The Migration to EMV Chip Technology

IIIII EMV Implementation in the U.S.

http://www.gemalto.com

VeriFone
THE WAY TO PAY™

gemalto
security to be free

Table of Contents

The Migration to EMV Chip Technology

EMV Implementation in the U.S.

1. Introduction

Most of the world has fully migrated or is in the process of migrating to EMV chip technology for debit and credit payments. According to EMVCo, approximately 1.2 billion EMV cards have been issued globally and 18.7 million POS devices accept EMV cards as of Q1 2011. This represents 40.1 percent of the total payment cards in circulation and 71 percent of the POS devices installed globally [EMVCO2011].

Given the prevalence of EMV chip technology in the rest of the world, many have questioned if and when the United States would move to EMV. U.S. financial institutions started issuing EMV chip cards to their frequently traveling customers; however the country seemed to be a long way off from acceptance [Gemalto2011]. All of this changed on August 9, 2011 when Visa announced plans to speed up chip migration and adoption of mobile payments in the United States. Visa announced a three-part acceleration plan [Visa2011]:

- **Expand the Technology Innovation Program to Merchants in the U.S.**
  Effective October 1, 2012, Visa will expand its Technology Innovation Program (TIP) to the U.S. TIP will eliminate the requirement for eligible merchants to annually validate their compliance with the PCI Data Security Standard 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 to support both contact and contactless chip acceptance, including mobile contactless payments based on NFC technology. Contact chip-only or contactless-only terminals will not qualify for the U.S. program. Qualifying merchants must continue to protect sensitive data in their care by ensuring their systems do not store track data, security codes or PINs, and that they continue to adhere to the PCI DSS standards as applicable.

- **Build Processing Infrastructure for Chip Acceptance**
  Visa will require U.S. acquirer processors and sub-processor service providers to be able to support merchant acceptance of chip transactions no later than April 1, 2013. Chip acceptance will require service providers to be able to carry and process additional data that is included in chip transactions, including the cryptographic message that makes each transaction unique. Visa will provide additional guidance as part of its bi-annual Business Enhancements Release for acquirer processors to certify that their systems can support EMV contact and contactless chip transactions.

- **Establish a Counterfeit Fraud Liability Shift**
  Visa intends to institute a U.S. liability shift for domestic and cross-border counterfeit card-present point-of-sale (POS) transactions, effective October 1, 2015. Fuel-selling merchants will have an additional two years, until October 1, 2017 before a liability shift takes effect for transactions generated from automated fuel dispensers.

Currently, POS counterfeit fraud is largely absorbed by card issuers. With the liability shift, if a contact chip card is presented to a merchant that has not adopted, at minimum, contact chip terminals, liability for counterfeit fraud may shift to the merchant's acquirer. The liability shift encourages chip adoption since any chip-on-chip transaction (chip card read by a chip terminal) provides the dynamic authentication data that helps to better protect all parties. The U.S. is the only country in the world that has not committed to either a domestic or cross-border liability shift associated with chip payments.

With this announcement from Visa, the United States payments landscape is no longer a future of magnetic stripe technology, but one of EMV chip technology and contactless and mobile payments. This paper will examine why the timing is good for EMV in the United States, and will discuss implementation and cost considerations for merchants and issuers.

2. Why EMV and Why Now?

There are many reasons why EMV chip technology makes sense for the United States. These are some of the major factors:

> **Physical World Fraud**
It is the consensus amongst observers – although there are no published fraud numbers 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, if the United States did not move to EMV, it could become the primary target of fraudsters and fraud rates will continue to rise. The move to EMV would, in theory, prevent this from happening.

> **Cardholder Inconvenience Abroad**
With market penetration of EMV technology deployment growing around the world, in particular the nearly 100% 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 POS refusing to take their cards and even more by not being served at unattended terminals [Aite2009].

> **Mobile and Contactless**
Implementing EMV chip technology in the United States will speed up mobile and contactless payments and make them more secure. The devices that accept EMV chip cards are dual contact/contactless devices. By installing these devices to accept EMV, merchants are also readying themselves to accept mobile and contactless payments as well.

3. What is EMV?

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.

3a. Fraud and EMV

EMV has been tremendously successful 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 physical points of sale (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 devices 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]

EMV Security

From a real-world fraud-prevention standpoint, EMV is significantly more secure than traditional magstripe cards. Through the use of advanced encryption, embedded card risk analysis capabilities, and online and offline authentication, most of the traditional methods used to steal card data or to clone cards using magstripe technology are rendered worthless, or at the very least, very difficult to accomplish.

That said, as with other major EMV rollout initiatives in the UK, Canada, Australia and other countries around the world, the migration to EMV Chip and PIN/Chip and Signature in the U.S. will occur in stages, with merchants, banks, processors and others working loosely towards a singular goal, but at their own speeds.

What this means is that best case card security scenarios—no magstripe fallback, DDA or CDA offline authentication only, smartcard onboard risk analysis capabilities, no manual PIN entry—can't be assumed. There will be an interim period while the infrastructure is being built, likely spanning several years, where prudent security practitioners will continue to invest in additional security measures such as point-to-point encryption products that ensure Track 1 and 2 data are encrypted prior to transmission and advanced tokenization techniques that replace card data with a random value, thereby protecting merchants from storing unsecured card data while also potentially releasing significant portions of their infrastructure from PCI scope.

3b. When the Card is Not Present

EMV is also helpful for authentication when the card is not present, i.e. online or over the phone. 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 experienced significant reduction. (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.

4. Benefits of EMV to Issuers and Merchants

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).

5. Benefits/ Considerations for EMV in the U.S.

In the United States, 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. Without the migration plan specified by Visa, the United States would certainly become the primary target of the fraudsters, and fraud rates would 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, these massive data compromises continue to occur (e.g., Sony, 2011). On the backs of these high-profile attacks, data clearly show a growing trend towards breaches occurring in smaller retail sites, albeit for smaller overall gains. But regardless of whether one gets 1 million records from one breach, or 1.5 million from ten breaches, the outcome is the same.

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 which 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]."

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 migration to EMV in the United States would therefore put many of the issues mentioned above to rest.

5a. U.S. and Travelers

One of the biggest benefits of the U.S. migrating to EMV is payment interoperability with most of the world.

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

Worldwide EMV Deployment and Adoption*

REGION	EMV CARDS	ADOPTION RATE	EMV TERMINALS	ADOPTION RATE
Canada, Latin America, and the Carribean	207,715,356	31.2%	3,900,000	76.5%
Asia Pacific	336,602,681	27.9%	3,480,000	43.0%
Africa and 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[1]				
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.
[1]Figures do not include data from the United Satates.

Particularly considering the nearly 100% 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).

To solve this traveler payment problem which would only grow worse, it is an ideal time for the United States to start the move to EMV.

5b. Costs

The business case for implementing EMV technology has changed for the better (in terms of their significance for the bottom line of the business case) over the last couple of years:

- 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 outside of the United States, and will now do the same for U.S. merchants.

- 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 payment and POS devices has come down significantly. Furthermore, a substantial proportion of POS devices 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 device shipped as part of the standard POS device 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.

5c. Moving at the Same Pace

With its announcement, Visa is urging issuers and merchants to move at the same pace, which is positive for the U.S. 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 devices 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 devices. If ATMs are not made EMV compliant in sync with the POS devices, 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 lessons and not commit the same mistakes.

5d. Contactless and Mobile Payments

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 device side to perform contactless and mobile transactions means to implement these new features and security measures and change hardware and software of the devices.

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 devices 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, the U.S. migrating to EMV devices supporting EMV contact and contactless would bring mobile acceptance as a bonus. The issuing side can then decide whether to issue dual interface cards (contact & contactless) and/or support mobile payments.

6. A Good Start

Before Visa's announcement, there was already a lot of support for EMV in the United States. 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 devices to be EMV compliant in order to streamline check out operations and avoid becoming the target of extended fraud.

7. Summary and Resources

In August 2011, Visa announced plans to accelerate the United States' migration to EMV payment technology and mobile payments. This announcement significantly changed the payments landscape in the United States from a future of magnetic stripe payments to one of EMV contact and contactless and mobile payments. Moving to EMV will significantly reduce fraud, has potential to make CNP transactions secure, and will make U.S. payments interoperable with most of the rest of the world. Because of lower costs of terminals and cards, as well as Visa's TIP program, migrating to EMV will be easier and less costly than it was even a few years ago.

Stakeholders interested in learning more about EMV and EMV migration are encouraged to review the EMVCo website at http://www.emvco.com, and review the Smart Card Alliance's U.S. EMV Roadmap white paper, located at http://www.smartcardalliance.org/pages/publications-card-payments-roadmap-in-the-us.

References

[EMVCO2011] EMVCo, May 2011, A Guide to EMV, http://www.emvco.com/media_center.aspx?id=48

[Gemalto2011] Gemalto Blog, July 2011: UNFCU Wins Big With America's First EMV Program, Jack Jania, http://blog.gemalto.com/blog/2011/07/13/unfcu-wins-big-with-americas-first-emv-program/

[Visa2011] News Release, August 2011: Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments, http://corporate.visa.com/media-center/press-releases/press1142.jsp

[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

Interested in learning more?

To speak with a Gemalto representative please call 888.343.5773 or send a message to Philippe Benitez at philippe.benitez@gemalto.com

Gemalto, Inc.
Arboretum Plaza II
9442 Capital of Texas Highway North, Suite 400
Austin, TX 78759

The world leader in digital security

http://www.gemalto.com

VeriFone
THE WAY TO PAY™

gemalto
security to be free