Six Myths Preventing EMV Migration in the U.S.

Fact vs. Fiction

White Paper

Contents

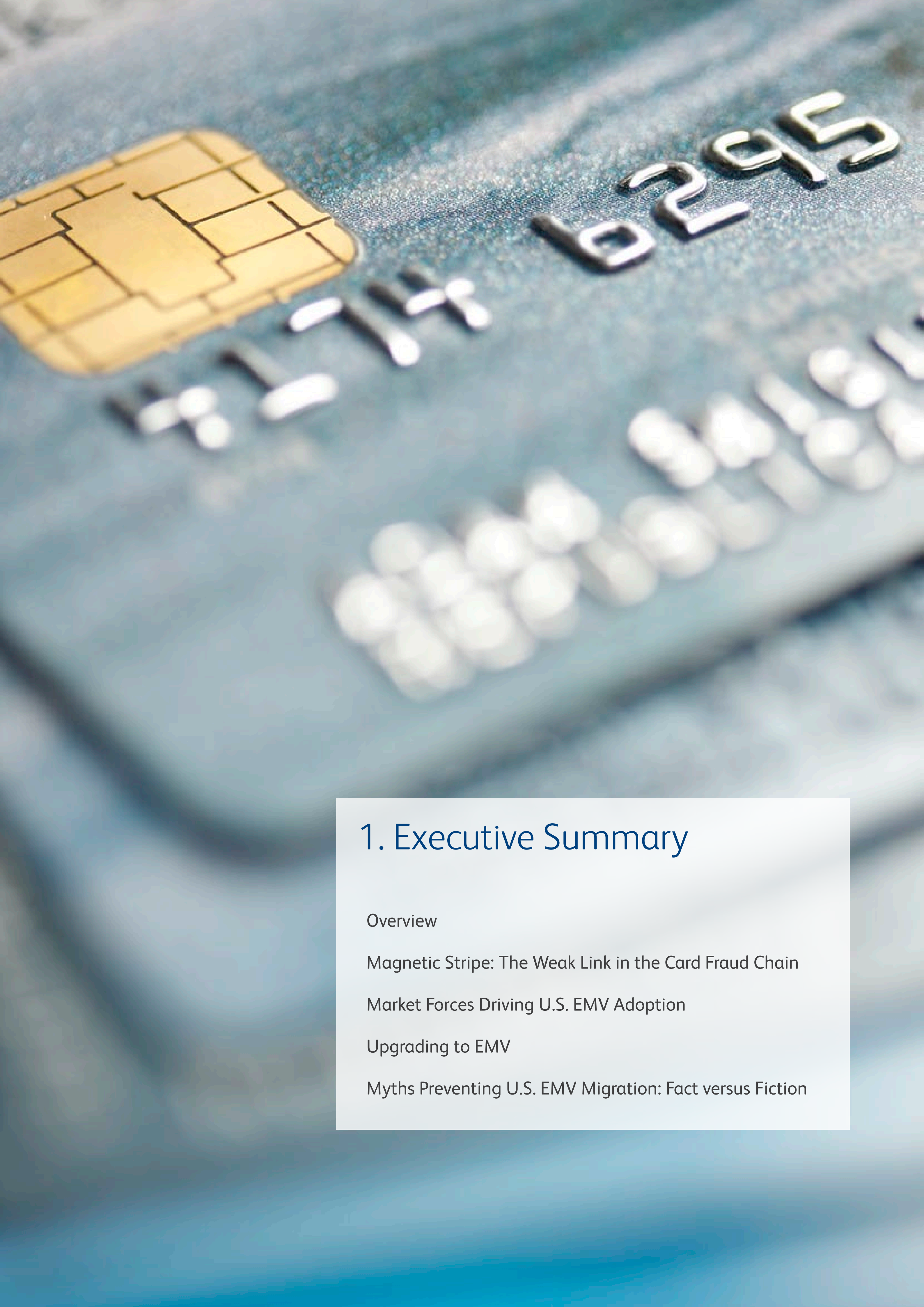
Abstract

EMV is a sophisticated fraud fighting technology that has already replaced magnetic stripe cards in 60 countries worldwide. The United States (U.S.) is the only member of the G20 not to have adopted EMV.

When the question, “why has the U.S. not yet embraced EMV?” is asked, the answers vary widely. Some merchants accuse issuers of greed; issuers and payment networks fear that EMV will erode their profits; acquirers are worried that they will be forced to bear migration costs; alternative technologies claim that EMV is outdated, and others claim that the level of fraud does not justify the investment....

This industry white paper considers the current U.S. card payments industry and stakeholders, and demonstrates how the $6.8 billion of annual U.S. fraud caused by magnetic stripe cards more than justifies investment in EMV. The six most commonly cited ‘reasons’ for the U.S. failing to embrace EMV are exposed as myths created by inaccurate media reporting and a lack of underlying EMV knowledge. Each individual myth is systematically debased by identifying the causes and by separating the effects from the symptoms, supported by industry statistics and financials as needed.

The conclusion of this detailed study is that EMV adoption in the U.S. is not only inevitable, but has in many ways already started. Recommendations are made as to an approach for the national deployment of EMV, while maintaining the current market status quo, and achieving a win-win situation for all participants in the payments chain.



1. Executive Summary

1. Executive Summary

Overview

Whether EMV will ever take off in the United States (U.S.), where magnetic stripe payment cards are still prevalent, has been hotly debated throughout the global payments industry for many years. While mass EMV migration may still seem like a long way off, there are both new developments on the U.S. payments scene and strong market forces at play which appear to confirm that it will happen – it is simply a question of when.

"EMV in the U.S. will happen – it is simply a question of when."

Despite positive signs for EMV in the U.S. there are obstacles to overcome. One of the key barriers to EMV migration at the present time is misinformation surrounding EMV and its impact on the U.S. market. The key aim of this paper is to address six common 'myths' which are delaying EMV migration in the U.S. and to present the facts behind them. Context to these myths has been set through an introduction which examines the following: why magnetic stripe cards in the U.S. need to be replaced with more secure EMV technology, the impact of liability shifts on fraud levels globally and in the U.S., regional and global market drivers for EMV in the U.S. and how the payments landscape must change to upgrade to EMV. Throughout this document 'EMV' refers to all form factors of EMV, including contact, contactless and mobile or Near Field Communication (NFC).

Magnetic Stripe: The Weak Link in the Card Fraud Chain

The ease and profitability of skimming and cloning magnetic stripe technology makes it inherently insecure. As long as the U.S. and other markets continue to rely on magnetic stripe technology, card-present fraud cannot be eliminated, since EMV-compliant countries will need to issue EMV cards with magnetic stripes to ensure compatibility across markets.

Local and global liability shifts, applied by the payment systems (also known as payment schemes) across 60 countries globally (with the exception of the U.S.), have led to EMV becoming firmly established as the primary payment standard worldwide. The success of EMV at preventing card-present fraud in EMV compliant countries has resulted in card fraud becoming concentrated in those areas where an EMV-based infrastructure has not yet been deployed. This makes the U.S. very vulnerable to an increase in card fraud over the next few years.

Market Forces Driving U.S. EMV Adoption

U.S. card fraud losses in 2009 totalled $6.89 billion. This figure is expected to reach $10 billion by 2015. The total cost to migrate the entire U.S. to EMV is estimated at $8.6 billion. The business case is obvious: assuming a two year phase-in, the cost of EMV migration could be recovered within one year and gains from fraud prevention would significantly outweigh the cost of migration in the long term.

"Within one year, the U.S. payments industry could recoup the cost of EMV migration by preventing fraud losses."

Some high profile private sector organisations in the U.S., including Walmart, have already announced their intentions to migrate to EMV on the basis that it offers enhanced security for their customers. This might stimulate other retailers to follow. Additionally, recent U.S. legislation to protect consumer identity through smart technologies and regulation of debit interchange in the U.S. are key drivers at a federal level which have the ability to drive forward the business case for EMV.

With magnetic stripe technology being a weak link in the card-present fraud chain, U.S. citizens increasingly find themselves unable to use their domestically issued magnetic stripe cards abroad, as EMV-compliant merchants protect themselves from fraud losses by refusing to accept payment on magnetic stripe cards.

Customer dissatisfaction may prompt U.S. issuers to offer EMV card products.

As the U.S. becomes a hot bed for global card fraud, the U.S. will come under increasing pressure from worldwide influencers to adopt better standards.

Upgrading to EMV

There is undoubtedly a lot of work to be done and significant financial investment to be made by issuers, acquirers, merchants and payment systems in preparation for EMV migration. Payment cards, Electronic Funds Transfer Point of Sale (EFT POS) terminals and Automated Teller Machines (ATMs) will need to be upgraded, in addition to issuer, acquirer and back office systems.

While substantial, the investment in upgrading to EMV will provide significant returns thanks to the more secure and advanced payments technology on offer. EMV cards can be managed as assets and updated rather than replaced; currently, magnetic cards are treated as expenses, and need to be reissued with every required update. In the case of terminals, most POS and ATM devices only have a three to five year lifespan. After this time, they generally need to be replaced or overhauled due to 'wear and tear' or obsolete security. The cost of upgrading the acceptance infrastructure should therefore be viewed as an assumed cost of business and this cost component taken out of EMV migration cost estimates altogether. The challenge in the U.S., where merchants are mainly responsible for funding upgrades to their POS infrastructure, will be incentivising the market to embrace EMV and the reduction in interchange it brings.

Myths Preventing U.S. EMV Migration: Fact versus Fiction

There are six common 'EMV myths' which are frequently cited as reasons why the U.S. is unlikely to migrate to EMV. Those myths, together with the facts behind them, are as follows:

1. 'EMV will cannibalise issuer interchange revenues'

As a more secure technology than magnetic stripe, EMV will certainly lead to a reduction in debit and signature interchange fees, however the loss in issuer interchange revenue will be substantially exceeded by the cost savings issuers will enjoy through fraud prevention. Independent calculations estimate that U.S. issuer interchange fees will fall by $1.68 billion annually while card fraud, most of which could be prevented by EMV, currently costs the U.S. $6.89 billion per year. The business case is clear.

> *"The loss in interchange revenue from EMV will be substantially exceeded by the cost savings issuers will enjoy through fraud prevention."*

Separately, many issuers wrongly believe that their interchange revenue will be eroded by EMV because it requires the cardholder to use Personal Identification Number (PIN) verification rather than signature verification. The higher interchange fee on signature-based transactions makes signature the preferred verification method among issuers. This fear is unfounded, since the issuer can choose to use EMV cards with either signature or PIN verification.

2. 'EMV does not prevent fraud'

The introduction of EMV has been proven to significantly decrease levels of card-present fraud. The key reason that this type of fraud has not been eliminated completely is because EMV-compliant issuers are still required to equip EMV cards with magnetic stripes so that they can be used in non EMV-compliant markets. EMV's success in preventing card-present fraud has caused fraud to migrate to the less secure card-not-present (CNP) channel. EMV and non-EMV security mechanisms which prevent CNP fraud do exist and where these are used across the globe, they are very effective at eliminating CNP fraud on EMV cards. As CNP fraud grows, more markets and regions are likely to deploy these tools.

3. 'Fraud in the U.S. does not justify migration costs'

From an industry perspective, EMV migration offers a substantial return in a very short time frame.

U.S. card fraud losses in 2009 totalled $6.89 billion and this figure is estimated to reach $10 billion by 2015. With the total cost of migrating the U.S. to EMV estimated at $8.6 billion, the U.S. payment market could potentially save $44.8 billion in fraud losses over the next five years, assuming linear growth in fraud losses from 2009 to 2015. Assuming a two year phase-in, the cost of EMV migration could be recovered within one year.

> *"The U.S. market could save $44.8 billion in fraud losses over the next five years."*

From a stakeholder perspective, issuers have the strongest business case to migrate to EMV, as they currently absorb most of the fraud losses. A liability shift would, however, transfer responsibility for fraud losses onto non-EMV compliant merchants, and this would present merchants with an equally strong business case for EMV.

4. 'EMV is outdated'

Far from being outdated, EMV standards are shaping the future of the global payments industry. While they originally applied only to contact cards and terminals, they are evolving all of the time to ensure they remain relevant to the needs of the payments market. In recent years, new specifications have been released to define EMV contactless card and NFC-based payment products.

5. 'EMV is not secure'

EMV is the most secure payments technology available today. Vulnerabilities recently reported by global media outlets have been rejected and discredited by payment security experts on many grounds. The security of the EMV Specifications is under constant review and updates are frequently made to ensure that EMV stays one step ahead of fraudsters.

6. 'EMV is slow'

Contact EMV transaction speeds may be marginally slower than those performed by magnetic stripe cards. The gap however is nominal; the minor difference in transaction speed has to be considered against the enhanced security benefits EMV offers to all participants. Contactless EMV transactions are faster than those delivered by both contact EMV and magnetic stripe cards.

2. The Problem with Magnetic Stripe Cards

The Ease of 'Skimming' Data

Reliance on Back-Office Fraud Detection Systems

2. The Problem with Magnetic Stripe Cards

Despite the evolution of advanced payment technologies, the payment card market in the U.S. is still dominated by magnetic stripe technology[1] which was introduced in the 1960s. The key failings associated with magnetic stripe cards are well known throughout the industry to be security based.

The Ease of 'Skimming' Data

The lack of sophisticated security on magnetic stripe cards makes them easy to copy and duplicate. In the card industry, the fraudulent practice of reading the data from the magnetic stripe of one card and writing it to another card is called 'skimming'.

Skimming usually happens without the knowledge of the cardholder and is the reason the cardholder should not lose sight of the card when paying. The fraudster reads the card data from the card and stores it for later exploitation. The cardholder typically only learns about the fraud when they receive their next bank statement, or when the card issuer calls to enquire about unusual card spending patterns.

Skimming devices are small and cheap. They can range from simple handheld devices, to expertly crafted attachments to ATMs or EFT POS[2] devices which are undetectable to the untrained eye[3]. These attachments may include digital cameras to capture PINs and use wireless technology to transmit card details and PINs to attackers. Many skimming devices are controlled by international crime syndicates, yet the ease and high profitability of skimming makes it equally attractive to local fraud gangs.

While skimming is alarmingly common, it only allows data capture from one card at a time. More highly advanced fraud attacks are those which compromise a large volume of cards simultaneously by breaching the security of servers and networks at payment processors and merchants to access databases containing magnetic stripe or CNP transaction details.

In recent years, a number of high profile attacks of this nature have taken place. The intention behind the fraud is to use stolen card and transaction records to create cloned magnetic stripe cards for withdrawing cash from accounts, purchasing luxury goods or for performing CNP transactions on the internet.

Card-present transaction data from EMV cards is not a primary target, as it is useless to a fraudster; EMV chips cannot be cloned and the increasing deployment of EMV-based two-factor authentication mechanisms across Europe, such as Card Authentication Program (CAP) and Dynamic Password Authentication (DPA), prevents CNP fraud.

In 2005, a breach at payment card processor CardSystems Solutions jeopardised roughly 40 million credit and debit card accounts. In 2007, hackers stole 45 million card records in an attack on retailing giant TJX and more recently, in 2009, hackers stole 100 million card records from Heartland Payment Systems[4]. The latter two of these events, both of which occurred in the U.S., are the two biggest known cases of identity theft worldwide. Some sources estimate that it costs $202 to deal with each customer record compromised. Estimates also suggest that in 2008 alone, the total cost of data breaches in the U.S. was $1 trillion[5].

> *"Magnetic stripe technology is inherently insecure"*

To address such security breaches, leading payment systems introduced the Payment Card Industry Data Security Standard (PCI DSS) in 2006 and are actively mandating its worldwide compliance in an attempt to prevent further attacks. The goal of the PCI DSS is to secure sensitive magnetic stripe card data by securing the systems that process it – not by increasing the security of the magnetic stripe itself. Interestingly, Heartland Payment Systems claims to be PCI DSS certified at the time of breach[6].

While PCI DSS attempts to enhance the security of data held on magnetic stripe cards, it is merely addressing a symptom of an underlying fundamental problem - magnetic stripe technology is inherently insecure.

Reliance on Back-Office Fraud Detection Systems

Over time, issuers of magnetic stripe cards have evolved back office systems to offer very sophisticated fraud detection processes. These aid in the detection of irregular spending patterns, taking into consideration not only the historic spending pattern of each cardholder, but the context of associated customer and account groups, including seasonal spending patterns.

While fraud detection systems can decrease card fraud, most only detect irregularities once the fraudulent transaction has taken place. If a card has been skimmed, it is likely that there will be a delay before any fraudulent activity takes place on the account, as this reduces the traceability of the skimming incident and subsequently the fraud perpetrator. Once an account is hit however, it is usually emptied as soon as possible and quite often within hours. Most fraud detection systems cannot respond that quickly.

There are some systems that employ real time processing of transactions and these are capable of preventing fraudulent transactions to a certain degree. This is especially challenging, however, now that consumer spending patterns have become extremely complex in today's globalised economy. A U.S. citizen on a European tour, for example, may draw cash at an ATM in Rome and moments later pay for the latest music album downloaded to their roaming mobile from a U.S. music store or purchase an item from a seller in Hong Kong via an internet auction site. Today, there is a very real risk to issuers that this type of fraud detection might actually prevent real transactions and end up inconveniencing and embarrassing the cardholder. The cardholder may, as a result, decide to switch their account to a competing bank.

3. The EMV Liability Shift and its Impact on Fraud Globally

3. The EMV Liability Shift and its Impact on Fraud Globally

EMV, the global standard in chip payment technology, was introduced by the leading payment systems in 1995, to combat the exponential rise in card fraud at an industry level and to help banks reduce fraud losses.

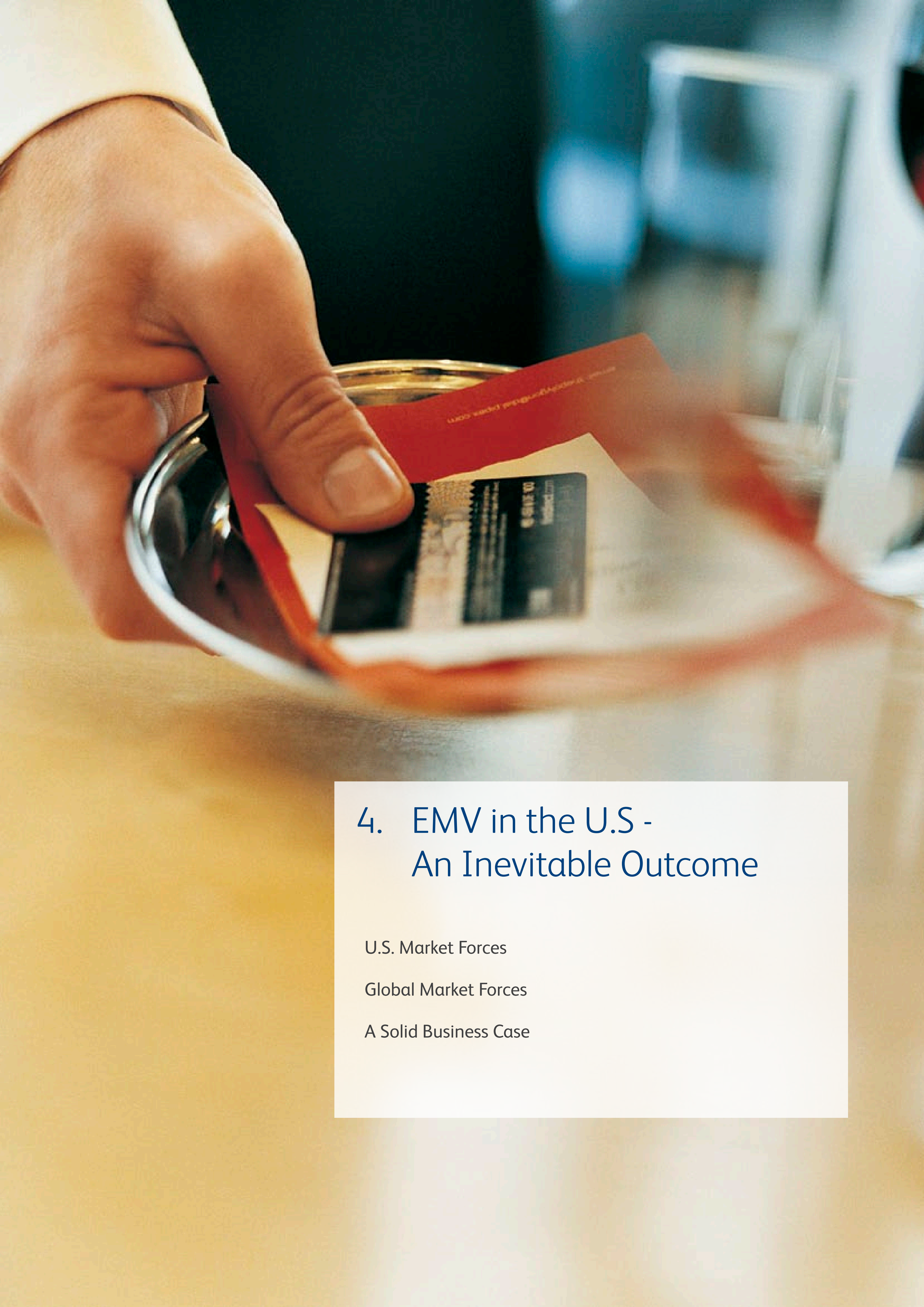
Following release of the EMV Specifications, the payment systems introduced phased local and global shifts in liability for fraud[7], covering more than 60 countries (excluding the U.S.). Issuers and acquirers who do not comply with the EMV standard beyond stated deadlines now bear responsibility for financial losses resulting from fraudulent transactions.

Over a billion EMV cards have been issued to date by financial institutions in 33 countries worldwide. The U.S. is the only member of the G20[8] who has not yet embraced EMV, and is still relying on magnetic stripe[9] card technology which is fifty years old.

While the liability shift is the primary driving force behind EMV migration worldwide, the fact that fraud is growing globally and shifting to regions of the world where EMV is not yet adopted also strengthens the case for EMV migration.

> *"The U.S. is extremely vulnerable to a sharp rise in card fraud."*

Market data on card fraud in the U.K.[10] substantiates that migration to EMV, or 'Chip and PIN[11]' as it is known in the U.K., forces card-present fraud to move to non-EMV compliant regions. With EMV largely established throughout Europe, Asia and Latin America, the U.S.'s closest neighbours – Mexico and Canada – are now following suit. This global situation leaves the U.S. market extremely vulnerable to a sharp rise in card fraud levels in the coming years.



4. EMV in the U.S - An Inevitable Outcome

U.S. Market Forces

Global Market Forces

A Solid Business Case

4. EMV in the U.S - An Inevitable Outcome

Despite the current dominance of magnetic stripe cards throughout the U.S. payments market, global and regional market forces already at play suggest that it is only a matter of time before mass EMV migration takes hold throughout the U.S.

U.S. Market Forces

The private sector in the U.S. is already beginning to show signs of deploying EMV on its own account, with some very significant early adopters leading the market. The retail giant Walmart has announced that it will be upgrading all of its stores to accept EMV cards by the end of 2011. The United Nations Federal Credit Union, one of the largest credit unions in the U.S., has started deploying EMV cards to its 80,000 plus members[12]. Some U.S. card issuers are starting to offer EMV cards to cardholders who frequently travel abroad[13].

At a federal level, the U.S. Government passed the Dodd-Frank Wall Street Reform and Consumer Protection Act in July 2010[14]. This act addresses the protection of consumers from identity theft using smart authentication mechanisms and the Durbin Amendment[15] addresses the regulation of debit-card interchange. If this Amendment results in an enforced decrease in debit interchange fee levels, the consequences are likely to be significant. Currently, the fear that EMV will erode issuer interchange revenue is acting as a key barrier to migration in the U.S. The reality is that any drop in interchange revenue that EMV brings, due to it being a more secure technology than magnetic stripe, will be far exceeded by the substantial savings issuers will make on fraud losses, thanks to EMV's prevention of fraudulent activity.

Global Market Forces

From a global perspective, the EMV liability shift will apply in most countries of the world by 2014, for both domestic and cross-border transactions. In regions where the liability shift applies, the non-compliant party is liable for the fraud and acquirers can deflect the cost of losses from magnetic stripe card fraud back to the issuer, by deploying EMV terminals.

Despite being against payment system rules which state that acquirers must honour all cards displaying the supported payment brands, the proliferation of EMV terminals is leading to an increasing number of merchants refusing to accept payment on magnetic stripe cards[16 17]. This approach is being used by merchants as a way of protecting themselves from fraud liabilities and losses[18]. This practice is already happening in EMV compliant countries and entire regions are even considering a total ban on magnetic stripe card transactions.[19 20 21]

Travellers from EMV compliant countries visiting the U.S. continue to be able to use their cards, which contain both chip and magnetic stripe technology, at U.S. POS terminals and ATMs. U.S. travellers are not quite as lucky. Nearly fifty percent of U.S. cardholders visiting Europe in the last four years have experienced some form of problem when using their payment card[22]. With other countries, including Canada and Mexico, continuing to make significant progress towards EMV migration, the situation only looks set to worsen in coming years[23]. Not being able to make a card payment when it is needed can cause enormous difficulties and embarrassment for cardholders and may cause them to switch banks.

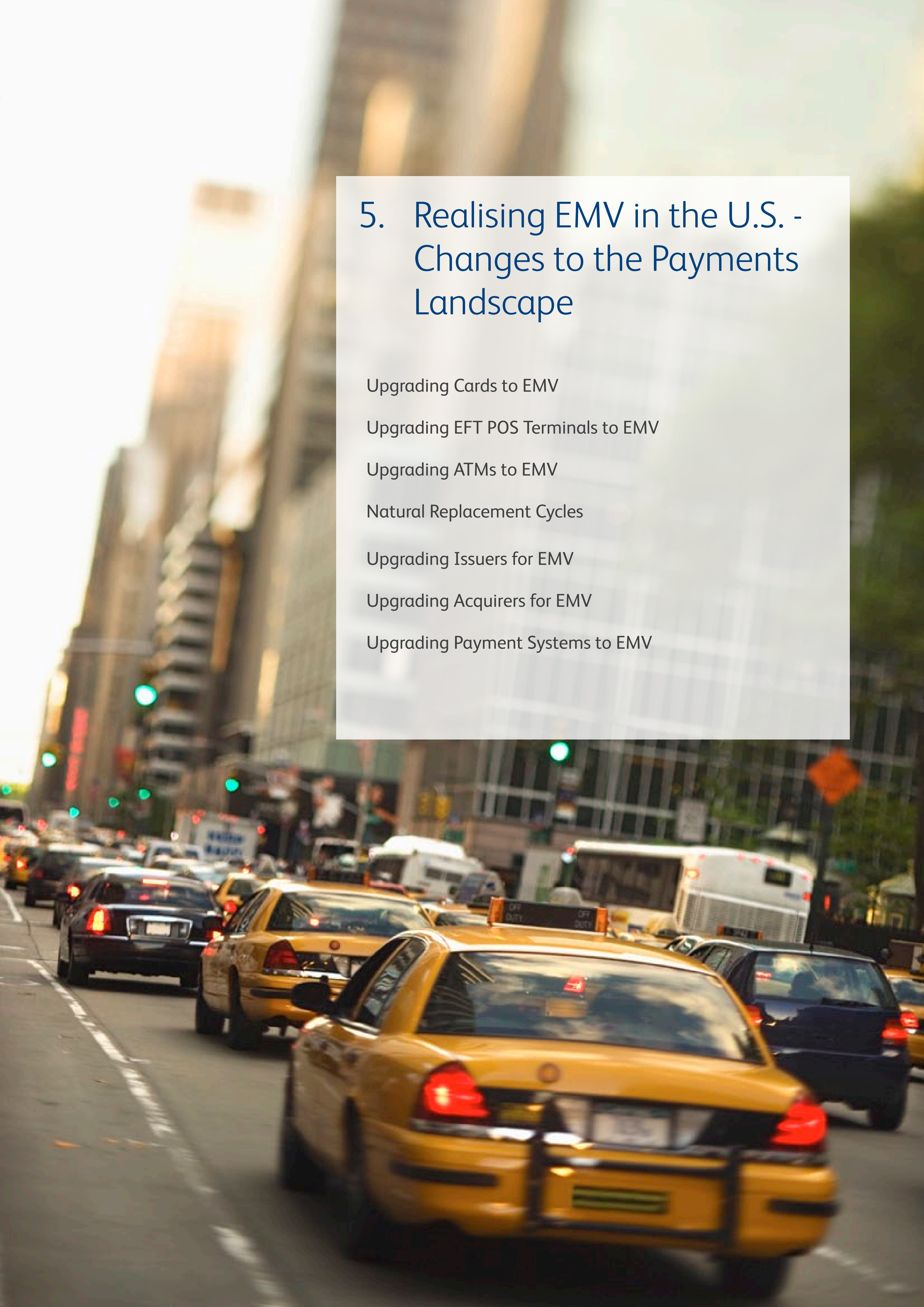
> *"Nearly fifty per cent of U.S. cardholders have experienced problems in the last four years when using their payment card in Europe."*

At a more extreme level and over time, if most card fraud in the world originates from the U.S., the rest of the world may start applying political pressure to force the U.S. to adopt better standards and fraud prevention technologies or at least to recover fraud losses.

A Solid Business Case

In 2009, fraud losses suffered on U.S. credit, debit and prepaid cards totalled $6.89 billion[24]. This figure is expected to reach $10 billion by 2015. As previously noted, given that the total cost to migrate the entire U.S. to EMV is currently estimated at $8.6 billion, the cost of EMV migration could be recovered within one year. This represents a very strong business case, in light of the risks involved in continuing with magnetic stripe technology.

With the rest of the world migrating to EMV, the U.S. will be at the receiving end of hyperbolic growth in card fraud costs. To date, the U.S. market has been slow to embrace EMV, however many issuers are beginning to realise that the U.S. cannot stand as an island in today's global economy. The time has now come to act – since EMV in the U.S. is an inevitability in the long term, early adopters have everything to gain.



5. Realising EMV in the U.S. - Changes to the Payments Landscape

Upgrading Cards to EMV

Upgrading EFT POS Terminals to EMV

Upgrading ATMs to EMV

Natural Replacement Cycles

Upgrading Issuers for EMV

Upgrading Acquirers for EMV

Upgrading Payment Systems to EMV

5. Realising EMV in the U.S. - Changes to the Payments Landscape

For EMV to become a reality in the U.S, a number of significant upgrades need to occur across the payments landscape.

Upgrading Cards to EMV

Issuers face the task of upgrading all of their cards from magnetic stripe to EMV technology. Magnetic stripe cards cost as little as 20 cents each, while EMV cards can cost between $2[25] and $10, depending on chip capabilities. The higher cost of EMV cards is largely justified by the memory and complex security offered by the embedded microcontroller[26] chip in the card. Considering that banks typically issue between 10,000 and 20 million cards on a three-year cycle, it is easy to see that the process of replacing magnetic stripe cards with EMV cards will be a costly process.

The substantial investment required by issuers to upgrade cards to EMV can be offset over time as EMV cards offer issuers the opportunity to treat cards as assets, which can be managed and updated when changes to the card become necessary. Historically, magnetic stripe cards have been classed as expenses, since they are inexpensive, disposable commodities, which are cheaper to replace than update if the card becomes unusable.

> *"EMV cards can be treated as assets; magnetic stripe cards are classed as expenses."*

Upgrading EFT POS Terminals to EMV

EFT POS terminals across the U.S. will need to be upgraded to accept EMV cards. This represents a significant undertaking, since it will largely be U.S. merchants funding the transition to an EMV acceptance infrastructure. Additionally, the complex architecture of the acquiring ecosystem model in the U.S., explained in detail below, means that millions of merchants will need to be encouraged to co-operate on EMV migration efforts.

In most countries globally, it is standard practice for acquiring banks to provide merchants with the hardware and software needed to accept payment cards and to provide the necessary maintenance support. For the purpose of this paper, this model is referred to as full service acquiring. Under this model, acquirers enjoy economies of scale when procuring POS terminals from manufacturers; a consequence of this however, is that the choice of hardware available to merchants is restricted. This standardisation of POS terminals across merchants results in relatively simple and cost-efficient upgrades across the acquirer's acceptance infrastructure. While the costs of hardware, software, infrastructure maintenance and upgrades under this model are initially borne by the acquirer, they are typically passed back to the merchant via service fees.

In the U.S. the full service acquiring model is not common. Merchants typically procure their own POS hardware and software, before integrating with an acquirer or payment service provider. The result is that in the U.S. market, small and mid-sized merchants do not benefit from economies of scale when buying their POS terminals, but they are presented with a vast choice of POS models. This choice has led to a wide range of disparate hardware and interfaces being deployed across the U.S. market. More aggregate work is therefore required to upgrade the POS infrastructure to EMV and merchants are directly responsible for upgrading their terminals and the associated upgrade costs.

While creating solidarity among millions of merchants and encouraging them to participate in mass deployment of EMV terminals will not be easy, incentives such as lower interchange fees and subsidised hardware will certainly help. High profile EMV adopters in the U.S. retail space may also set an example for other retailers to follow; Walmart did not need any more incentive to migrate to EMV than the increased acceptance and security it offers for their customers[27].

The cost of purchasing and/or upgrading EFT POS terminals for EMV will vary significantly depending on the type of terminal involved. The complexity and diversity of the POS terminal market reflects different market requirements for a number of variables, such as features, functionality, quality, support and form. As such, purchase and upgrade costs will vary greatly between models and suppliers.

Upgrading ATMs to EMV

Many of the ATMs in the U.S. are typically owned or operated by an issuing bank or service companies connected to a payment system. An increasing number of ATMs are operated by independent sales organisations (ISOs) and these are much smaller in size, use less advanced technology and offer far fewer payment services than many bank-owned ATMs. In general, there are fewer manufacturers and models of ATMs. As a result, migration to EMV is much less complex than in the POS market.

ATMs are typically highly modular, and when viewed from the service panel, usually consist of discrete components such as a card reader, cash dispenser, document accepter, control unit, display unit, keyboard and printer, all wired together in a metal frame. This modular nature makes ATMs relatively easy to upgrade by a field engineer; upgrading an ATM to accept EMV cards typically involves replacing the card reader hardware and upgrading the control unit software. Upgrades are typically carried out in conjunction with regularly scheduled maintenance visits and can also be combined with ATM upgrades to Payment Card Industry PIN Transaction Security (PCI PTS) standards.

The cost for upgrading ATMs to accept EMV cards will be mostly borne by card issuers and service companies for their own ATMs. These costs are likely to be recovered from cardholders through service fees.

Natural Replacement Cycles

While the cost of replacing POS and ATM terminals to accommodate EMV is often cited as excessive and prohibitive to EMV migration, this cost has to be considered in context of the average three to five year lifespan of an ATM or POS terminal. Daily 'wear and tear' inflicted by the general public can result in buttons and printing heads wearing out, displays cracking and terminals becoming vandalised, among other things. Security also becomes outdated, and as such, the value of terminals is amortised over their useful life span and replacement or overhaul is eventually inevitable. As such, there are grounds to suggest that this cost component should be removed from EMV migration estimates altogether.

Today, it is increasingly difficult to buy a non-EMV and/or non-PCI compliant terminal. As the worldwide population of terminals is continually renewing itself, due to wear and tear and advances in technology, EMV terminal migration should be considered as an assumed cost of business, rather than a separate cost that needs to be budgeted for. Many replacement terminals deployed today typically include contact and contactless chip readers and secure

PIN pads, even though they may not be activated or used until some point in the future.

“The cost of upgrading terminals to EMV should be removed from migration estimates, due to their short life span.”

Upgrading Issuers for EMV

In addition to issuing payment cards to members, issuers authorise transactions originating from those cards. Transactions are routed from payment terminals through payment systems and third-party processors to the card issuer, who checks for available funds or credit, validates the card and account status, performs fraud checks and ultimately approves or declines the transaction through a message back to the acquirer.

EMV card issuers must upgrade their card issuing systems to provide the risk parameters, security elements and other chip data needed to personalise the EMV chip. Due to the increasing complexity and cost of chips, full card and application management will help issuers reduce card issuance costs and enable advanced functionality such as post-issuance application loading and updating of card parameters. This is especially true when multi-application cards are deployed.

EMV transaction authorisation includes card and issuer authentication using strong cryptography. Support for EMV transaction authorisation must be added to the issuer’s authorisation or host system. Third party processors manage much of the transaction processing activities for issuers’ debit and credit cards in the U.S. They are required to make the same changes to their card issuing and processing systems that issuers make in order to support EMV.

Upgrading Acquirers for EMV

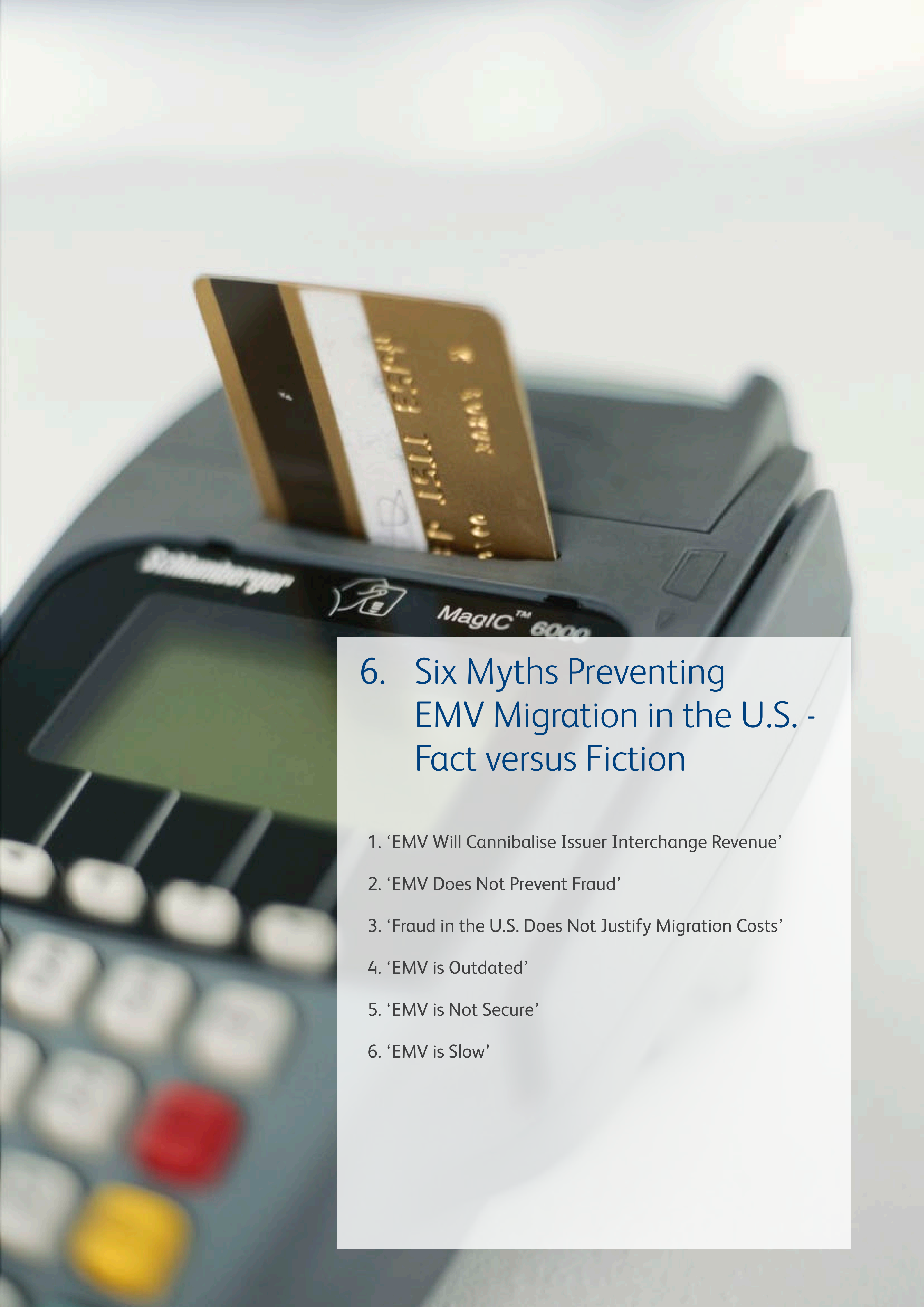
Acquirers are companies that accept and process electronic transactions from merchants. They can be retail banks, divisions of banking conglomerates, or processors. Acquirers connect directly to the payment systems. Their role is to route transactions through a switch to the proper network, which will in turn route the transaction to the issuer for authorisation.

Besides carrying EMV data in the individual transaction record, acquirers need not change anything on their payment processing system in order to route EMV transactions. As mentioned earlier in this section, it is common for acquirers outside of the U.S. to upgrade the POS terminal infrastructure used by their merchants.

Upgrading Payment Systems to EMV

Issuers and acquirers are connected via payment systems, processors, and clearing houses in order to accept cards, process and settle payments. Migrating to EMV implies additional chip data being carried over these networks with each EMV transaction. While international payment systems such as Visa and MasterCard already have networks capable of carrying this data, domestic payment systems in the U.S. (such as the STAR, NYCE, Pulse and Interlink networks), switches and networks will have to upgrade their network infrastructure in order to carry EMV transaction data.

“A number of ‘EMV myths’ are cited as reasons why the U.S. is unlikely to migrate to EMV.”



6. Six Myths Preventing EMV Migration in the U.S. - Fact versus Fiction

1. ‘EMV Will Cannibalise Issuer Interchange Revenue’

2. ‘EMV Does Not Prevent Fraud’

3. ‘Fraud in the U.S. Does Not Justify Migration Costs’

4. ‘EMV is Outdated’

5. ‘EMV is Not Secure’

6. ‘EMV is Slow’

6. Six Myths Preventing EMV Migration in the U.S. - Fact versus Fiction

With very little experience of EMV in the U.S., there is a lot of misinformation around the subject which is exacerbated by inaccurate media reporting of a very complex technology. Attempts by the media to simplify EMV for mass consumption have led to terminology errors and false assumptions. These in turn have given rise to a number of EMV 'myths' which are commonly cited as reasons why the U.S. is unlikely to migrate to EMV.

In this part of the paper, the most common EMV myths are exposed and the objective facts behind them are presented. The paper aims to clarify popular misunderstandings surrounding EMV and reinforce the fact that the U.S. market is now, more than ever, ready to commence the process of EMV migration.

Myth One: 'EMV will Cannibalise Issuers' Interchange Revenue'

The U.K. has an established and high profile 'Chip and PIN' programme, where EMV cards are used alongside PINs by cardholders nationwide. This has led to a false assumption among many parties in the U.S. that EMV and PIN are inseparable. A large scale shift in the market from signature-based transactions to PIN-based transactions is an uncomfortable thought to many U.S. issuers. Indeed, the struggle between card issuers and merchants over interchange is as old as the payment card industry. Issuers prefer signature-based transactions which earn a higher interchange fee per transaction, while merchants prefer PIN-based transactions, which are associated with lower interchange fees. The general misconception among issuers is that EMV will significantly erode their debit interchange revenue because it is based on PIN-based debit. This belief is so widely held that merchants are citing it as a reason why U.S. issuers are choosing not to implement EMV[28].

The Facts

At a high level, it is necessary to correct the common assumption that EMV cards can only be used with PIN verification. EMV cards support both PIN and/or signature in any combination, for example PIN for cash withdrawal and signature for purchase or even no cardholder verification for low value transactions. Quite simply, whether a card uses PIN and/or signature is the issuer's decision, and one which can be altered post card issuance. EMV terminals automatically select the first authentication method supported by the card and the terminal which matches the transaction conditions. This functionality is expressed by a card application parameter known as the Cardholder Verification Method (CVM) List, as defined in EMV Book 3[29].

It should be noted that there are payment system rules that apply to certain payment products, which may require either PIN or signature or both for a certain payment instrument. These rules, however, typically apply regardless of whether it is a magnetic stripe or EMV card.

> *"EMV cards support both PIN and/or signature in any combination."*

Slightly more complex is the notion that despite the fact that EMV does not rely solely on PIN verification, and will therefore not erode issuer interchange revenues on that basis, it is likely to cause a decline in issuer interchange revenue simply by virtue of being a more secure payment technology than magnetic stripe. As a general rule, the more secure a transaction, the lower the interchange fee. To justify the revenue decline, however, U.S. issuers need only look at the potential annual savings which can be recouped against fraud losses when secure EMV technology replaces current magnetic stripe cards. As explained in detail below, savings on fraud losses are estimated to significantly outweigh any decrease in debit interchange revenue following the introduction of EMV.

The following sections provide additional information on the security of signature and PIN verification, and the impact of PIN, signature and EMV on interchange, in order that the overview above can be understood more clearly.

"Savings on fraud losses will significantly outweigh the fall in debit interchange due to EMV."

PIN versus Signature

PINs and signatures are used together with cards to prove the cardholder's identity. The three 'pillars of identity' are commonly known as something you are (signature), something you know (PIN) and something you have (card). The more pillars that are present during a card transaction, the more confident the verifying party can be that the person holding the card is the authorised user. A counterfeit-proof card, such as an EMV card, used together with signature and PIN verification would therefore provide the strongest method of identification available. While this combination is used in some countries today, the need to consider consumer convenience and deliver optimal transaction speed usually leads to either signature or PIN verification being used in conjunction with a card.

How Secure is Signature Verification?

Signature is one of the most basic biometric identification methods. It is produced by an individual through a unique combination of movement, speed, pressure, hand used, wrist movement, grip and angle exercised onto a writing instrument that leaves an ink trail on paper. As with all biometric identification, the uniqueness of signature is easy to understand, however it can be quite difficult to verify accurately.

The theory is very simple. When cardholders receive their card, they sign the signature panel on the back. Each time they perform a transaction, they sign the receipt, which the cashier compares to the signature on the card. If the signatures match, the cardholder 'proves' themselves to be who they claim to be.

The problem with this approach is that many cashiers do not check the signature on the card against that on the receipt. Of those that do, very few are trained in handwriting analysis. Additionally, the signature on the card is the only historic data sample for cashiers to compare against, wrongly implying that all cardholders produce a consistent signature every time[30]. While payment systems do have very clear rules on how to check a card signature[31], these guidelines are not followed precisely by merchants and cashiers in practice[32]. There are electronic solutions for accurately verifying signatures, however they require costly equipment for signature capture and are not typically supported by payment systems. They are therefore not widely used.

The conclusion can therefore only be that signature verification by cashiers is not a secure method of proving someone's identification[33]. Its only true value may be that a valid signature is binding in a court of law.

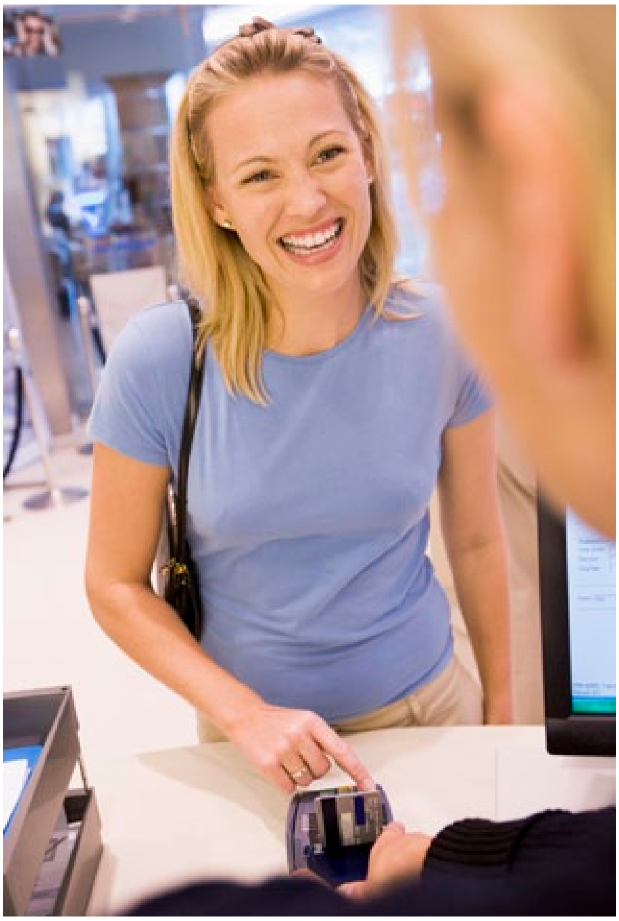
The security of signature-based cards can be further compromised by transactions that do not require signatures at automated POS terminals, or due to the merchant's transaction processing rules.

How Secure is PIN Verification?

A PIN is a short numeric password known only to the cardholder, which can be verified quite simply by a transaction authorisation system. A typical PIN contains four digits and is either chosen by the cardholder or randomly generated and assigned to the cardholder.

In cryptographic terms, a four digit numeric password is extremely weak; with only 9999 different combinations, an average computer would be able to crack a four digit PIN by brute force in milliseconds. Card issuers prevent brute force attacks by maintaining a 'PIN try counter' for each PIN, commonly set to three.

For each attempt to verify the PIN, the PIN try counter is decremented by one. When the correct PIN is entered, the PIN try counter is reset to the PIN try limit. When three incorrect PINs are entered and the PIN try counter reaches zero, the PIN is blocked and further verification is not allowed. This means that an attacker has a three in 9999 chance of guessing the right PIN.



Despite the security offered by the PIN try counter, PINs can still be stolen. Stolen PINs are typically used by fraudsters in conjunction with skimming, to allow them to access cardholder funds. Simple methods of stealing a PIN include 'social engineering' (the manipulation of a situation to get an unsuspecting victim to do something they should not do), shoulder surfing and distraction techniques at ATMS by fraudsters pretending to be bank staff or helpful passers-by. More advanced approaches involve illegal tampering with ATMs and the installation of unauthorised keypad overlays and spy cameras.

Today, most PIN pads used on financial payment terminals such as ATM and POS are certified to PCI PTS[34] (formerly known as Payment Card Industry PIN Entry Device or PCI PED). PCI PTS devices have a number of advanced security features; they can detect when they are being tampered with and destroy sensitive data inside the device before attackers can get to it; they are tamper-evident so that tampering attempts are obvious to users; and they offer a shielded keypad surface so that keystrokes cannot be observed by anyone but the user.

Overall, PINs offer a more secure verification method than signatures. Both signatures and PINs however, offer far more effective security when used with an EMV card than when used with a magnetic stripe card.

How Secure are Magnetic Stripe Cards versus EMV Cards?

As magnetic stripe cards are easily copied, a verifying party wishing to confirm the identity of the cardholder during a transaction cannot be sure whether the card is the original or a fraudulent copy. The signature on a cloned card will be that of the fraudster, so signature verification is inconclusive. Equally, PINs can be stolen and used alongside cloned cards, so identity proved in this way is not necessarily authentic. The underlying issue with magnetic stripe card technology is the inability to prove that the card itself is genuine. This weakens the value of both signature and PIN verification methods and ultimately, means that only a low grade of identity can be established whichever method is used. For this reason, some merchants ask for additional proof of identity, such as a driver's license or passport, especially when processing a high value transaction. As the card may be in the name of the fraudster however, the value of this authentication method is also questionable.

EMV cards have built in security mechanisms that use strong cryptography to authenticate the card, card issuer and the data stored on it. The verification of the card's authenticity during each transaction, combined with signature or PIN to verify the cardholder, allows a high degree of identity to be established and ultimately results in EMV cards being much more secure than their magnetic stripe counterparts.

Interchange Fees and the Impact of Transaction Security

In a financial transaction a processing fee, commonly known as 'interchange', is typically paid by the merchant and shared between the issuer, acquirer and payment system. The issuer is the primary beneficiary, as the merchant pays mainly for the privilege of accepting payment via the issuer's debit or credit cards, to save on cash handling fees. The acquirer and payment system take a smaller fee for card acceptance services and processing respectively.

While interchange fees have a complex pricing structure based on many variables, signature-based transactions generally attract a higher fee than PIN-based transactions, regardless of whether magnetic stripe technology or EMV is used. The reason for this, as previously explained, is because signature represents a less secure way of verifying the authenticity of the cardholder; the financial risk is greater for the issuer when asked to release funds from an account where a low-grade of cardholder identity has been established by the merchant.

The Impact of EMV on Issuers' Interchange Revenue

Interchange fees represent a substantial revenue stream for issuers. According to The Nilson Report[35], $19.7 billion of interchange was generated on MasterCard and Visa cards in the U.S. throughout 2009, averaging 1.63% of ticket values.

> *"The fall in interchange revenue caused by EMV will be recouped very quickly by savings from fraud prevention."*

It was established, earlier in this section, that issuers derive a higher interchange fee from signature-based transactions than PIN debit-based transactions. As a result, issuers favour signature-based transactions, while merchants would prefer more PIN-based transactions. A key fear among U.S. issuers has always been that the introduction of EMV will impact negatively on their signature-based transaction interchange revenues, because it has been an assumption that EMV necessitates a switch to PIN-based transactions. While this paper has outlined that this assumption is not correct – that EMV actually supports both signature and PIN verification – the reality is that EMV will result in a reduction in U.S. issuer interchange revenues.

Rather than being caused by EMV's reliance on PIN verification, however, decreased fees will result from EMV being a more secure technology than magnetic stripe. This will be factored into the equation upon which interchange fees are based. Quite simply lower interchange fees will be charged because EMV offers more transaction security. The important thing for issuers to be aware of, however, is that the fall in interchange revenue brought about by the increased security of EMV will be recouped in a very short period of time by the cost savings EMV delivers through fraud prevention.

Independent calculations conducted by Bell ID (Appendix 1) have put a figure on the estimated projected loss of U.S. EMV debit interchange, based on the assumption that the difference between magnetic stripe and EMV interchange in the U.S. will be the same as in Europe. According to these calculations, U.S. issuers will lose approximately $1.68 billion per year in revenue when the U.S. migrates to EMV. With current total card fraud costing U.S. issuers $6.89 billion per year, however, and with the majority of payments in the U.S. consisting of debit transactions, the act of sacrificing $1.68 billion of revenue per year to prevent an even more costly fraud bill should make good business and financial sense to U.S. issuers as a collective.

While EMV migration will decrease interchange values, it will not affect the interchange struggle between card issuers, networks, merchants and acquirers; a universal linear reduction in interchange should not change market dynamics, which include the competition among networks for issuers, the desire among customers to earn loyalty points and merchants' preference for lower interchange fees[36].

The Impact of Legislation on Interchange

While EMV should not affect the status quo in the interchange struggle, U.S. legislation and the regulation of debit interchange might. While the exact impact of this legislation is not clear at this moment in time, the U.S. Federal Government is expected to take a cost-based regulation approach, setting maximum limits for debit interchange per transaction that are reasonable and proportional to the cost of processing a transaction. Such legislation could close the gap between signature and PIN based debit interchange.

Myth Two: 'EMV does not Prevent Fraud'

There have been claims that EMV does not reduce fraud[37]. These claims are founded on the belief that EMV simply causes fraud to migrate away from card-present transactions to the CNP channel.

The Facts

EMV offers effective fraud prevention in card-present scenarios. As a result, fraud has naturally migrated to the less secure CNP channel, leading to a significant rise in reported CNP fraudulent activity. Some might argue that this activity should be classified under 'internet fraud' since the card is not involved.

The payments industry has introduced effective EMV and non-EMV mechanisms to combat CNP fraud, such as two factor authentication techniques and Short Message Service (SMS) authorisation codes. These mechanisms are already widely deployed in Europe and are likely to become increasingly popular internationally as CNP fraud grows. The decision whether or not to implement these tools is the responsibility of individual issuers and merchants.

No technology is one hundred per cent secure or fraud-proof. Even hard currency gets counterfeited. Equally, no single technology can seamlessly integrate with every payment method (cash, SMS, online etc) to provide effective universal security. For these reasons, it is essential to secure as many fraud channels as possible, on an individual basis yet within the structure of a multi channel security domain. In the world of payment cards, this means starting with card-present fraud, followed by CNP fraud, while continuously improving back office application screening and risk detection.

EMV's Impact on Card-Present Fraud

Where EMV has been deployed with PIN cardholder verification, there has been a substantial decline in card-present fraudulent activities, including transactions on lost and stolen cards, skimming and counterfeiting.

Card-present fraud has not been eliminated completely however. While fraudsters are prevented from making card-present transactions in EMV compliant regions, there is currently nothing to stop them from skimming the magnetic stripes on EMV cards, in order to produce cloned cards for use in non-EMV regions. Magnetic stripes continue to be a feature of EMV cards issued globally, to ensure backwards compatibility and acceptance in non-EMV countries, where EMV cards may potentially be used with magnetic stripe only terminals.

This type of card-present fraud will continue for as long as the U.S. and other markets retain magnetic stripe only terminals. This situation puts both U.S. issuers and acquirers at risk, for as the rest of the world migrates to EMV, fraudulent activity will focus increasingly on non-EMV regions. This puts the U.S. in danger of becoming a global centre for card fraud[38].

EMV's Impact on CNP Fraud

As witnessed in many countries including the U.K., EMV has caused card-present fraud to migrate to non-EMV countries and to CNP channels such as internet banking, eCommerce, voice authorisation and mail-order.

To address the problem of growing CNP fraud, most major banks in the U.K. and Europe already provide, or are in the process of providing, cardholders with personal card readers for use with their cards for internet banking and eCommerce transactions. When combined with two factor authentication mechanisms such as 3-D Secure[39], CAP[40] or DPA[41], Chip and PIN offers extremely effective CNP fraud protection.

Other effective and readily available authentication mechanisms introduced to fight CNP fraud include Universal Serial Bus (USB) security tokens and SMS authorisation codes. As these mechanisms are disconnected from the card, however, they represent a separate device or identify factor to manage. For this reason, they do not increase the consumer's confidence in the card and fall beyond the scope of this paper.

In summary, security mechanisms to address CNP fraud do exist in the current market and are already widely implemented across Europe. As CNP fraud losses grow exponentially across the world, an increase in the global uptake of these tools is very likely.

Myth Three: 'Fraud in the U.S. does not Justify EMV Migration Costs'

Many parties believe that there is no solid business case for EMV migration in the U.S. The misconception is that the cost of migrating the industry to EMV is larger than the cost savings EMV will bring about through fraud prevention.

The Facts

This myth needs to be addressed on two levels, since the cost justification of EMV migration needs to be examined from both an industry and individual stakeholder perspective.

The Cost-Benefit Analysis of EMV Migration: An Industry Viewpoint

There is no doubt that the process of migrating to EMV is expensive. Payment terminals such as ATMs and POS will typically need to be replaced or upgraded, new payment cards will need to be issued and from a back office perspective, payment networks and processing system upgrades will be required. While estimates place the total cost of migrating the U.S. to EMV at $8.6 billion, this has to be put in context; the reality is that the savings on fraud losses that can be made by EMV will significantly exceed this total cost of migration. Fraud losses on credit, debit, and prepaid cards in the U.S. totalled $6.89 billion in 2009. This figure is estimated to reach $10 billion by 2015. Assuming a linear growth in fraud losses from 2009 to 2015, the U.S. payment market could potentially save $44.8 billion in fraud losses over the next five years alone and achieve a return on the investment in EMV migration within one year.

"The U.S. could save $44.8 billion in fraud losses in the next five years."

From an industry perspective it is clear that the cost of EMV migration offers a substantial return within a very short time frame and can be fully justified on those grounds.

The Cost-Benefit Analysis of EMV Migration: A Stakeholder Perspective

While the industry stands to benefit as a whole from the introduction of EMV in the U.S., issuers have the strongest business case to drive it forward since they currently absorb the greatest proportion of card fraud losses. Acquirers and merchants do share the cost of fraud, but to a much lesser extent.

Significantly, merchants are currently not held accountable for fraud if they follow the payment system rules when accepting payment – except for in the case of CNP transactions which represent approximately three per cent of transaction volumes[42]. Many merchants are therefore opposed to EMV migration as the need to upgrade terminals represents a significant cost, yet EMV will not necessarily bring them any cost savings apart from lower interchange.

In the future, however, as U.S. issuers stimulate EMV migration by issuing EMV cards and lobbying for the introduction of the liability shift which applies in other countries globally, the situation for merchants will change. The liability shift will transfer fraud costs to acquirers and in turn to non-EMV compliant merchants. This will present merchants with a stronger business case for EMV migration, as they will be required to replace or upgrade their terminals in order to avoid responsibility for fraud losses.

Myth Four: 'EMV is Outdated'

The misconception that EMV is an outdated technology is based on the incorrect assumption that EMV only applies to contact chip cards. With issuers increasingly deploying contactless chip payment cards and tokens globally, in response to consumer demand for greater convenience and faster transaction speed, some parties are unaware that EMV technology has not only evolved with the market, but in many respects is shaping future payments.

"EMV is shaping future payments."

The Facts

The first EMV Specifications were drafted in 1995. These provided a global interoperability standard for contact chip payment cards and terminals. Today, the EMV Specifications are developed and maintained by an industry body called EMVCo, which is owned and operated by American Express, JCB, MasterCard and Visa. As with any 'living' technology standard, the EMV Specifications are constantly evolving to address the requirements of the market and reflect technology advancements. This evolution equally prevents the technology from becoming vulnerable and insecure.

EMV: An Evolving Technology

EMVCo continuously reviews, amends and updates the EMV Specifications and new releases of the technology are published in cycles of approximately three years. In recent years, new specifications have been released to define EMV contactless card and NFC-based payment products. The adoption of these specifications by the payment systems has resulted in them underpinning the development of payment products globally.

While EMV technology continues to advance, new specification releases are always backwards compatible to avoid interoperability issues. Over time payment systems phase new versions into use while older versions are phased out.

"EMV Specifications define contactless and Near Field Communication-based payment products."

In early 2010, EMVCo launched an Associates Programme[43] to encourage payment industry stakeholders to play a more active role in guiding the organisation's strategic and technical direction. The programme creates opportunities for interested organisations, including card issuers, acquirers, merchants, processors, card and terminal vendors, networks and their representative associations, to provide input into the enhancement of existing and creation of future EMV Specifications. By encouraging industry engagement in the development of EMV, at both a strategic and technical level, EMVCo is ensuring that EMV technology remains relevant and responsive to the current and future needs of the market.

Myth Five: 'EMV is not Secure'

Recent media exposure[44] generated by a team of U.K. researchers who claimed to have identified vulnerabilities associated with EMV has perpetuated a popular misconception that EMV is not secure. The research proved that it is possible to bypass the PIN verification process of some EMV cards, by routing the card to terminal communication through a fake card; the fake card in the attacker's hand has to be attached - via wires running up his sleeve – to a laptop in his backpack. The laptop is then connected to a real card.

The vulnerability claim was rejected and discredited by many payment industry experts and security specialists on a number of grounds[45]. Firstly, the EMV cards that were 'cracked' by the researchers did not comply with current card security recommendations; the card issuers chose not to implement available security measures due to cost and risk considerations. Secondly, it would be very difficult to use this tactic to defraud in the real world, due to the complex preparation and equipment 'set-up' required: stolen genuine cards; social engineering; wires up sleeves; and laptops in backpacks. Finally, the impracticality and difficulty in scaling the technique, coupled with the high risk of discovery and very limited financial gains on offer, renders it an unattractive proposition to fraudsters.

The Facts

Since the introduction of EMV fifteen years ago, its security features have been under constant review and numerous updates have been made. While nothing can be made one hundred per cent secure, EMV offers the most advanced security available for payments today. Continual security upgrades ensure that EMV remains one step ahead of fraudsters; most cases of reported EMV vulnerabilities are a result of issuers not keeping up to date with the latest best practices in EMV security.

> *"EMV offers the most advanced security available for payments today."*

Advanced Authentication Protocols and Encryption Algorithms

Early EMV card authentication was performed using Static Data Authentication (SDA) and Dynamic Data Authentication (DDA). SDA prevents card data from being counterfeited, but not the card itself. DDA prevents both the card and card data from being counterfeited, but is vulnerable to man-in-the-middle attacks, which are difficult and impractical to execute. Once vulnerabilities were discovered with these protocols, Combined Cryptogram Generation and Dynamic Data Authentication (CDA) was introduced. CDA prevents both the card and card data from being counterfeited and prevents man-in-the-middle attacks. Today the use of SDA in EMV is being phased out while the use of DDA/CDA for EMV card authentication is being mandated in Europe.

EMV cardholder authentication methods have also been extended in recent years. In addition to signature and PIN, EMV now supports biometrics for cardholder verification. EMV deployments supporting biometrics however, remain very rare in today's market.

EMV has been designed to have interchangeable encryption algorithms and variable key lengths and the technology uses public key cryptography and certificates similar to those used to secure websites. The encryption algorithms used by EMV have evolved through the years. EMV originally supported Rivest, Shamir and Adleman (RSA) public key cryptography and the Triple Data Encryption Standard (3DES or TDES), but today also supports more secure algorithms including Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC).

Until recently, the 3DES algorithm was regarded as perfectly acceptable. Due to advances in computing power and the potential risk from brute force attacks, however, it is becoming increasingly possible to use a massive distributed network to crack one session key of a card transaction in just a few days. EMV counters this risk by applying many layers of key derivation when using these algorithms. This means that only individual transactions performed by an individual card – rather than all cards sharing the same master key– can be compromised days after the transaction has occurred. Attackers using this method would therefore be required to invest a significant amount of money to employ complex hardware in order to be rewarded with, at most, one fraudulent transaction.

Facilities producing EMV cards and terminals are audited at least once annually for physical security and to check compliance with physical and logical security standards such as PCI DSS.

Myth Six: ’EMV is Slow’

When EMV was introduced, transaction processing times were in some cases slower than those associated with magnetic stripe technology. The widely held belief that EMV transactions are still noticeably slower is unfounded, since modern EMV terminals use multi-threading and parallel processing to optimise transaction speeds and are subsequently much faster.

“EMV terminals use multi-threading and parallel processing to optimise transaction speeds.”

The Facts

Transaction speed from a consumer point of view starts from the moment they insert their card into a terminal or hand it over to a cashier. It ends when they receive their receipt and card back. The largest amount of transaction time is consumed by the cardholder entering their PIN and/or signing a receipt, followed by the receipt printing process and online authorisation, which includes the establishment of connectivity to the payment gateway. The time it takes for the terminal to read the chip on the card is much shorter than these other processes and much of this interfacing is done while the cardholder is entering their PIN.

While modern contact EMV transaction speeds have improved significantly over the years, they may in general still be marginally slower than those offered by magnetic stripe technology. The gap however is nominal; the minor difference in transaction speed has to be considered against the enhanced security benefits EMV offers to all participants. Contactless EMV transactions are faster than those delivered by both contact EMV and magnetic stripe cards.

Appendix 1 - Loss of U.S. Debit Interchange: Bell ID Calculation Table

The table below shows Bell ID's own projection of U.S. EMV debit interchange, based on calculations which assume that the difference between magnetic stripe and EMV interchange in the U.S. will be the same as in Europe. The calculation takes the difference between European interchange for magnetic stripe and EMV and applies it to existing U.S. magnetic stripe interchange in order to calculate the expected U.S. EMV interchange. The U.S. magnetic stripe interchange and expected U.S. EMV interchange volume is calculated based on U.S. total transaction value and the difference is calculated to result in the total reduction in interchange.

This calculation shows that if the U.S. migrates to EMV, U.S. issuers will lose an estimated $1.68 billion of combined PIN debit and signature debit interchange revenue per year. Considered in context of the $6.89 billion card fraud losses suffered by the U.S. annually, this loss in interchange revenue will be far exceeded by the fraud prevention gains issuers will enjoy thanks to EMV deployment.

	PIN Debit	**Signature Debit**
Europe : Magnetic Stripe Interchange MasterCard Europe Consumer Card Interchange Fees[46] signature debit is not used in Europe. The interchange difference for signature debit is assumed to be the same as for PIN debit.	0.16% + € 0.05	n/a
Europe : EMV Interchange MasterCard Europe Consumer Card Interchange Fees[47] signature debit is not used in Europe. The interchange difference for signature debit is assumed to be the same as for PIN debit.	0.14% + € 0.05	n/a
Europe : Interchange Difference EMV interchange being lower than magnetic stripe interchange and expressed as a percentage difference.	-12.5%	-12.5%
U.S. : Magnetic Stripe Interchange Rate U.S. Retail Tier I signature debit pricing for signature debit in 2009 ranged from 0.62% + $0.13 to 0.70% + $0.15, while PIN debit ranged from 0.45% + $0.08 to 0.55% + $0.04[48] . Interchange pricing and caps do differ from network to network; for simplicity an average interchange is used by assuming an equal transaction spread.	0.50% + $0.06	0.66% + $0.14
U.S. : EMV Interchange Rate Expectation based on European difference in interchange.	0.44% + $0.06	0.57% + $0.14
U.S. : Total Transaction Volume Based on 2008 volumes[49]. Not accounting for growth.	$527 billion	$1513 billion
U.S. : Reduction in Interchange The difference between magnetic stripe interchange on U.S. Total Transaction Volume and EMV interchange on U.S. Total Transaction Volume.	$0.32 billion	$1.36 billion
U.S. : Total Reduction in Interchange	$1.68 billion	

Appendix 2 – Card Payment Alternatives

There are many alternative forms of payment besides cash, cards and cheques for purchases made in both the real world and online. Despite the variety on offer, however, cash and payment cards remain the world's leading payment methods. Information is provided below on some alternative payment methods which can be found in today's global market.

Alternative Entry Payment Methods

Alternative Entry Payment Methods involve physical or virtual tokens replacing payment cards. These tokens either link to cards for CNP transactions, or to a prepaid account, an ePayment service, a bank account, or in some exceptional cases a mMoney or eCurrency account.

A good example is the use of mobile phone cameras to scan Quick Response (QR) barcodes[50] of products or bills in the real word directly into online shopping carts where payment is collected. The Mobio[51] QR-based payment system is used by some Canadian restaurants for bill payment in this way. Another approach, being piloted by both Starbucks and PayPal[52], is to use QR codes to encode payment card/membership details. The QR code is displayed on the customer's mobile device screen as a virtual card, which in turn is scanned at POS when the customer wants to pay.

Bump[53] is a promising and innovative payment application. A PayPal payment is initiated between the owners of two mobile devices, by bumping these devices together. The devices have to be girometer-equipped, location-aware and connected to the internet. The shockwave generated during the bump will be identical and unique to the location where the bump happened. When the shockwave and its location are uploaded to a server (a process known as geotagging) and bumps are matched accordingly, the server determines which two devices were bumped together. Payment between owners is then initiated.

ePayment and eCheckout

The strongest perceived competitors of card payments are ePayment and eCheckout services such as PayPal, Google Checkout, the Apple iTunes Store and Application Store. Many of these services claim to be more secure or easier to use than credit cards and in general this may be true; in most cases, these services do provide value and a solid business case. They certainly will not replace card payments however, as the core payment functionality of ePayment and eCheckout services is based on CNP credit card transaction processing methods. These services are dependent on card payments and cannot exist in their current form without the cards upon which they are based.

eCurrencies

Historically, eCurrencies failed spectacularly to penetrate the mass payment market and remained on the sidelines of the payment landscape. Today, they mainly exist for niche applications, such as Facebook's Credits and Second Life's Linden Dollars which are both virtual currencies used for in-game purchases.

The main obstacle for eCurrencies is that there are not enough outlets in the real world where consumers are able to purchase them with cash. In most cases you have to buy eCurrency with a direct bank transfer or with a credit card. This seems to defeat the object; unless you are buying eCurrency for increased security or protection against currency fluctuations, why not just purchase the goods directly with the card, or an ePayment or eCheckout service?

Additionally, two of the most successful and well established general purpose eCurrencies, eBullion[54] and e-gold[55] have given eCurrencies in general a poor reputation. Both products were shut down due to money laundering violations.

mMoney

M-PESA[56] [57] is an excellent example of a successful mobile money payment system. M-PESA has become very popular in a short amount of time and has been outperforming card-based payments throughout Kenya. It was also recently launched in Tanzania. The success of the product lies in the large informal economy in Kenya where payments between unbanked or underbanked consumers and small retail businesses are common. In this environment, the profits earned by informal traders do not justify the expense of POS terminals in order to accept cards. Large proportions of the population however, have a mobile phone and the ability to send an SMS.

Among other services, M-PESA enables cellular subscribers to transfer money to other subscribers using SMS. Cash gets into and out of the system through a network of distributors including prepaid airtime voucher distributors, banks, post offices and grocery stores. The service is secured through the Subscriber Identity Module (SIM) card and the use of a PIN.

M-PESA is a low cost, person-to-person payment and stored value system with wide acceptance and it is applauded for the positive impact on local economies in developing countries. It is unlikely however, that an SMS-based payment system will ever displace card payments in a developed economy. Cards are much more user friendly, widely accepted, and increasingly fast at checkout lanes.

Cash and Cards: Nothing Comes Close

There are many small scale payment alternatives to cash and cards and all seem to enjoy their own niche applications. The alternative payment market is notoriously difficult, with strong competition and a high failure rate among new start ups[58].

A key criteria for the success of any payment system is its ambiguity. In other words, the payment method must be widely accepted and allow easy access to the world's primary payment method, cash.

Payment cards remain unchallenged by alternative payment methods. Today plastic cards are the second most widely used form of payment and there are no viable alternatives to replace this in the next five to ten years. Unless a new payment instrument can provide a cash distribution network equivalent to the 1.8 million ATMs worldwide[59], or offer an acceptance network with more than 40 million POS terminals[60] worldwide where consumers can easily, securely and instantly pay with their cards, alternative payment instruments will remain a value-add to cards and will not be able to displace them.

The next iteration in the evolution of cards is expected to be the deployment of NFC contactless payments. These will be delivered via a contactless card implemented on an NFC-enabled device, such as a mobile phone with embedded NFC secure element. An NFC token is a card in another form factor. From a terminal perspective an NFC contactless transaction is indistinguishable from a contactless card transaction.

Appendix 3 - Example EMV Card Models for the U.S. Market

An EMV card that reflects the usage model currently active in the U.S. should mimic the user experience of the current environment and should not affect the interchange status quo (see Myth One).

The potential designs for EMV cards presented in this section make use of multi-application functionality and rely on EMV application selection to enable the cardholders' choice of application. EMV applications are displayed to cardholders using either the application label or preferred application name. Both are personalised on the card, read by the terminal and displayed to the cardholder. This allows issuers to choose the names of the applications used by cardholders.

Magnetic stripe cards rely on terminals to determine which cardholder authentication mechanism to be used. EMV terminals automatically select the first authentication method supported by the card and the terminal which matches the transaction conditions[61].

EMV cards can be designed in many ways. Only a few brief and simple examples have been provided here to illustrate some of the options available.

U.S. EMV Debit Cards

If a cardholder wants to pay with their debit card in a U.S. retail environment, they will typically hand their card to the cashier who will swipe the card at the POS. A prompt will appear offering the choice of debit or credit. The cashier will then ask the cardholder whether they want to pay using credit or debit. In the U.S., the choice between credit and debit in this scenario where they have already chosen to pay with their debit card, is simply the difference between paying with signature verification (credit) or PIN (debit).

To ensure that this current customer experience is replicated on EMV cards, a multi-application card should be used, together with EMV application selection. This way, the cardholder can select either a 'credit' or 'debit' application. The card would contain at least two applications, both of which would be debit applications pointing to the same account. The difference would be in the labelling and in the cardholder verification methods. This is indicated in Table 1 below.

Table 1: Example Model of a U.S. EMV Debit

Application	Displayed to cardholder	Cardholder Verification Method	Account
Debit (PIN - Primary)	'Debit'	PIN	Debit
Debit (Signature)	'Credit'	For cash: PIN For purchase: Signature	Debit

In this illustration, PIN debit is the primary application because debit purchases outside of the U.S. normally require PIN verification. Primary applications can be automatically selected at terminals that do not support cardholder application selection. This might include unattended terminals such as those found in vending machines, parking meters and toll road booths.

U.S. EMV Credit Cards

In the U.S., credit applications are usually verified by signature. While internationally the trend for both debit and credit is to use PIN, EMV does offer issuers the choice of using PIN or signature, as shown in the illustrations provided in Table 2 and Table 3 below.

Table 2: Example Model of a U.S. EMV Credit Card (Signature)

Application	**Displayed to cardholder**	**Cardholder Verification Method**	**Account**
Credit	‘Credit’	For cash: PIN For purchase: Signature	Credit

Table 3: Example Model of a U.S. EMV Credit Card (PIN)

Application	**Displayed to cardholder**	**Cardholder Verification Method**	**Account**
Credit	‘Credit’	PIN For terminals that do not support PIN: Signature	Credit

U.S. EMV Combi Cards

Combi (or Combo) cards are EMV cards that can be used to access multiple accounts. Combi cards are used in Canada, South Africa, Australia and Singapore. Card issuers who issue both debit and credit cards to the same cardholders can save card issuing costs by issuing one EMV Combi card instead of two cards per cardholder.

An EMV debit card, as illustrated earlier in this section, can easily be extended to include a credit application, as shown in Table 4 below.

Table 4: Example Model of a U.S. EMV Combi Card

Application	**Displayed to cardholder**	**Cardholder Verification Method**	**Account**
Debit (PIN)	'Online Debit' or 'PIN Debit' or 'Debit'	PIN	Debit
Debit (Signature)	'Offline Debit' or 'Signature Debit' or 'Scheme Debit'	For cash: PIN For purchase: Signature	Debit
Credit (Primary)	'Credit'	For cash: PIN For purchase: Signature	Credit

To avoid confusing the cardholder, signature debit and PIN debit labels are changed to indicate the different types of debit. Application labels used here may be tailored to represent issuer's brands in order to make them more recognisable to cardholders.

In the case illustrated, the credit application is the primary application since the brand printed on the card and on the magnetic stripe will probably be a credit brand. To the consumer such a card will primarily be a credit card with additional debit functionality.

Glossary of Abbreviations

3DES -	Triple Data Encryption Algorithm
ATM -	Automated Teller Machine
CAP -	Chip Authentication Program (MasterCard)
CDA -	Combined Cryptogram Generation and Dynamic Data Authentication
CNP -	Card-not-Present
CVM -	Cardholder Verification Method
DDA -	Dynamic Data Authentication
DPA -	Dynamic Passcode Authentication (Visa)
DSA -	Digital Signature Algorithm
ECC -	Elliptic Curve Cryptography
EFT POS -	Electronic Funds Transfer Point of Sale
EMV -	Globally accepted payment standard developed by EMVCo, which is owned by AmericanExpress, JCB, MasterCard and Visa
G20 -	The Group of Twenty Finance Ministers and Central Bank Governors
ISOs	Independent Sales Organisations
NFC -	Near Field Communication
Payment System -	Also known as Payment Scheme/Payment Network
PCI DSS -	Payment Card Industry Data Security Standard
PCI PED -	Payment Card Industry PIN Entry Device
PCI PTS -	Payment Card Industry PIN Transaction Security
PIN -	Personal Identification Number
POS -	Point of Sale
QR -	Quick Response
ROI -	Return On Investment: the total value gained after a solution has been deployed[62]
RSA -	Rivest, Shamir & Adleman (public key cryptography)
SDA -	Static Data Authentication
SIM -	Subscriber Identity Module
SMS -	Short Message Service
U.K. -	United Kingdom
U.S. -	United States
USB -	Universal Serial Bus

List of References

1. Wikipedia - Magnetic Stripe
2. Wikipedia - EFT POS
3. Gizmodo.com - Attack of the Card Skimmers
4. Nilson Report
5. SC Magazine - Retailers Get Compliant with PCI
6. TheTechHerald.com - Does the Heartland Breach Prove PCI Useless?
7. MasterCard - Liability Shifts
8. Wikipedia - G20
9. Cobweb.ecn.purdue.edu - Magnetic Stripe
10. UK Cards Association - Card and Banking Fraud Figures
11. Wikipedia - Chip and PIN
12. Computerworld - Smart Credit Cards Arrive in U.S.
13. Gemalto - Is it time for EMV in the U.S.?
14. Pymnts.com - What's Next With Card Regulation?
15. Smart Card Alliance - Will the Durbin Amendment Lead to Chip and PIN in the U.S.?
16. Smart Card Alliance - EMV Cards Issued in US
17. Creditcards.com – U.S. Mag Stripe Credit Cards on Brink of Extinction
18. Bankrate.com - Will your Credit Card Work Abroad?
19. Vigilant.tv - Banks Call for Ban on Mag Stripe Readers
20. Bankinginsurancesecurities.com - Malaysia to Ban Mag Stripe ATM Cards
21. Digitaldebateblogs - Help! I Can't Stop Posting About SEPA
22. Getfluentc.com
23. Gemalto - Is It Time for EMV in the U.S.?
24. Portals and Rails- Can Chip and PIN Technology Address Payment Card Fraud in U.S.?
25. Smart Card Alliance - Visa Announces New Smart Card as Chip Card Prices Drop
26. Wikipedia - Microcontroller
27. Smart Card Alliance - Wal-Mart Calls for Chip and PIN
28. American Banker - Wal-Mart Claims Issuers Block Progress of EMV in U.S.
29. EMVCo.com
30. Fenton, University of Ottawa - Introduction to Handwritten Signature Verification
31. Visa
32. Zug.com - Crazy Signature
33. Moneybluebook.com - What's the Point of Signing your Credit Card Receipt Anymore?
34. PCIsecuritystandards.org
35. NilsonReport.com
36. Mercator, The Economics of Debit Acquiring, February 2010
37. Computeractive - APACS Releases Fraud Figures
38. Finextra – U.S. Risks Becoming Global Centre for Card Fraud
39. Wikipedia - 3-D Secure
40. Wikipedia - Chip Authentication Program
41. Visa Europe - Dynamic Passcode Authentication
42. Sullivan - The Changing Nature of U.S. Card Payment Fraud
43. EMVCo.com
44. ZDNet.co.uk - Chip and PIN is Broken
45. Digitalidnews.com - EMV Hack may be Overstated
46. MasterCard Interchange Rates and Fees
47. MasterCard Interchange Rates and Fees
48. Mercator, The Economics of Debit Acquiring, February 2010
49. Mercator, The Economics of Debit Acquiring, February 2010
50. Nokia - QR Codes
51. Mobio
52. PayPal Payment with a QR Code
53. Bump
54. Wikipedia - E-Bullion
55. Wikipedia - E-gold
56. Wikipedia - M-Pesa
57. Pymnts.com - Mobile Payments go Viral M-PESA in Kenya
58. Pymnts.com - Is it a Dud on Not? Views on Payments Innovation
59. Wikipedia - ATM
60. Hot Times at the POS: Annual POS Vendor Survey
61. EMVCo, EMV 4.2, Book 3 – Application Specification, June 2008
62. Open Options Glossary

About Bell ID

Bell ID is the world's leading provider of management software for smart cards, associated applications and cryptographic keys. Its dynamic, trusted and totally secure management systems are in use by high-profile organisations, institutions and governments across the globe because they offer an unparalleled lifecycle management solution for cards, applications and cryptographic keys across single and multi-application smart card programmes.

Bell ID supports many leading international banks and financial institutions as they phase their migration from magnetic stripe to chip technology in order to provide more secure and enhanced applications, such as debit / credit, electronic purse and loyalty. Bell ID's technology addresses mass issuance, data preparation, cryptographic key management, EMV parameter management, EMV issuer script delivery, branch / instant issuance, static and dynamic multi-application management, post-issuance personalisation, Mobile (NFC) application management and other features.

For more information on how Bell ID can assist in your smart card operations, please visit www.bellid.com or contact us directly on +31 10 885 1010 / info@bellid.com.