TSYS® People-Centered Payments

White Paper

U.S. EMV Adoption

Lessons Learned from a Canadian-Based Value Added Resource (VAR)

I. History of EMV – how we got to where we are today and why was a new standard needed?

In 1991, Brussels-based Europay International, which is now part of MasterCard, conducted a European study on the card authentication method that was being driven by the European Council for Payment Systems. The study concluded that the only effective way of addressing the problem of magnetic-stripe card-related fraud was to move toward a chip card or a smart card. In 1992, one of the key members, France, was reaching critical mass in the introduction of chip cards as a way to authenticate payments in the French marketplace. France's project had started back in 1984, when they began testing the technology and came to an agreement as a community that this was the way they wanted to proceed. By 1992, France reached a point where all of the country's point-of-sale (POS) devices and all payment cards had become chip-enabled.

In 1993, EMV was formed, which stands for **E**uropay/**M**asterCard/**V**isa, based on the ascendancy of the alphabet and the fact that smart cards were coming out of the European marketplace, in terms of patents and first use.

In 1994, there was focus on the foundations for a business plan for driving the technical development of a chip or smart card. The first focus was on fraud and counterfeit cards, lost and stolen cards, and trying to mitigate that fraud through the use of the chip. Secondly was to continue to allow the offline authorization or approval of credit cards in an environment where telecommunications costs were rather expensive and people were talking about 30 or 40 cents per call to authorize a credit card transaction. EMV members didn't want to move, like the U.S. and North America had, to a 99 percent authorization rate; they wanted to stay down in the 25 to 40 percent rate that they were used to in the European market. France had reached about 40 percent before they began their migration and had reduced the online authorization rate to about 10 percent when they completed the migration to smart card (chip and PIN – as it is now called). Thirdly was the fact that signature was not an effective cardholder verification method, but to go to an online PIN environment would be a very expensive investment, especially with regard to cross-border transactions, which were rather important to Europay since it was the mainstay of business (international transactions between the various countries

within the European markets). So, they were looking at a way of adding PIN to a credit card without requiring an online authorization. Finally, they looked at value-added multi-application services (the ability to put multiple payment cards on a single piece of plastic, to add loyalty, identity, healthcare, or whatever facilities and services the issuing bank might agree on with its partners).

Since this time, Europay has been purchased by MasterCard. Currently, EMVCo (which is owned by American Express, JCB, MasterCard and Visa) manages, maintains and enhances the EMV Integrated Circuit Card Specifications to ensure global interoperability of chip-based payment cards with acceptance devices including POS terminals and ATMs.

There are an estimated 5 billion magnetic stripe payment cards in use worldwide, with 15 million magnetic stripe POS terminals in the U.S., according to the market research publication The Nilson Report. There is a tremendous amount of existing infrastructure to support payments initiated with magnetic stripe cards. For example, consider the cost to replace these 15 million magnetic stripe POS devices[1], more than 360,000 ATMs[2], 609.8 million credit cards and 520 million debit cards[3]. The cost estimated by Javelin Strategy and Research is about $500 million for ATM upgrades and at least $8 billion to implement EMV. With the international pleas and pressure to bring EMV chip and PIN payments to the U.S. market, it is certain it won't happen overnight. To do so would be comparable to a nationwide replacement of all standard-speed rail service with high-speed trains.

However, the pressure to adopt the EMV standard is very clear in the U.S. As the majority of the world has already adopted EMV or in the process of doing so, the opportunity for fraudulent magnetic stripe transactions to occur in the U.S. is higher than ever before, as crooks move their efforts to the U.S. – where magnetic card acceptance and processing is still very prevalent. Realizing that the U.S. is a very unique entity in terms of the number of payment handling banking institutions (8,000) and the very intertwined and established payment infrastructure revolving around magnetic stripe card processing, it is easy to understand why adoption of EMV has not been embraced as it has in other countries or regions of the world. However, other countries have realized the fraud-preventing advantages of EMV chip cards for some time, as EMV ensures a card is authentic by utilizing encrypted data stored on the card (although it does not encrypt the actual transaction). Additionally, no government mandate to adopt EMV, as has been the case in some countries already utilizing EMV, has also possibly contributed to slow U.S. adoption.

II. What are the advantages to utilizing this standard?

The most significant advantage to utilizing the EMV chip and PIN card standard is an obvious one – that being, reduction in card fraud resulting from counterfeit, lost and stolen cards. The EMV standard also allows interoperability with the larger global payment infrastructure. In other words, consumers with EMV chip payment cards can use their card on any EMV-compatible payment device anywhere they are accepted in the world. EMV also supports greater cardholder verification methods. EMV payment cards, unlike magnetic stripe cards, can also be used to perform secure online payment transactions.

III. What countries are currently playing?

Simply put – the majority of the world, with the exception of the U.S., is utilizing EMV payment cards. As of the first quarter of 2011[4]:

- Canada, Latin America and the Caribbean = 31.2% of cards and 76.5% of terminals
- Asia Pacific = 27.9% of cards and 43.0% of terminals
- Africa and the Middle East = 17.6% of cards and 60.7% of terminals
- Europe Zone 1 (western Europe) = 73.9% of cards and 89.0% of terminals
- Europe Zone 2 (eastern Europe and the Russian Federation) = 12.7% of cards and 65.4% of terminals

IV. Why is the U.S. slow to adopt EMV?

The reluctance to adopt EMV in the U.S. until 2011 has been mostly due to cost. Replacing cards is pegged at nearly $3 billion, and replacing payment terminals will cost merchants more than $2.5 billion collectively. Also, issuers and merchants have not seen a justification for this cost because fraud losses, while increasing, are still a very small percentage of overall revenue. Issuers have not wanted to spend the additional amount per card to produce chip cards since there have been virtually no chip acceptance devices in the U.S. Merchants did not want to invest in chip acceptance devices since there were no chip cards being issued in the U.S. It has been a bit of a Catch-22 scenario. Also, there has been a fear of adopting the technology and investing in hardware when the next and newest devices are always just around the corner, so what was just invested in could be considered obsolete.

V. Where is the U.S. today in relation to EMV?

As one of the last remaining non-EMV markets, the U.S. has been increasingly vulnerable to fraudsters, driving up losses and improving the business case for EMV adoption.

In the U.S., 4.5% of card-present transactions originate from chip terminals, primarily at big box merchant locations like Walmart and Best Buy. In February 2012, Visa announced that U.S. financial institutions have reported issuing an estimated one million Visa-branded, EMV chip-enabled cards as of the end of 2011. It should be noted that there are well over a billion Visa-branded credit cards in the U.S., so this one million EMV chip-enabled number is a very small percentage.

VI. How are the card brands helping to ease the adoption of EMV in the U.S.?

Visa – Key Dates:

- **August 2011 –** Visa announced plans to accelerate chip migration and mobile payment adoption in the U.S. The use of PINs in non-debit transactions is discouraged.
- **October 1, 2012 –** Visa's Technology Innovation Program (TIP) is extended to U.S. merchants. To qualify, merchants must process at least 75% of their Visa transactions on terminals capable of both contact and contactless EMV to support contact and contactless chip.
  - While merchants must still comply with Payment Card Industry (PCI) rules, TIP eliminates the requirement for eligible merchants to annually validate Visa's PCI compliance.
    - There are several qualifiers and criteria for a merchant to receive its benefits.
    - No Safe Harbor and other brands must follow suit in order to be truly effective.
- **April 1, 2013 –** Acquirer processors are required to support merchant acceptance of chip transactions; some infrastructure updates will be required.
- **October 1, 2015 –** Liability will shift to acquirers for domestic and cross-border counterfeit fraud card-present POS transactions if the merchant does not have an EMV-enabled POS device.
- **October 1, 2017 –** Liability shift takes effect for transactions generated from automated fuel dispensers – this allows more transition time to account for higher equipment/pump costs.

MasterCard – Key Dates:

- **February 2012 –** MasterCard will offer incentives to merchants who will favor EMV with PINs at the point of sale. And it will adopt and expand upon the Visa program that offers relief from audit requirements for the PCI data-security standard. In addition to audit relief, the network will offer to reduce, and eventually eliminate, certain costs merchants must bear related to data breaches, provided those merchants have adopted EMV. MasterCard will have "an immediate focus" on working with acquirers to make sure they are ready to support Dynamic Authentication by April 2013, the deadline set out by Visa.
- **October 2012 –** It will reduce by 50% a merchant's liability for card-reissuance and fraud costs in the case of a data breach, if the merchant processes at least 75% of its MasterCard transactions on terminals capable of both contact and contactless EMV.
- **April 2013 –** MasterCard will also work to meet Visa's goal of April 2013 for acquirer processing of EMV transactions. All acquirers and sub-processors (any entity that processes on behalf of an acquirer; for instance if this entity were to contract directly with an acquirer (instead of a merchant), even if they sent the transactions to a processor (and not directly to MasterCard), they would be a sub-processor) must be able to fully process EMV transactions. Also, cross-border Maestro ATM liability shifts to non-EMV ATMs.
- **October 2013 –** Account Data Compromise (ADC) relief takes effective (50%). ADC represents that if the merchant's data is breached, MasterCard is offering shift in liability, depending on whether the merchant has EMV POS devices. The amount of protection depends on the level of EMV supported (chip and signature has less protection than chip and PIN).
- **October 2015 –** ADC relief takes effect (100%) if the merchant is processing at least 95% of its MasterCard transactions on EMV devices. Merchant acquirers' liability hierarchy takes effect (excluding fuel dispensers).
- **October 2017 –** Merchant acquirers' liability hierarchy takes effect at fuel dispensers.
- MasterCard's policy also provides for an indirect incentive for PINs to be used with EMV chip cards for authentication, a topic Visa specifically excluded in its August 2011 release. While MasterCard is not mandating the use of either signatures or PINs, it will introduce what it calls a "liability hierarchy" in which the cost of fraud from lost or stolen cards will fall upon "whichever party adopts the less secure approach."
- To speed up deployment of chip-enabled terminals, MasterCard says the network will provide for "true financial benefits" to merchants who install the devices.

One of the benefits will be relief from PCI assessments, following Visa's policy. Installation and use of the devices is still without Safe Harbor, however. While there may be a reduction in fraud expenses, but there is still the requirement to comply with PCI rules.

Discover – Key Dates:

- **March 15, 2012 –** Announcement that it is implementing a 2013 EMV mandate for acquirers and direct-connect merchants in the U.S., Canada and Mexico.
  Discover will support:
  - All card authentication channels – including online and offline.
  - All cardholder verification methods – including both chip and PIN or chip and signature transactions.
  - All commerce channels – including contact and contactless (including mobile).

VII. In general, what is required by those affected (e.g., acquirers, merchants) for EMV adoption?

The acquiring community, to include acquirers and merchants, will be responsible for the cost of upgrading or replacing their POS devices. The smaller merchants will likely take the lead from their acquirer, but larger merchants will do their own research since they have larger volumes of equipment to consider upgrading or replacing. Whether large or small, all merchants will want to build in the ability to include future upgrades and functions.

Since there is more data sent to the acquirer from an EMV-compliant transaction than a current magnetic stripe transaction, merchants will need to work with their acquirer or processor to accommodate the transaction messaging for EMV-based payments.

Liability shift will occur as well (see VI above). In the current environment, financial institutions bear the liability for fraud, but new policies by VISA and MasterCard will assign liability to acquirers in certain instances. There will need to be clear understanding of who has responsibility for fraud.

VIII. What best practices or lessons learned can be gleaned from Canada's EMV adoption?

Following are some experiences and key considerations from a Canadian VAR's perspective for the acquiring community as EMV migration begins:

Show Merchants the Business Case

The potential elimination of yearly PCI DSS assessments and validation can, in some cases, offset the cost of upgrading to new terminals. For ATM operators, many existing ATMs can be retrofitted with the new card reader and a software upgrade, making the transition less costly than complete replacement. Some newly-manufactured ATMs are already EMV capable (though not activated) in anticipation of EMV adoption. With merchants bearing a share of the multibillion dollar fraud losses in the U.S., the prospect of lower fraud should be a key driver for larger merchants to do their part.

Work with EMV-Experienced Vendors

The acquiring community should start reviewing the offerings of terminal vendors in preparation for EMV migration. Review Visa's terminal requirements to ensure that the vendor's offerings will position the merchant for future elimination of PCI DSS requirements, including NFC-based contactless payments. Look for transaction processors with an EMV solution offering which enables an EMV-compliant terminal.

Watch Developments in Mobile Payments

An example of one card brand's affect on adoption of EMV in the U.S. is Visa's announcement which should spur a dual drive towards EMV and NFC-based mobile payments. Mobile payments include transactions conducted from a mobile phone, but also from other mobile devices, such as tablets. It includes a consumer using the device to enhance or conduct a transaction at the point-of-sale, or a merchant replacing a traditional POS device. All of these possibilities will move closer to mainstream reality as Visa's initiatives take hold, and there will be a necessity to stay abreast of these developments and the vendors who are working on solutions.

Expect Bumps in the Road

Migrating to a new payment infrastructure will not be without its trials. Merchants and their service providers will face technical challenges as they roll out and test new payment terminals and ATMs. The EMV specification will require the POS device/application and host system to undergo more intensive end-to-end testing to accommodate a wider range of possible processing scenarios. In this, too, the acquiring community should look to find counterparts in EMV-experienced countries like Canada, to share their knowledge.

IX. What are some of the pitfalls of EMV? Is it foolproof? Is it the silver bullet?

EMV may be only the first step. With the utmost certainty, criminal elements will find holes in this standard as well. The acquiring industry needs to look for other technologies to ensure that the consumer making the purchase is legitimate and authorized to make the purchase. Out of necessity,

acquirers will make operations more efficient and will need to significantly lower the risk to merchants and acquirers. This may take shape in many forms including the near-term adoption of encryption and tokenization and, in the long term, new techniques like biometric authentication. There always needs to be a layered approach to addressing security and fraud, as EMV alone is not the silver bullet.

Major markets having already deployed EMV are predominately utilizing chip and PIN as the authentication method, as this has proven to be the most secure. With the dynamic authentication feature, the "chip" in the card is the authentication component of the card, and the PIN is the authenticator of the cardholder. Some of the data on the chip changes with each transaction, allowing the issuer to confirm that the card is authentic.

One transaction type that is not covered from an EMV security standpoint is card-not-present (CNP) transactions. Statistics from the U.K. and other EMV-enabled countries prove that fraudsters go the route of least resistance – that being CNP Internet transactions and mail or telephone orders. There are some workarounds to thwarting this type of EMV CNP fraud, like utilizing a small EMV-compliant card reader in the hands of the individual consumer to authenticate the card for online purchases or banking. This is not widely implemented due to the resistance in cost to the consumer, which is generally under $50. There are other types of workarounds like protocols such as Visa's "Verified by VISA" and MasterCard's "Secure Code" which ties the financial authorization process with an online authentication like a password that is verified by the issuing bank. The cost to the merchant to implement these services can be significant; thus, adoption has been low. Visa has recently announced its "V.me" online payment process, which from a consumer standpoint provides an extra layer of security by storing credit card information with Visa and not with the merchant. A participating merchant will only require an email address and password during the online checkout process.

X. Summary

When, and not if, the U.S. migrates to the EMV chip-based payment standard, which, from a processor's standpoint is known to be April 1, 2013 (these entities must be able to fully process EMV transactions), it will essentially put the world on a single global standard for fraud protection. This will allow all players in the payments value chain to focus their resources on revenue generation versus allocating contingencies for fraud losses by shifting the percentage, but not completely eliminating it.

The fact that there has not been a U.S. government mandate for conversion to the EMV standard is one of many reasons why the U.S. may have not moved more quickly. In Canada, the Interac Association (a non-profit organization that links proprietary networks and is the only debit network in Canada) set forth migration dates for cards and terminals, which is thought to be one of the catalysts for their adoption of EMV. While there is a strong belief that the U.S. payments industry can institute the EMV standard on its own, if the process doesn't go smoothly, it just might need an "act of Congress" and possibly regulatory oversight to move the process along at an expedited rate. In some countries that have transitioned to EMV, government — not industry — has mandated the change. Whether or not one believes government intervention is a good thing, it could nonetheless happen. However, as long as the industry works together towards the common goal of adding a proven fraud-prevention technology to the U.S. payments industry, intervention should not be necessary.

SOURCES

[1] The Nilson Report

[2] ATM & Debit News says there were 360,659 ATMS in service in 2007

[3] Ben Woolsey and Matt Schulz, "Credit Card Statistics, Industry Facts, Debt Statistics" http://www.creditcards.com/credit-card-industry-facts-personal-debt-statistics-1276.php

[4] Figures reported as of Q1 2011 and represent the latest statistics from EMVCo, as reported by their member financial institutions globally.

TO LEARN MORE

+1.480.333.7878 or acq-sales@tsys.com. You can also visit us at www.tsysacquiring.com.

GET TO KNOW TSYS

AFRICA	ASIA-PACIFIC	COMMONWEALTH OF INDEPENDENT STATES	EUROPE	INDIA & SOUTH ASIA	JAPAN	MIDDLE EAST	NORTH & CENTRAL AMERICA, MEXICO & THE CARIBBEAN	SOUTH AMERICA
+27 21 5566392	+603 2173 6800	+7 495 287 3800	+44 (0) 1904 562000	+911204191000	+81 3 6418 3420	+971 (4) 391 2823	+1.706.649.2307	+55.11.3504 6600