EMV Or Not? by Jim Schlegel, May 1, 2010, American Banker; Six Myths Preventing EMV Migration in the U.S., Bell ID, 2011; EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions; FirstData, 2011; Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?, Smart Card Alliance, 2011

Card issuance is expected to cost around $1.4 billion and will have to be borne mainly by issuers. Financial institutions will have to bear the cost of renovating and replacing bank-owned ATMs, which might cost as much as $500 million. The good news for them is that most new ATMs do not need to be replaced to accept EMV cards. EMV-capable terminals have been available from most ATM manufacturers for at least 5-7 years.

5 Roadmap for EMV Compliance in the U.S.

In order to be fully prepared for adoption of EMV standards, the U.S. payments industry needs to take into consideration several important factors.

5.1. Considerations Relevant to Card Issuers

Preserving brand, choosing card applications, and deciding the prefixes to use are some of the key considerations for issuers.

Issuers will have to take several decisions, significant among which are: preserving the brand in face of card design changes, deciding on the application and BIN/ prefixes to use, deciding on the chip functionalities to support, and deciding on a chip issuance strategy.

Brand Preservation

The card, with the issuer's logo on it, is a key brand promotion and reinforcement tool. Transitioning to EMV standards will require a chip to be placed on the card which will alter its design. However, regulations are very specific about the exact placement of the chip on the card. Reusing the magnetic strip card design without relocating logos might be difficult for issuers. Issuers might also like to retain magnetic stripes on their cards so as to enable use at non-chip-enabled POS terminals.

Which Products to Use

Choosing the right product is another key consideration for issuers. They can choose to implement either contact or contactless cards depending upon how they see the payments industry evolving in the future and the degree to which they may want to future-proof their solutions. Issuers need to make the choice between issuing chip cards with existing BINs/prefixes and using new BINs/prefixes. In the latter case, the new BIN can be an extended BIN (sharing the first 'n' digits with the BIN owned by the issuer) in which case the issuer can establish host parameters for card authorization by BIN. Or the BIN might be a completely new short BIN which can be used to distinguish cards by function, service, and products.

Which Chip Applications to Use

When it comes to applications to include on the cards, an issuer's choice might be limited by the mandates of associations, switch networks, and regulators. If however the issuer has a choice, the priority should be take the views of her card/ switch network into consideration and then chose an application which is pre-certified (so as to get cards into production faster). Alternatively, if issuers choose to develop their own ICC application, they need to factor in the additional time which might be required for getting the application certified. While deciding on the functionalities to be included in the card, issuers should always focus on supporting those functionalities which allows them to get the chip card into the market in the shortest possible time-span while conforming to EMV standards.

How to Handle Transition from Non-PIN to PIN-Based System[14]

Issuers may also have to decide whether or not they want to allow their customers to use the PIN from their magnetic stripe cards for their chip cards. If so, issuers need to have these existing PINs in their databases and will have to pass them on to card manufacturers for card personalization. Doing this might prove difficult. Many organizations do not maintain a record of PINs and rely on PIN offset (which can be stored on the stripe card) for PIN verification. Alternatively, the PIN may be stored in an encrypted format on the chip card which will help in carrying out functions such as offline card verification at chip-enabled terminals.

Whether to Support the PIN Change Function

Issuers will also have to decide how they wish the PIN change function to be carried out. Allowing PIN change to be carried out only at branches might result in diminished customer satisfaction. On the other hand, if the issuers allow PIN change at ATMs, then the cards as well as the host systems will need to carry the requisite features and programs to support this functionality.

How to Perform Chip Card Authentication[15]

Issuers have a choice between performing the chip card authentication task themselves, in which case they need to have in place the appropriate chip card authentication keys and cryptograms as well as an appropriate hardware security module (HSM). Alternatively, if they choose to use the services of a network for performing the authentication, then they need to provide the network with the requisite keys and cryptograms.

How to Handle Technology Transition

Issuers will also have to plan for the technological transition which will result from migration to EMV standards. For this, they should factor in functional aspects such as transition of legacy back-end systems to chip-ready systems and training of functional staff. They also need to consider database migration issues such as choosing between a phased or one-go approach towards migration of the database. Finally, issuers should also develop a customer education program which focuses on notifying and training customers about all functional aspects of chip-based cards.

[14] In order to reduce the barriers to EMV adoption, Visa is actually promoting the idea of signature verification, thus, pin transition to pin-based system might not be an immediate consideration

[15] In order to reduce the burden on banks Visa is keen to perform the card authentication itself

5.2. Considerations Relevant to Acquirers

Considerations relevant to card acquirers include identification of network inventory, and identification of certification, testing, training, and infrastructure related requirements.

Identifying and Optimizing the Network Inventory

From an infrastructural viewpoint the key priority for acquirers would be to take stock of their network, starting with the identification of the makes and models of their ATMs and the hardware/software being used in them. The objective is to categorize their inventory into terminals which can be retrofitted and those which need to be replaced. The acquirer would then have to factor the direct costs, such as cost of purchasing equipment, price of third-party service agreements and vendor maintenance agreements, and associated costs such as testing, consultation, and development costs.

The strategy of acquirers at this stage should be to minimize the number of terminal types that they support, so as to extract more favorable terms from vendors. Acquirers should also take care that the terminal vendors they enter into a relationship with, have both level 1 (interface/card reader functions) and level 2 (terminal software application functions) certifications, and that the devices and kernels supplied by them are already in use (so that they do not get put into the position of being a beta tester for the vendor).

Changes to Physical Structure and Infrastructure

Acquirers will need to take into consideration changes to physical structure and technical infrastructure which might be required for migration to EMV standards. For example, brick-and-mortar-level changes might be required at ATM locations, such as the replacement of through-the-wall ATMs which may require remodeling of the location and could have a significant impact on budget and timelines. Acquirers will also need to ensure that their online transaction processing and batch processing software have the capability to process EMV data.

Devising a Launch Strategy

Acquirers need to identify controlled and friendly locations where EMV devices can be launched first (possible examples being office premises and employee cafeterias) so that any implementation-related issues may be resolved before publicly launching the EMV devices.

At a functional level, acquirers will to take the following into consideration:

Determination of the Functionalities to be Offered to Chip Card Users

Acquirers will need to decide whether they wish to offer the same transaction set to their chip-card users as they offered to their magnetic stripe card users. This decision is closely linked to the choice of devices that the acquirer makes.

Determination of Certification Requirements

Acquirers will have to ascertain the certifications they need to complete in order to comply with the requirements of their association/switch network. Typically, apart from the Level 1 and Level 2 certifications of EMVCo, an acquirer might be required to complete the following certifications:

- Terminal application-level certification, known as a) Terminal Interface Process (TIP) for MasterCard and b) Acquirer Device Validation Testing (ADVT) for Visa
- MasterCard/Visa acquirer functional certification
- Other (national or regional) financial network/switch certifications

Determination of Testing and Training Requirements

The acquirer will have to carry out regression testing to ensure that migration to EMV standards did not adversely impact current processes. Stress and load testing too would have to be carried out to ensure that systems are ready to handle the anticipated increase in transaction volumes. Finally, disaster recovery systems will have to be tested to ensure that no further modifications are needed in support of chip-enabled devices.

Acquirers will also need to train their operations team about the system log and error messages which might be generated by EMV devices. Internal training of branch personnel will have to be carried out to ensure that they are adequately equipped to assist customers about the usage and operation of chip-cards.

How to Handle Technological Transition

Finally, acquirers will need to devise their technology transition strategy wherein the primary consideration will be to decide whether to adopt a one-go or phased approach.

5.3. Considerations Relevant to Merchants

Merchants will need to identify the external and internal business drivers for EMV implementation, ascertain the cost of migration, determine the business impact of migration, and identify timelines in which they will need to complete the migration.

Merchants should focus on future-proofing investments, partnering with acquirers, and devising a sound implementation plan.

Identification of Business Drivers

Merchants, who will bear the greatest burden of the cost of migration to EMV standards, should start by identifying the internal and external business drivers for the transition. The greatest external driver to EMV migration would be liability shift dates as envisioned by Visa and MasterCard. While estimating the cost of fraud at this stage, merchants need to factor in not only the direct fraud costs (in absence of EMV compliance) but also the cost of fraud which will arise from fraud migrating to them from other merchants who make the shift to EMV. Internally, merchants should focus on identifying potential changes to the POS which they can leverage for boosting customer loyalty, such as issuing gift cards or launching a loyalty program.

Assessment of Potential Business Changes

The current practice of signature verification of customers is time consuming and tends to increase the customer servicing time for merchants. Migration to EMV standards would make this process obsolete. Though merchants will benefit from the decreased customer servicing time, they need to factor in the increased input (in terms of number of customers) that EMV adoption might entail and the impact it could have on cashier requirements during peak hours. If merchants operate both online as well as in retail stores, they need to factor in the cost of fraud which may migrate from the retail to the online channel. Moreover, merchants need to plan for exigencies such as handling customers who forgot their PINs and processing transactions during power failures.

Preparation of Project Timeline and Identification of Migration Cost

Merchants need to prepare a timeline for EMV implementation keeping in mind the liability shift dates. For creating an effective timeline merchants should work closely with acquirers to synchronize their EMV migration plans, and should factor in the time which might be spent on training staff, developing training material, and conducting in-store pilots.

Merchants also need to arrive at the cost of migration to EMV standards. As part of this exercise they should ascertain whether they need to shift from Datapac to an IP connection and whether they need to replace their cash registers. Moreover, they should identify and make budgetary allocations for costs involved in purchasing POS software, making back end changes, integration, training, and installation/ issuance of new PIN pads.

Focus on Future Proofing of Investments

While carrying out all the aforementioned activities the focus of merchants should be on future-proofing their EMV POS investment by making allowances (to the extent possible) for mobile payments, contactless interface, offline transactions, and NFC marketing.

6. Conclusion

In conclusion, migrating to EMV standards has become a strategic necessity for the payments industry in the U.S. With most of the developed world having already transitioned to EMV standards, the payments industry in the U.S. stands to lose a lot by further delaying the shift. Not only could the industry become the chief target of fraudsters globally, but it may also suffer revenue losses from U.S. travelers visiting EMV-compliant regions. Additionally, liability shift, which will become applicable in the U.S. shortly, will end up adversely impacting the cost structure of non-EMV-compliant merchants.

If the industry chooses to migrate to EMV standards, it has the potential to reap the benefits of reduced fraud costs, improved customer satisfaction, new revenue streams, accelerated acceptance of mobile payments, and enhanced productivity. Merchants, in particular, stand to benefit from the waiving of PCI-DSS validation requirements.

The case for the U.S. payments industry to adopt EMV standards is thus very strong, and judging by the recent spur of activity in this direction in the U.S., it can be assumed that this transition is going to pick up further momentum in the future. It is in the best interests of all payment participants to start looking at how to make this transition in a smooth and coordinated way.

All payment participants should adopt the three-stage approach of assessing-planning-executing for effecting a smooth migration. The assessment stage should typically involve obtaining an overview of one's current capabilities, understanding the capabilities which might be required due to migration to EMV standards, and indentifying the gaps that exist between the current and desired capabilities. The planning stage should focus on identifying ways of fixing the identified gaps and devising an EMV implementation strategy. The execution stage should be focused on implementation of the strategy arrived at in the planning stage. At this juncture, participants are advised to leverage the capabilities of vendors who have expertise and experience in this area.

References

1. *A Guide to EMV* by EMVCo, May 2011, http://www.emvco.com/download_agreement.aspx?id=599

2. *The Migration to EMV Chip Technology*, by Gemalto, 2011, http://pymnts.com/assets/Shared/Gemalto-EMV-Whitepaper.pdf

3. *Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?*, by Smart Card Alliance, Feb 2011, http://www.smartcardalliance.org/resources/pdf/Payments_Roadmap_in_the_US_020111.pdf

4. *2011 Credit Card Facts & Statistics*, by Richard Barrington, http://www.indexcreditcards.com/finance/creditcardstatistics/2011-report-on-credit-card-usage-facts-statistics.html

5. *Nilson Report*, by Nilson, September 2011

6. *European Payment Card Fraud Report*, 2010, http://www.paymentscardsandmobile.com/Payments-Cards-Mobile-Affiliates/fraud-report/PCM_Fraud_Report_2010.pdf

7. *Six Myths Preventing EMV Migration in the U.S.*, by Bell ID, 2011, www.finextra.com/Finextra-downloads/featuredocs/ White%20Paper%20-%20EMV%20Migration%20US%201.9.pdf

8. *Top 10 Reasons the U.S. Should Consider EMV*, by Smart Card Alliance, 2010, http://www.smartcardalliance.org/pages/activities-events-top-ten-reasons-us-should-consider-emv

9. *Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud*, by Smart Card Alliance, 2009, www.smartcardalliance.org/resources/lib/ Fraud_EMV_Contactless_20091007.pdf

10. *Chip in the U.S.- The Facts* by Toni Merschen Consulting, 2011, http://www.smartcardalliance.org/resources/pdf/Chip_in_the_US_The_Facts_090611.pdf

11. *Press Release* by Financial Fraud Action UK, 7th March 2012, http://www.financialfraudaction.org.uk/cms/assets/1/end%20of%20year%20fraud%20figures%20final.pdf

12. *EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions*, by FirstData, 2011, http://www.firstdata.com/downloads/thought-leadership/EMV_US.pdf

13. *U.S. Mobile Payments: The Time Has Come*, by Gwenn Bézard, Aite Group, 2010, http://www.aitegroup.com/Reports/ReportDetail.aspx?recordItemID=722

14. *Newsroom: Press Releases*, by VIVOtech, 2010, www.vivotech.com/newsroom/press_releases/NBK_Visa_Zain_Middle%20East.asp

15. *NFC trial begins at Mobile World Congress*, NEAR FIELD COMMUNICATIONS world, http://www.nfcworld.com/2010/02/15/ 32738/nfc-trial-begins-at-mobile-world-congress/

16. *EMV Resources*, by Smart Card Alliance, http://www.smartcardalliance.org/pages/smart-cards-applications-emv

17. *US: To EMV Or Not?*, by Jim Schlegel, May 1, 2010, American Banker, http://www.americanbanker.com/btn/23_5/us-to-emv-or-not-1018371-1.html

18. *EMV Implementation for Issuers: 7 Decisions You Must Make Before Issuing Your First Chip Card*, by Paragon Application Systems, http://www.paragonedge.com/Paragonweb/news/industry_insights/chip-card-implementation-for-issuers.pdf

19. *EMV Implementation for Acquirers: 11 Questions to Answer When Formulating Your EMV Device Budget and Timeline*, by Paragon Application Systems, http://www.paragonedge.com/Paragonweb/news/ industry_insights/EMV-Planning-for-Acquirers.pdf

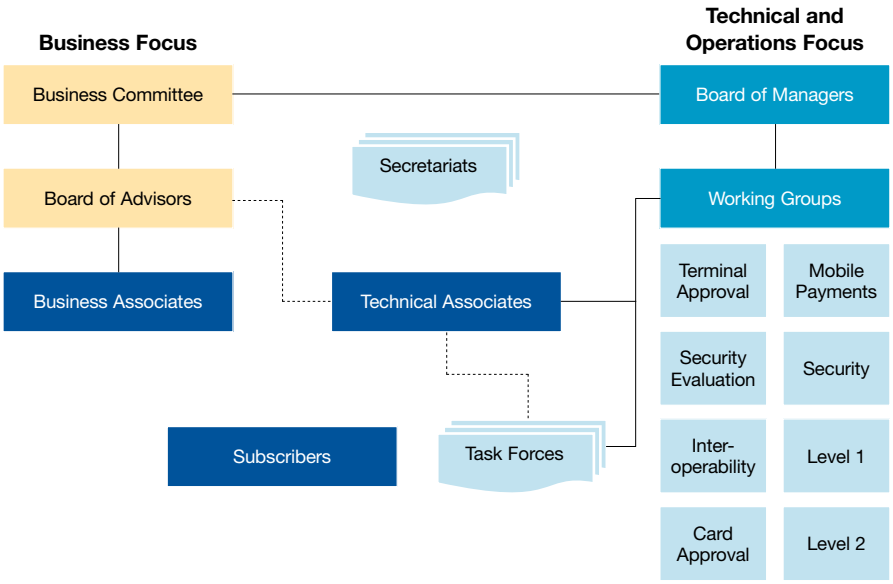
20. *EMV Best Practices*, by EMVCanada, http://www.emvcanada.com/merchant_documents/best_emv_practices.pdf

21. *Organisation Structure*, by EMVCo, http://www.emvco.com/about_emvco.aspx?id=45

Appendix: EMVCo Governance Structure

EMVCo, which looks after the revision, updating, and maintenance of EMV standards, is governed by its board of managers under the guidance and direction of its executive committee. The organization has established several working groups, comprised of representatives from its members, which helps in the execution of EMVCo's responsibilities.

Exhibit 10: EMVCo Governance Structure



Source: Capgemini Analysis, 2012; *Organisation Structure*, by EMVCo

About the Author

Saurabh Kumar Choudhary is a Senior Consultant with the Market Intelligence team in Capgemini Financial Services with over four years of experience specializing in banking and capital markets.

The author would like to thank **William Sullivan**, **David Wilson**, **Ashish Kanchan**, **Nirmal Surekutchi**, **Dolagobinda Mohanty**, **Kripashankar Rajappa**, **Prasanth Perumparambil**, and **Deborah Baxley** for their contributions to this publication.

For more information, visit **www.capgemini.com/cards** or e-mail **cards@capgemini.com.**

About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™.

The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients.

Present in 40 countries, Capgemini reported 2011 global revenues of EUR 9.7 billion and employs around 120,000 people worldwide.

Capgemini's Global Financial Services Business Unit brings deep industry experience, innovative service offerings and next generation global delivery to serve the financial services industry.

With a network of 21,000 professionals serving over 900 clients worldwide, Capgemini collaborates with leading banks, insurers and capital market companies to deliver business and IT solutions and thought leadership which create tangible value.

For more information please visit **www.capgemini.com/financialservices**

Rightshore® is a trademark belonging to Capgemini