Chip in the U.S.-
The Facts

Debunking the myths concerning EMV advancement in the United States

Written by

Dr. Toni Merschen
Principal at Toni Merschen Consulting
t.merschen@online.de

Table of Contents

1. Introduction 3
2. EMV in General 4
   2.1. Myth: EMV doesn't solve the problem. 4
   2.2. Myth: EMV has been deployed mostly to make offline transactions more secure. 5
   2.3. Myth: EMV cannot be leveraged for card-not-present (CNP) transactions. 5
   2.4. Myth: EMV is not secure enough. 6
   2.5. Myth: EMV is outdated and not relevant for contactless or mobile transactions. 6
   2.6. Myth: EMV only benefits the issuers 7
   2.7. Myth: EMV has too many options and is too complicated to implement. 7
3. EMV in the U.S. 8
   3.1. Myth: It ain't broken, don't fix it. 8
   3.2. Myth: The U.S. Business Case for EMV migration is not positive 10
   3.3. Myth: The Durbin amendment and the suggested caps on interchange fees prevent the U.S. from migrating to EMV. 11
   3.4. Myth: Everybody can go his own pace and may follow a standard replacement cycle. 12
   3.5. Myth: An issuer can take a laggard position and wait until the market has settled. 12
   3.6. Myth: The U.S. financial industry is ready and prepared to start the migration. 13
   3.7. Myth: After having spent billions on PCI DSS compliance, EMV just adds another major expenditure for the merchant side. 14
4. EMV's Relationship with Contactless and Mobile 14
   4.1. Myth: We can skip EMV Chip & PIN and move straight to contactless and mobile. 14
5. Summary 15
6. References 17
7. Contact information 19

1. Introduction

The discussion of introducing EMV[1] compliant chip cards, terminals and ATMs in the United States has been going on for more than 10 years. Many contributions to this discussion have stayed on the surface of the issue and have lacked intimate knowledge of the cost and benefits, challenges and opportunities of EMV. As is often the case with heated topics, the arguments for and against EMV are heavily influenced by the position the participants hold in the payment system value chain, whether they are banks, merchants, technology suppliers, analysts or the media. The aim of this paper is to explain the basic facts of EMV against the backdrop of a considerable set of myths that have been nurtured over the years, some of which have come to light more recently.

Fraud prevention is at the heart of EMV. In the U.S., the technical evolution of card payment systems over the last five decades has certainly been conducive to the somewhat entrenched status quo of addressing card payment fraud in the country. The U.S. banking industry has significantly invested in payment networks and back-end systems and benefitted from the low-cost and ubiquitous telecommunications infrastructure. Since – as a consequence - transactions are almost 100 percent authorized online the back-end systems can filter fraudulent transactions based on transaction scoring techniques and cardholder purchase behavior analysis. This happens sometimes while the transactions are happening, but mostly after the fact. The remaining fraud expenditure is still huge in nominal dollar terms, and a fundamental reason is the use of outdated magnetic stripe technology. By and large, however, the fraud cost has so far been regarded as tolerable by many market players when compared to the total turnover of the underlying card transactions, particularly when put in contrast to the perceived cost of a technology update toward chip cards and terminals.

Some aspects, however, have changed recently as related to several trends including U.S. payment card fraud, the growing level of inconvenience U.S. cardholders experience abroad and questions about fraud associated with innovative payment methods such as contactless and mobile.

- **Physical World Fraud**
  It is the consensus amongst observers – although there are no published fraud numbers[2] in the U.S. like there are in other domestic markets – that physical world fraud in the U.S. is already above the global average and still on the rise. Furthermore, the lessons learned from the many migration activities worldwide clearly indicate that fraud migrates towards those regions which have not yet migrated to EMV chip technology (Malaysia to Thailand, UK to mainland Europe, etc.). Since the rest of the world has either already migrated to EMV or has firm plans to do so the U.S. will certainly become the primary target of fraudsters and fraud rates will continue to rise unless the U.S. decides to migrate, too.
- **Data Base Breaches**
  A second fraud topic on everybody's mind is the theft of personal payment data from merchant and processor data bases. The direct and indirect fraud cost, and the cost of trying to protect against these breaches by means of implementing protective measures according to PCI DSS

[1] EMV stands for Europay, MasterCard, and Visa, the companies that originally created the global EMV® standard for credit and debit payment cards based on chip card technology. The EMV® Integrated Circuit Card Specifications are managed, maintained and enhanced by EMVCo, a company owned by American Express, JCB, MasterCard and Visa. For details see www.emvco.com.

[2] The SCA report 'Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?' from February 2011 says: 'There are no reliable, precise, consistent statistics for U.S. payment fraud. Rather, the industry relies on surveys and extrapolations to gauge the levels and trends for payment fraud. By any account, however, the value of losses are significant.'

requirements and other technologies such as encryption and tokenization, goes into the tens of billions of dollars [MAG 2010]. In spite of this effort and expense, the industry does not seem to be able to fundamentally prevent data base breaches.

- **Cardholder Inconvenience Abroad**
  With market penetration of EMV technology deployment growing around the world, in particular the nearly 100 percent coverage in the Single Euro Payment Area (SEPA) and soon to be in Canada, the magnetic stripe technology becomes more and more archaic. Tens of millions of U.S. cardholders have been inconvenienced abroad over the last few years by attendants at physical points of sale (POS) refusing to take their cards and even more by not being served at unattended terminals [Aite2009].
- **Mobile and Contactless**
  Finally, there are those who think that the industry can skip EMV chip & PIN and move straight to contactless and mobile, whereas others are not sure if these new and innovative methods of payment can be securely implemented on the basis of the old magnetic stripe infrastructure prevalent in the U.S. market.

Against this backdrop we will review the state of the art of EMV in general and the fit for purpose of EMV chip technology in the U.S. market, including some considerations on a potential EMV migration strategy and process in the U.S. Since the discussion has been a polarized one over the years, the various positions are best demonstrated by dismantling the major myths that have obscured the EMV discussions over time.

2. EMV in General

2.1. Myth: EMV doesn't solve the problem.

The fact is that EMV has been a tremendous success in preventing fraud. Wherever EMV has been implemented comprehensively, including the objective PIN verification by the chip, significant fraud reduction ratios have been achieved and sustained. The regularly published fraud statistics from many national banking and regulatory authorities such as the Banque de France (www.observatoire-cartes.fr), the UK Payments Administration (http://www.theukcardsassociation.org.uk), and Interac in Canada (http://www.interac.ca), to name a few, clearly prove the point. EMV reduces counterfeit and lost & stolen fraud in the world of POS and automated teller machines (ATM) as well as in card-not present (CNP) scenarios where EMV provides strong, dynamic cardholder authentication. In fact, EMV is the only available technology to prevent card payment fraud from happening in an efficient, systematic and globally interoperable way. Equally important, no other technology that is advertised as an alternative to EMV has the global deployment and support base and the maturity of EMV. In other words, EMV represents a mature ecosystem with established roles and benefits for all stakeholders:

- The underlying standards have been stable for more than a decade. Any necessary evolutionary changes have been carefully managed in a way that each new release or version is always backwards compatible with prior releases. This ensures that the significant

investments in software, hardware, communication networks and backend systems are protected.

- The standards are complemented by an efficient certification regime executed by EMVCo and the payment systems making sure the cards and terminals interoperate worldwide.
- There are a tremendous number of industry suppliers from around the world providing a vast portfolio of certified components. This ensures global competition on price and product quality and innovation.
- Thousands of banks, processors, and domestic and international payment systems in almost every country on the globe have integrated EMV into the fabric of their daily operations; a total of more than 1.2 billion EMV cards and more than 18.7 million EMV compliant POS terminals have been deployed so far. [EMVCo2011]

2.2. Myth: EMV has been deployed mostly to make offline transactions more secure.

The reality is that, while EMV is fully capable of operating offline in a secure way, the vast majority of all EMV chip transactions are globally authorized online. An advantage of EMV is that transactions – whether authorized online or offline - are made more secure by using the chip as an objective electronic verification tool. When an EMV card is inserted into a POS or ATM reader, the terminal will authenticate the card presented as a genuinely valid card in the payment system (card authentication). By using the PIN securely stored in the chip, card and terminal can objectively confirm that the card is being used by the rightful cardholder (cardholder verification), whether the transaction is face-to-face or card-not-present.

It is certainly worth noting that EMV's offline capabilities have indeed proven efficient in situations where online authentication and authorization are not practical, e.g. for turnstile scenarios in public transport, in low value payment situations or in exceptional situations when communication lines have become unavailable after technical or natural disasters. In any case, the associated risk management parameters stored in the card are under full control, and management of the issuing bank and can be changed individually if necessary post-issuance. Issuers have the choice of forcing every transaction online, but they can also allow a certain number of consecutive low value transactions to execute offline. They can also distinguish between domestic and cross-border transactions.

2.3. Myth: EMV cannot be leveraged for card-not-present (CNP) transactions.

On the contrary; EMV cards and the EMV back-end authentication infrastructure are very well suited as a base for strong, dynamic cardholder authentication using one-time-passwords (OTP). The card can verify the cardholder's PIN offline, either with the help of a small hand-held card reader device (e.g. Barclays PINsentry, http://www.barclays.co.uk/Helpsupport/IntroducingPINsentryforOnlineBanking/P1242559314766) or by using a 'keyboard' integrated into the card (e.g. MasterCard's Display Card http://www.theasianbanker.com/press-releases/mastercard-unveils-first-display-credit-card-with-bank-sinopac-in-taiwan) and then produce an OTP which is displayed on the device or on a small display embedded in the card. During an online transaction, the

cardholder transmits this OTP to the issuing bank who is then in a position to verify the OTP using its EMV back-end authentication system. This constitutes dynamic two-factor authentication (2FA) on the base of something you have and something you know. Handheld readers have been distributed to tens of millions of cardholders in Europe and Asia. When these devices are used, online banking fraud has been basically reduced to zero (e.g. http://www.silicon.com/management/cio-insights/2008/07/18/has-barclays-stamped-out-fraud-with-pinsentry-39261452/.

It is worth noting that weak authentication in the non-face-to-face world is at the root of much of the negative news on data breaches and identity thefts. Indeed, identity theft has ranked first among complaints to the U.S. Federal Trade Commission for 11 consecutive years, with 1.34 million in 2010, twice as many as in the next category, which is debt collection. Much of that theft could be avoided if authentication in non-face-to-face situations would not only be based on something you know (i.e. something could be stolen from a database) but would be made much stronger by, for example, using OTPs generated by EMV cards.

2.4. Myth: EMV is not secure enough.

As a matter of fact, EMV is based on strong cryptography (both symmetric and asymmetric) and elaborate key management; a fundamental EMV principle is to digitally sign payment data to ensure transaction integrity. As opposed to magnetic stripe technology, a chip is extremely difficult to crack; card authentication and PIN verification are performed automatically and objectively by the chip. An important aspect of EMV is its use of dynamic data. Each transaction carries a unique 'stamp' which prevents the transaction data from being fraudulently reused, even if it is stolen from a merchant's or processor's database. EMV's dynamic data feature basically says 'if you can't prevent data from being stolen, make the stolen data useless' because dynamic data is only useful for the sole transaction it characterizes, nothing more.

Although EMV has been heavily scrutinized by criminals and the academics, there have been no reported real-life, in-market, or business relevant breaks of the EMV technology. Every once in awhile, academics point to weaknesses in EMV in general or identify shortcomings in individual implementations of EMV. In any one of these cases, which are mostly only relevant under laboratory conditions anyway, either the EMV specifications have an answer to the challenges already built in or the residual risk can be eliminated by standard payment system security mechanisms.

2.5. Myth: EMV is outdated and not relevant for contactless or mobile transactions.

EMV specifications are continuously monitored by EMVCo and the other stakeholders reflecting the ever growing implementation experience in multiple markets across the globe. They have been updated in an evolutionary and backwards compatible way to meet the changing requirements of the payment industry. EMVCo has been constantly assessing the strength of its cryptographic base and adapting the lengths of its current

cryptographic keys periodically. Longer keys are more secure than shorter keys in a similar way that long passwords are more secure than short passwords. Looking into the future, EMVCo working groups are currently assessing how a migration to Elliptic Curve Cryptography can help to reduce the necessary key lengths, streamline cryptographic processing and reduce the number of data authentication mechanisms in EMV while increasing security at the same time.

Contactless and mobile EMV technology is actually at the base of contactless payment applications currently supported by the international payments systems. The use of ”secure elements” for securely storing sensitive consumer data and the notion of digitally signing payment data to achieve transaction integrity and avoid data reuse are common in contact, contactless and mobile payment scenarios. Since standardization in this area is essential, EMVCo has worked in close cooperation with other relevant standardization groups such as the NFC Forum, the GSM Association and GlobalPlatform to arrive at a suitable architecture for EMV contactless and mobile payments. This includes requirements for mobile handsets, for the customer user interface and for the mobile secure element containing the EMV payment application. When mobile proximity payments become more widespread the existing EMV infrastructure stands ready to ensure that they are as secure as contact chip and PIN transactions are today (for more details see section 4.1).

2.6. Myth: EMV only benefits the issuers.

Issuers are generally liable for card fraud related to face-to-face transactions and therefore benefit from the reduction of direct fraud cost in this channel. One of the most understated aspects of the migration to chip, however, is the productivity increase on the merchant and acquiring side of the equation. Significant savings result from replacing signed paper slips by electronic records simplifying the handling of fraud, in particular the retrieval of payments records while dealing with chargeback requests. Likewise, the checkout process at the POS, cash handling in general and the cashier’s after-hours balancing procedures are streamlined and shortened.

When CNP fraud is included in the equation, the picture gets even more attractive for the merchants. Merchants are liable for CNP fraud unless they are participating in strong authentication programs based on 3DSecure technology. These programs can be enhanced by the dynamic data features of EMV which also helps to dramatically reduce maintenance and continuous auditing cost for PCI DSS on the merchant side (for more details see section 3.7).

2.7. Myth: EMV has too many options and is too complicated to implement.

Indeed, EMV is a powerful toolbox to reduce fraud in many channels and commerce environments. It is not a one size fits all, canned solution. All stakeholders need to make changes to their parts of the payment infrastructure and associated processes. These modifications span the entire card payments space from the acceptance terminals installed

at retailers or in unattended purchase and cash withdrawal scenarios, through acquirer switches and networks, all the way to issuer authorization and card production systems. A proper choice of the appropriate solution elements and parameters is necessary to achieve optimal results. But it is not “rocket science.” Thousands of successful implementations have been launched by banks, merchants and processors – big and small – across the globe and as said earlier, there is a mature support infrastructure offered by the international payment systems and the vendor community to assist the banks and merchants.

So much for the state of the art of EMV technology and its deployment worldwide. In the next chapter we will describe some of the perceived inhibitors of a successful migration of the U.S market to EMV.

3. EMV in the U.S.

3.1. Myth: It ain’t broken, don’t fix it.

The U.S. card payment system is certainly not broken as far as its basic functionalities are concerned, at least not in the U.S. domestic payment market environment. There are, however, two aspects which are getting more and more annoying to say the least, and these are threats to payment security and the decline of global acceptance for U.S. issued cards.

- Security

  The scene on the security and fraud side is becoming dramatic. It is the consensus among observers – although in the U.S. there are no published fraud numbers like in other domestic markets – that physical world fraud in the U.S. is already above the global average today and is on the rise. The lessons learned from the many migration activities worldwide clearly indicate that fraud migrates toward those regions which have not yet migrated to EMV chip technology. The rest of the world has either already migrated or has firm plans to do so. If the U.S. will not migrate soon it will certainly become the primary target of the fraudsters, and fraud rates will continue to rise. A second fraud topic is the theft of personal payment data from merchant and processor data bases. The direct and indirect fraud cost and the cost of trying to protect against these breaches by means of implementing protective measures according to PCI DSS requirements goes reportedly into the tens of billions of dollars [MAG 2010]. In spite of this effort and expense, the size and frequency of massive data compromises seem to be growing. It is the consensus of industry experts that the industry will be unable to prevent every attack. The use of dynamic data as specified by EMV, however, will make sure that the data that could potentially be stolen is useless to the criminal. The current security situation in the U.S. card payment industry has already raised significant concerns with the cardholders and the media. As a consequence the U.S. regulators (represented by the FFIEC) are investigating and they have recently published a Supplement to the 2005 Guidance entitled ‘Authentication in an Internet Banking Environment’ [FFIEC2011] to ‘reinforce the Guidance's risk management framework and update the Agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment.’ Politicians have turned to the issue, e.g. U.S. Senator Robert Menendez, D-N.J., in a June 15 letter to the head of

the OCC, called for a deeper investigation into the breach, asking that the bank's customer notification policy be reviewed. "As Citigroup's primary regulator with jurisdiction for data security issues, I hope that you also believe this to be unacceptable for consumers," Menendez says. "Over the last six years, there have been 288 publicly disclosed breaches at financial services companies that exposed at least 83 million customer records. ... This problem is widespread and must be properly addressed by all parties [Bankinfo2011]."

- Global acceptance

  Market penetration of EMV technology deployment has been growing around the world since 2003, with CAGRs of 43% for cards and 48% for terminals between 2003 and 2010. Here are the latest numbers as published by EMVCo as of May 2011 [EMVCo2011]:

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribbean	207,715,356	31.2%	3,900,000	76.5%
Asia Pacific	336,602,681	27.9%	3,480,000	43.0%
Africa & the Middle East	23,003,747	17.6%	345,000	60.7%
Europe Zone 1	645,472,323	73.9%	10,500,000	89.0%
Europe Zone 2	27,516,286	12.7%	513,600	65.4%
United States†				
TOTALS	1,240,310,393	40.1%	18,738,600	71.1%

* Figures reported in Q1 2011 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally.

† Figures do not include data from the United States.

Particularly considering the nearly 100 percent coverage in the extended Euro zone and soon in Canada, the magnetic stripe technology becomes antiquated. Tens of millions of U.S. cardholders have been inconvenienced abroad over the last few years [Aite2009] by attendants at POS terminals refusing to take their cards and even more by being unable to buy gas at unattended terminals or transportation tickets at ticket machines (and therefore being forced to join the usually long lines at the few remaining - if any - attended ticket booths). U.S. media are more and more frequently covering the issue, not only via the trade press but also in daily newspapers. *The New York Times*, for instance, published a feature article in its popular travel section on June 8, 2011 stating: 'Until businesses change their minds, American travelers will continue to encounter payment issues abroad. The problem is two-fold. Even though most European cash registers are equipped to handle American cards, some cashiers simply don't know how to process them. And many automated ticket kiosks like those commonly found at train stations, gas pumps and parking garages simply don't accept cards without a chip and PIN' [NewYorkTimes2011].

The negative trend vis-à-vis acceptance of magnetic stripe cards will be aggravated by the recent resolution of European banks - at the request of their regulators at the

European Central Bank - to eliminate the magnetic stripe from European cards altogether and/or to allow merchants generally to reject magnetic stripe card based transactions. Europeans on the other hand will resort more and more to cash when they come to the U.S. when their debit and credit cards no longer work because of the absence of the magnetic stripe. (http://travel.nytimes.com/2011/07/03/travel/credit-card-problems-abroad-readers-respond.html?ref=practicaltraveler)

So, in a sense, it **is** broken.

3.2. Myth: The U.S. Business Case for EMV migration is not positive.

While this may have been true five or ten years ago, today the U.S. business case is definitely positive. A couple of business case elements have changed for the better (in terms of their significance for the bottom line of the business case) over the last couple of years and contributed to this new situation:

- Direct cost of fraud in the U.S. is definitely on the rise as described above. Additionally, the industry needs to fully acknowledge that cost of fraud is not limited to the direct net fraud losses; fraud management expenses contribute rather substantially to the overall fraud cost. Visa suggests that indirect fraud costs are “at least equal to direct fraud losses, and can often be much higher” [Visa2009]. Visa also claims that ”opportunity costs, which include the behavior of cardholders subsequent to experiencing fraud, vary considerably — but can easily account for more than 15 percent of total fraud costs.” As said before, the cost of the alternative measures that the U.S. payment industry uses for detecting and mitigating fraud as described above have been growing significantly. For instance, as a result of the well known mass data compromises, millions of cards had to be reissued, and customer service costs for issuers and merchants have been increasing. Most of this can be avoided through a proper and comprehensive implementation of EMV. Consequently, Visa has waived significant parts of PCI maintenance and continuous auditing for those merchants who perform more than 75 percent of transactions in EMV mode. Obviously, this only applies outside the U.S.
- The cost of chip cards has decreased considerably over the last couple of years as a result of growing card production capacities, maturing card manufacturing technology and the decreasing prices of the integrated circuit chips. Certainly, the financial industry has benefitted in this regard from the fact that EMV chip technology is very similar to the technology supporting billions of mobile telephones.
- Similarly, the cost of POS terminals has come down significantly. Furthermore, a substantial proportion of POS terminals in the U.S. market already contain chip-reading hardware capabilities onto which EMV software can be downloaded. This situation improves with every new EMV capable terminal shipped as part of the standard POS terminal maintenance cycle.
- Most of the big issuers, acquirers and processors in the U.S. are already issuing chip cards and/or are acquiring EMV transactions based on the fact that they are operating in EMV territory abroad and have had to adapt as a result. They are at least familiar in

principle with the impact of migrating to EMV, and most of them have modified at the very least their international issuing and back end systems to integrate EMV.

Assuming reasonable migration scenarios, the business case for the U.S. is definitely positive with payback periods beginning at a five-year horizon.

There is one problem in this context though which will nearly make sure this myth stays with us for a while unless properly addressed: the lack of proper fraud measurements and reporting in the U.S. As Rich Oliver, executive vice president of the Atlanta Fed and director of the Retail Payments Risk Forum, states: “Much of what exists publicly today in terms of payments system measurements and metrics for fraud comes from independent survey work initiated by trade associations or consultants, such as the American Bankers Association, the Independent Community Bankers Association, and the Association for Financial Professionals. While the data flowing from these efforts is extremely helpful, each survey has its own focus, methodologies differ, and voluntary participation levels vary the statistical accuracy of results” [AtlantaFed2011b]. He suggests: “Perhaps it is time for the government or collective industry groups to address this shortcoming and organize an effort to design and support an approach to collecting statistically accurate, cross-channel payments fraud data to be publically shared. Metrics stemming from a data-gathering initiative could go a long way toward helping a troubled industry wrestle with the business case behind more aggressive fraud-management efforts” [ibid].

3.3. Myth: The Durbin amendment and the suggested caps on interchange fees prevent the U.S. from migrating to EMV.

The Durbin Amendment of the Dodd-Frank Wall Street Reform and Consumer Protection Act gave the Federal Reserve the power to regulate debit card interchange fees. The Federal Reserve has published its rule on June 29, 2011 accordingly, [FRB2011], and established a debit card interchange standard with a cap composed of a base component of 21 cents and an ad valorem component of 5 basis points to reflect a portion of fraud losses. It allowed an additional fraud prevention adjustment of 1 cent per transaction conditioned upon the issuer adopting effective fraud prevention policies and procedures. These regulations become effective on October 1, 2011.

With or without the Durbin rules, it is in the common interest and a joint responsibility of the banks and the merchants to minimize fraud in the payment system. Today, payment card fraud is a significant element of the cost side of the payment card ecosystem. In the current environment, the issuer is liable for the direct fraud at physical world point-of-sale terminals, whereas the merchants generally bear the liability for e-commerce fraud. Additionally, merchants have spent billions of dollars to ensure compliance with PCI DSS in an attempt to properly protect payment transaction data stored in their systems (with questionable success given the continuing series of published data base breaches). Finally, both sides share the indirect cost of handling fraud including chargebacks which has been estimated to be 50 percent of the total if not more.

A proper implementation of an EMV infrastructure in the U.S., both covering physical transactions at the POS terminal and enabling strong, dynamic authentication for remote, non-face-to-face transactions would – besides all its other benefits - provide the base for reducing direct and indirect fraud expenditure. It would also address ongoing PCI DSS efforts. As Visa has concluded outside the U.S., driving the EMV penetration for POS transactions beyond 75 percent would eliminate the need for future PCI DSS maintenance and auditing.

In summary: Properly implemented EMV technology is obviously capable of dramatically reducing direct and indirect fraud cost in the card payment system, both for face-to-face and card-not-present transactions. The crucial point is that the necessary investments to migrate to EMV and the resulting savings need to be rationally reflected in the discussion - both on the issuers' and the merchants' sides. While the industry as a whole seems to have quite a way to go in this direction, the Durbin amendment should provide the much needed motivation to get started on the journey. In particular, since the planned caps on debit interchange fees do not seem to make a difference between signature and PIN, a proper rollout of chip & PIN seems to be more palatable than ever. [3]

3.4. Myth: Everybody can go his own pace and may follow a standard replacement cycle.

In order to optimize the business case of the two market sides, issuers and acquirers / merchants / ATM providers have to move in lock step. In order to achieve this, the stakeholders are well advised to consider forced replacements of cards and terminals outside of the normal replacement cycles. The additional investment has a clearly identifiable return. It is even more important to initiate the migration of the ATM installed base synchronously with the cards and terminals. If ATMs are not made EMV compliant in sync with the POS terminals, the life of the magnetic stripe technology will be prolonged and ATMs become the single point of failure (or fraud for that matter) in the card payment system. This is clearly demonstrated by the cross border fraud migration problems encountered in other parts of the world; the U.S. should benefit from these learnings and not commit the same mistakes.

3.5. Myth: An issuer can take a laggard position and wait until the market has settled.

The fact is that by doing so an issuer risks attracting fraudulent activities to his portfolio and at which point he will have trouble catching up, both technically and from a reputational perspective. Take Brazil as an example: Mauricio Icaza, director of operations for Banco Bradesco SA in Sao Paulo, said "Brazil learned the hard way that a slow transition to EMV cards, commonly called chip-and-PIN cards, creates a rapid shift in fraud for the banks that

[3] Note: There is a big educational deficit considering that on one hand the President and Chief Executive of the Independent Community Bankers of America thinks that reissuing cards helps preventing fraud: "These data breaches are a reminder that interchange revenue is so critical to local community banks; it helps them quickly reissue debit and credit cards to their customers to protect them against fraud" [ABA2011a] and on the other hand the Director of Government Relations of the Food Marketing Institute quotes "Independent analysts have found that U.S. banks are not doing enough to protect against fraud because their ability to transfer so much of those costs onto merchants doesn't leave them with the right incentives" [ABA2011b].

are lagging in their conversions" (American Banker May 2, 2011).

3.6. Myth: The U.S. financial industry is ready and prepared to start the migration.

There is a long list of stakeholders in this country: consumers, merchants, issuers, acquirers, processors, ATM service providers, regulators, media, analysts, etc. The composition of this set of market participants is very inhomogeneous: there are the four or five major nationwide issuers and hundreds of small banks and credit unions; there are giant merchant chains and mom and pop shops, regional PIN only networks and international payment systems. The knowledge base on the principles, operational implications, opportunities and challenges of EMV technologies across this broad stakeholder base is on average rather thin. The U.S. is many years behind the curve. The recent migration examples in Canada, Australia and New Zealand, to name a few, have demonstrated how much time and effort it takes to start from scratch, define a nationwide deployment strategy and execute it. It can obviously be done, but it is hard work. The supply side of the industry, with their products, services solutions and by providing highly specialized consultancy offerings, is more than ready to help based on its international standing and the established EMV standards that can be exploited.

There is also good news in this situation. As a latecomer, the U.S. can learn from the mistakes made by other markets during their migration. As Douglas A. King from the Atlanta Fed puts it: "Based on available data from countries around the globe with EMV experience, EMV chip-enabled cards have been highly successful at reducing counterfeit and lost or stolen card fraud within market. However, these cards have had less impact on overall fraud levels. Fraud has simply shifted to different products (from credit to debit), other channels (from card-present to card-not-present, or CNP), or other geographies (fraud perpetrated abroad). If the U.S. payments industry does decide to move forward with EMV, the experiences in markets that have already undergone or are undergoing the migration to EMV teaches us that issuers, networks, and merchants across all payment channels must make a coordinated effort in order to achieve a positive impact on overall payment card fraud levels. Without coordination, the United States would likely see fraud shifting to other products and channels but not geographies—by then, all developed countries will have converted to EMV, including our neighbors, Canada and Mexico" [AtlantaFed2011a].

The single biggest hurdle for the U.S. to get going is the absence of a nationwide governing body that can consolidate the facts of the business model, facilitate agreement between the major stakeholders and trigger decisions regarding a U.S. EMV migration plan. The existence of organizations such as Cartes Bancaires in France, APACS in the UK, BKM in Turkey or ZKA in Germany has helped tremendously to create and execute migration plans with the necessary rigor and project management discipline. Such a forum needs to be urgently formed and put to work by the stakeholders in the U.S.; as one merchant representative put

it ”to find a way to act together before a catastrophe happens that might force government intervention” (alluding to what happened in the airport security space after 9/11).

3.7. Myth: After having spent billions on PCI DSS compliance, EMV just adds another major expenditure for the merchant side.

The goal of PCI DSS is to “protect cardholder and sensitive authentication data anywhere this data is present within the payment eco-system, thus limiting the availability of this data to fraudsters” [PCI2010]. In contrast, by using dynamic data, EMV aims to reduce fraud before it happens and to eliminate the reusability of payment transaction data for fraudulent transactions. EMV’s dynamic data feature basically says “if you can’t prevent data from being stolen, make the stolen data useless”. Dynamic data is only useful for the sole transaction it characterizes, nothing more. As the PCI Security Standards Council states [PCI2010]: “By design, PCI DSS does not distinguish between underlying transaction security mechanisms, but instead seeks to protect the PAN and other sensitive authentication data as a goal in and of itself without examining the underlying fraud risk should this data be compromised. In the future, should EMV become the sole means of payment in a given face-to-face channel, coupled with a globally adopted robust authentication process for card-not-present (CNP) transactions, the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. As a consequence the PCI DSS would be updated to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly”.

Outside the U.S., Visa already acknowledged the fact that the use of EMV technology makes the continued efforts of maintaining a PCI DSS infrastructure somewhat redundant. They announced a new Technology Innovation Program (TIP) that "will eliminate the requirement that eligible merchants annually validate their compliance with the PCI DSS for any year in which at least 75 percent of the merchant's Visa transactions originate from chip-enabled terminals. To qualify, terminals must be enabled for contact or dual contact and contactless interface chip acceptance."

With future adoption of EMV in the U.S., this rule should be easily applicable to the U.S. market as well and minimize future merchant PCI DSS compliance expenditure.

4. EMV’s Relationship with Contactless and Mobile

4.1. Myth: We can skip EMV Chip & PIN and move straight to contactless and mobile.

Contactless and mobile payment transactions are based on the EMV specifications. This relates to their functionality and transaction flow as well as to the associated security fundamentals. As a result, a mobile transaction is no different from a card transaction at the POS. Enabling the terminal side to perform contactless and mobile transactions means to implement these new features and security measures and change hardware and software of the terminals.

The penetration of contactless terminals supporting proximity payments in the U.S. market is still very low today (at present, only about two percent of the roughly 7 million card-accepting merchant locations in the United States have been equipped with contactless POS terminals since the U.S. contactless-payment rollout began seven years ago [NFCTimes2011]). This means that the bulk of the hardware and software upgrades are still in front of the industry in order to make contactless and mobile payments a success. It would only take a small incremental investment to also provide EMV contact transaction capabilities in these new terminals and thereby open up the U.S. acceptance infrastructure for the globally accepted EMV standard represented by more than 1.2 billion cards as of today. In other words, if the U.S. decides to migrate to EMV terminals supporting EMV contact and contactless, the mobile acceptance comes along as a bonus. The issuing side can then decide whether to issue dual interface cards (contact & contactless) and/or support mobile payments.

5. Summary

There are major technology related challenges the card payment ecosystems face these days, on a global scale and specifically in the U.S. They range from fighting fraud in the physical and card-not-present environments to maintaining global acceptance and interoperability to protecting the integrity of the card payment system in the light of growing attacks from organized crime. Additionally, there are new technologies such as mobile communications entering the payment ecosystems which have the potential to be quite disruptive, both from the functionality and security perspectives. On the basis of the presented facts it becomes obvious that EMV chip card technology presents a mature, efficient and user-friendly solution to address many of the essential challenges in a comprehensive and systematic way – both in the traditional plastics card world and in a converged mobile world. Several efforts have started in the U.S. both on the issuing and the acquiring and merchant sides. Wells Fargo, JPMorgan and U.S. Bancorp, State Employees Credit Union, United Nations Credit Union, Silicon Valley Bank and others have started (or have announced to start) issuing EMV cards mostly to reduce the inconveniences their cardholders have experienced abroad. At the same time, Travelex, a major currency exchange company, began selling a preloaded EMV-enabled pre-paid card in 2010 at major airports and now have extended this service to offering these cards for purchase and home delivery beforehand via the Internet. On the merchant side, Walmart is in the process of upgrading all of its POS terminals to be EMV compliant in order to streamline check out operations and avoid becoming the target of extended fraud.

These efforts must not be confounded with a national migration plan comparable to the ones that were executed in the UK, Turkey or Canada. These efforts alone will not address the key problem, i.e. preventing fraud from happening on all channels, domestically and cross border. Probably the single biggest hurdle for the U.S. to get going is the absence of a nationwide governing body that can facilitate agreement and execute decisions regarding a U.S. EMV migration plan. The U.S. payments infrastructure is highly fragmented in terms of ownership making it difficult to agree on the principles of an EMV migration plan and then execute it in a rigorous and controlled way that allows all stakeholders to reap the return on their investments.

Given the severity of the problems at hand, regulatory intervention can no longer be excluded from

the future set of options if the players in the U.S. card payment ecosystem don't sit down and agree on a strategy. As Randy Vanderhoof, executive director of the U.S. Smart Card Alliance said recently, "the writing is on the wall" for U.S. government direction regarding EMV migration domestically. "The federal government is definitely going to be looking closely at consumer payment issues," he said. "It's a strong signal to the industry that says, 'If you don't address this issue, we are capable of stepping in to regulate or create rules you may or may not appreciate' "[ABA2011c].

So the U.S. payments industry seems to be at the same point the UK was a couple of years ago when the regulator said: "Either you fix the card fraud problem or I will fix it for you." The UK financial industry got the message, joined forces with the merchants and together executed a rigorous chip and PIN migration program with admirable results. The stakeholders in the U.S. payment card ecosystem would be well advised to arrive at a similar conclusion and get going with EMV.

6. References

[ABA2011a] US Banker, Viewpoint, May 2011,: Michaels Breach is Warning on the Durbin Amendment, Camden R. Fine, http://www.americanbanker.com/bulletins/-1038183-1.html?zkPrintable=true

[ABA2011b] American Banker, Bank Think, June 6, 2011: Durbin Rule Will Help Make Payments More Secure, Liz Garner, http://www.americanbanker.com/bankthink/Durbin-Secure-Magstripe-Michaels-1038512-1.html

[ABA2011c] American Banker, June 14, 2011: EMV Migration Proceeding in U.S., But Banks Not in Lockstep, Will Hernandez, http://www.americanbanker.com/issues/176_113/emv-migration-proceeding-in-us-1038854-1.html

[Aite2009] Aite Group, October 26, 2009: The Broken Promise of Anytime, Anywhere Card Payments: The Experience of the U.S. Cardholder Abroad, http://www.aitegroup.com/Reports/ReportDetail.aspx?recordItemID=603

[AtlantaFed2011a] Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, May 09, 2011:United front needed to prevent EMV card fraud from picking low-hanging fruit, Douglas A. King, http://portalsandrails.frbatlanta.org/2011/05/united-front-needed-to-prevent-emv-card-fraud-from-picking-low-hanging-fruit-1.html

[AtlantaFed2011b] Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, May 23, 2011: The dilemma of measuring fraud in the U.S. payments system, Rich Oliver, http://portalsandrails.frbatlanta.org/2011/05/dilemma-of-measuring-fraud-in-us-payments-system.html

[Bankkinfo2011] Bank Info Security, June 17, 2011: Citi Breach: 360K Card Accounts Affected, Tracy Kitten, http://www.bankinfosecurity.eu/articles.php?art_id=3760

[ECB2010] European Central Bank, October 22, 2010: Seventh SEPA progress report, http://www.ecb.int/press/pr/date/2010/html/pr101022_1.en.html

[EMVCo2011] EMVCo Press Release, May 20, 2011: EMVCo Publishes 'A Guide to EMV' as Adoption of the Payment Standard Continues to Increase, www.emvco.com

[EPC2011] European Payments Council, January 31, 2011: Resolution: Preventing Card Fraud in a mature EMV Environment, http://www.epc-cep.eu/knowledge_bank_download.cfm?file=EPC424-10 Approved Resolution on Mature EMV Fraud Prevention.pdf

[FRB2011] Federal Reserve Board, June 29, 2011: Debit Card Interchange Fees and Routing, http://www.federalreserve.gov/newsevents/press/bcreg/20110629a.htm

[FFIEC2011] Federal Financial Institutions Examination Council, June 28, 2011: Supplement to Authentication in an Internet Banking Environment, http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf

[MAG 2010] Merchant Advisory Group, December 13, 2010: Pulling Open the Curtains on the Payment System: Merchant Advisory Group Recommendation on the Mobile Transformation Opportunity, http://merchantadvisorygroup.org/PDFs/MAG_Mobile_Payments_Position_Paper.pdf

[PCI2010] PCI Security Standards Council, October 5, 2010: PCI DSS Applicability in an EMV Environment, A Guidance Document Version 1, https://www.pcisecuritystandards.org/security_standards/index.php

[Visa2009] Payments Cards and Mobile, September/October 2009 Fraud Supplement

[NewYorkTimes2011] New York Times, June 8, 2011: 'How to Avoid Credit Card Problems Abroad' http://travel.nytimes.com/2011/06/12/travel/how-to-avoid-credit-card-problems-abroad-practical-traveler.html?scp=7&sq=june%2012,%202011&st=cse

[NFCTimes2011] NFC Times, June 23, 2011: Google's Schmidt Predicts Contactless Terminal Rollout, Dan Balaban, http://www.nfctimes.com/news/google-s-schmidt-predicts-contactless-terminal-rollout

7. Contact Dr. Toni Merschen

For more information on this white paper or to reach Dr. Toni Merschen directly, please refer to his full contact information listed below.

Dr. Toni Merschen
Principal at Toni Merschen Consulting

Herrberigstr. 5, D-52152 Simmerath, Germany
GSM: +49 1525 3122456
Phone: +49 2473 5493290
FAX: +49 2473 5493291
e-mail: t.merschen@online.de