Testimony of Randy Vanderhoof

Executive Director, Smart Card Alliance

Before the Committee on Science, Space and Technology, Subcommittees on Oversight and Research & Technology

"Can Technology Protect Americans From International Cybercriminals"

March 4, 2014

On behalf of the Smart Card Alliance and its members, I thank you for the opportunity to testify today. We applaud the Subcommittees' leadership and foresight in examining important issues in the payments industry, especially on increasing instances of international cybercriminals committing payment data breaches and the role of EMV chip payment technology to help secure the U.S. payments infrastructure.

The Smart Card Alliance is a non-profit organization established in 2001 that provides education about smart card chip technology and applications and operates a collaborative, open forum among leaders in various industries including payments, mobile, transportation, government, healthcare, and access security. The Alliance's members from the payment ecosystem include payment brands, card issuers, payment processors, merchants and technology providers.

Shortly after the four major payments brands, American Express, Discover, MasterCard and Visa, announced incentives to introduce secure EMV chip cards for the U.S. market and aligned timelines for fraud liability shift dates in 2015 and 2017, the Smart Card Alliance organized a new payments-only industry association, the EMV Migration Forum. The Forum was formed specifically to address issues that require broad cooperation and coordination across many constituents in the payments space to ensure the successful adoption of EMV-enabled cards, devices, and terminals across the U.S. market, and to ensure that migration in the U.S. market is efficient, timely and effective. The Forum has more than 150 members companies, including global payments brands, financial institutions, merchants, processors, acquirers, regional debit networks, industry associations and industry suppliers.

The Smart Card Alliance and the EMV Migration Forum have been the leading advocates for accelerating the adoption of secure payments technology to address the growing fraud problem in the United States and to ensure citizens traveling outside of the U.S. will have a safe and convenient payments experience.

The focus of my testimony will be on the state of payment card technology and the payments acceptance ecosystem, including differences between the magnetic stripe cards used in the U.S. and EMV chip cards used in more than 80 countries, the status of U.S. migration to EMV chip cards, and the benefits for the U.S. moving to EMV chip cards to increase security, reduce counterfeit card fraud, and reduce the likelihood of future data breaches by devaluing the payments data that is present in the retail and financial systems.

Increasing Instances of Cybercrime in the U.S. Highlight Need for EMV Chip Cards

Cybercrime targeting government and commercial enterprises is a growing problem in the U.S. In 2013, data breaches became more damaging, with one in three people who received a data breach notification letter becoming an identity fraud victim, up from one in four in 2012[1].

While cybercrime is a known threat across many industries, criminals are increasingly targeting retail store chains with sophisticated attacks in order to extract credit card data from millions of transactions. Attacks against retailers are particularly damaging because of their effects on large numbers of consumers, banks and merchants at the same time. The results of a single attack, which we saw most recently with retailer Target, can be millions of dollars' worth of credit card fraud and the need to close and reissue tens of millions of payment card accounts to prevent further fraud. There are also other unquantified costs of payment data breaches, including the time and money to investigate and clean up after the breach, lost business and damaged reputations for the merchants and banks involved.

The opportunity for huge financial gains with little chance of criminal prosecution from these stolen card accounts also provides the incentive for hackers to penetrate deeper into compromised networks to extract additional personal information beyond payments data, including email addresses and phone numbers, putting consumers' privacy at further risk.

Increasing instances of attacks against retailers are due in part to the fact that U.S. magnetic stripe payment card information is highly valuable data for hackers, who can sell it on the black market to criminals for large profits. For example, the black market price for several million card accounts stolen from the Target breach was between $26.60 and $44.80 each prior to Dec. 19, 2013[2].

Criminals are willing to pay such high prices for U.S. magnetic stripe card data because of the ease with which that data can be used to create counterfeit payment cards for fraud. It's very simple to write stolen magnetic stripe payment card information to a different magnetic stripe payment card. This is why the U.S. is the only region where counterfeit card fraud continues to grow. The U.S. accounted for

[1] Javelin Strategy & Research, "2014 IDENTITY FRAUD REPORT: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends," February 2014.

[2] Krebs, Brian. "Fire Sale on Cards Stolen in Target Breach." *Krebs on Security*. Web. 26 Feb. 2014. <http://krebsonsecurity.com/2014/02/fire-sale-on-cards-stolen-in-target-breach/>.

47.3% of global fraud losses in 2012, despite only accounting for 23.5% of the total transactions, and U.S. issuer losses due to counterfeiting account for 26.5% of global fraud losses[3].

The financial industry has very strict data security standards, called the Payment Card Industry Data Security Standard (PCI DSS), in place to protect payments data and other sensitive personal information captured and stored by retail systems and processors. These standards and best practices are effective deterrents against a lot of criminal activity, but not enough for increasingly sophisticated criminals and attacks. Additional security measures are needed and are already used globally including EMV chip cards, advanced encryption technologies and tokenization.

EMV chip cards in particular can reduce the threat of financial cybercrime by removing the economic incentive for criminals. Replacing magnetic stripe payment data with secure EMV chip payment data devalues U.S. payment data in the eyes of criminals because, if stolen, EMV chip payment data cannot be used to create counterfeit payment cards.

The positive news is that the U.S. payments system is undertaking a migration to EMV chip card technology, and this will present significant barriers for criminals engaging in payment card counterfeiting. Although the U.S. payments system is complex, the industry has recognized the need to move as quickly as possible to EMV chip card payments. I am encouraged by the movement and progress from all industry stakeholders towards implementation of the technology.

Next, I will explain EMV chip card technology and why it is secure, how it can help to address mounting U.S. payment data security problems, and what the current status of U.S. EMV migration is.

Introduction to EMV Chip Payment Technology

EMV chip payment cards are based on widely used and highly secure smart card technology, also referred to as “smart chip” technology. Smart cards – which can look like a card but can also take on different forms – have embedded integrated circuit chips, powerful minicomputers that can be programmed for different applications. Through the chip, the smart card can store and access data and applications securely, and exchange data securely with readers and other systems. Smart cards are ideal for many applications, especially payments, because they provide high levels of security and privacy protection, are easily carried, and do not require their own power source to operate effectively.

Figure 1: EMV chip card

Smart cards are currently used to secure many applications worldwide, including:

[3] "Global Credit, Debit, and Prepaid Card Fraud Losses Reach $11.27 Billion in 2012.” The Nilson Report, Web. 27 Feb. 2014.

- Identity applications including employee ID badges for physical access to buildings and secure computer and network access; citizen ID documents; electronic passports; driver's licenses; and online authentication devices. Today, smart card technology is used by all U.S. federal employees and contractors with Personal Identity Verification (PIV) credentials to secure access to government systems and buildings; in U.S. citizens' passports to secure identity information; and in federal programs like the TSA First Responder Authentication Credential (FRAC), the TSA Transportation Worker Identification Credential (TWIC) and the Department of Defense Common Access Card (CAC)

- Healthcare applications including citizen health ID cards; health provider ID cards; portable medical records cards. Smart card technology is now being recommended in legislation to create a pilot for a proposed Medicare Common Access Card (H.R. 3024)

- Mobile applications including billions of mobile phone subscriber identity modules (SIMs) in use today, plus in NFC-enabled phones to secure mobile wallets

- And lastly, with global payment standard EMV chip cards, now used in more than 80 countries worldwide with 1.6 billion payments cards issued to date, and the focus of this testimony

EMV: A Global Perspective

It was growing counterfeit card fraud that originally led the global payments industry to move to smart chip technology for bank cards and to develop the global EMV standard for bank cards based on chip card technology. The EMV specification, first available in 1996 and managed by EMVCo, defines the global interoperable standard for smart chip-based bank cards.

Financial institutions in Europe, Latin America, Asia/Pacific and Canada are issuing EMV chip cards for credit and debit payment or migrating to EMV issuance. According to EMVCo, approximately 1.6 billion EMV cards have been issued globally and 24 million point of sale (POS) terminals accept EMV cards as of Q4 2012. This represents 44.7% of the total payment cards in circulation and 76.4% of the POS terminals installed globally[4].

There have been a number of historical factors behind the adoption of EMV chip technology in these other countries. The most important factors have been high fraud rates and the cost and reliability of the communications infrastructure. In markets in Western Europe, Australia, Latin America, and Canada the rate of credit card fraud had been much worse than what the U.S. market has historically experienced. These higher fraud rates, plus the lack of low cost, reliable communications at the retail level, led countries to adopt EMV chip technology to enable greater security at the card and offline payments processing at the terminal level. Each of these markets are smaller than the U.S. market, with fewer financial institutions and merchants to convert to chip technology, so the business case to make

[4] "Latest EMVCo Figures Reveal Continued Market Adoption of EMV Technology." EMVCo, Web. May 2012.

the investment in EMV has been very strong. Countries that have implemented EMV chip technology have seen their counterfeit fraud decline by as much as 67%[5].

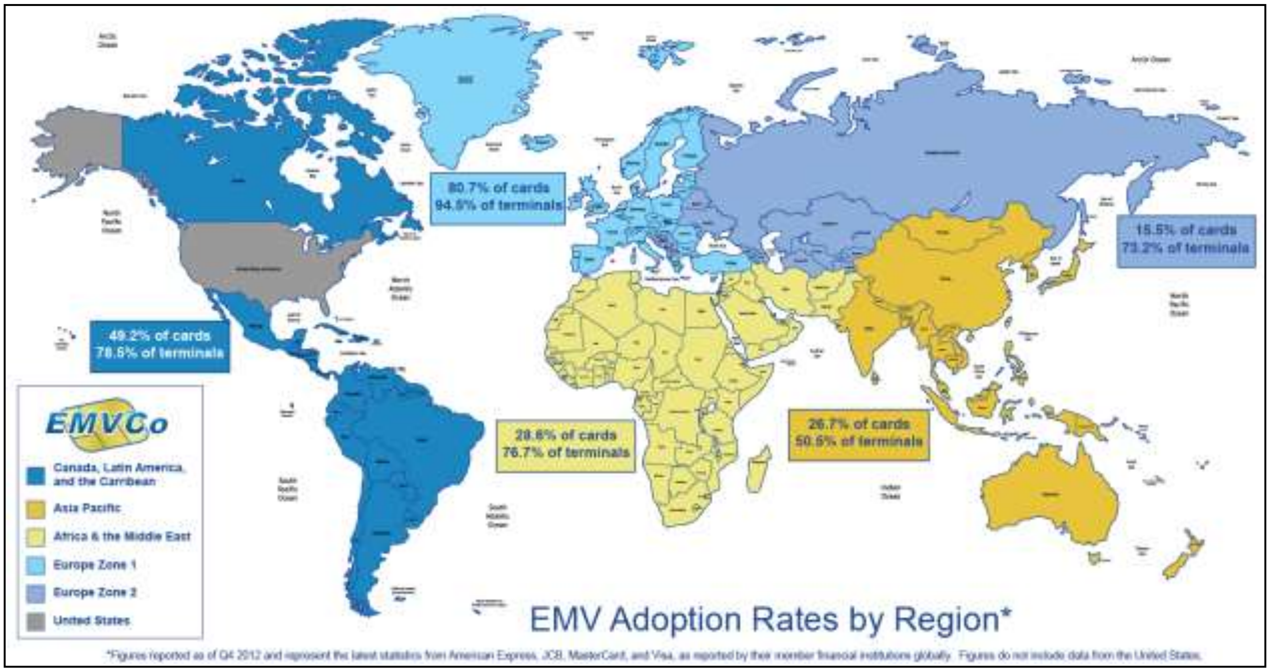
80.7% of cards
94.5% of terminals
15.5% of cards
73.2% of terminals
49.2% of cards
78.5% of terminals
28.6% of cards
76.7% of terminals
26.7% of cards
50.5% of terminals
EMVCo
Canada, Latin America, and the Carribean
Asia Pacific
Africa & the Middle East
Europe Zone 1
Europe Zone 2
United States
EMV Adoption Rates by Region*
*Figures reported as of Q4 2012 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.

Figure 2: EMVCo map, "EMV Adoption Rates by Region"
http://www.emvco.com/documents/EMVCo_WorldMap2.png

The U.S. is one of the last countries to move to EMV chip technology, but has now started its migration. Between July 2011 and June 2012, American Express, Discover, MasterCard and Visa announced plans for moving the U.S. to an EMV-based payments infrastructure. The plans included a series of incentives and policy changes aligning around a target date of October 2015 for card issuers and merchants to complete their implementation of EMV chip cards, terminals and processing systems. ATM operators and retail petroleum outlets were given until 2016 and 2017, respectively, to complete their EMV migrations.

It is important to note that the target dates are not mandates, as U.S. payment brands do not have the ability to set requirements. What they can, and did, was mandate payments processors who connect through their global networks to support EMV chip data in transactions by April 1, 2013. This is the only mandate for U.S. EMV chip implementation.

The payment brands have offered card-issuing financial institutions and merchants an incentive to move to EMV chip technology in the form of a counterfeit fraud liability shift. After the target EMV chip migration dates, the payment brands will shift the responsibility for any fraud resulting from a payment

[5] "Fraud: The Facts." UK Cards Association, Web. 2012.

transaction to the party using the least secure technology. This may be either the issuer of the card or the merchant accepting the payment card.

As an example, if a merchant can accept EMV chip cards and the cardholder presents a magnetic stripe card and there is fraud, the issuer would bear the liability for fraud. Conversely, if a cardholder presents an EMV chip card for payment and the merchant only accepts magnetic stripe cards, the merchant would be liable for any fraud. If both parties have deployed EMV and fraud results from that transaction, the current rules for fraud liability are applied.

This fraud liability shift ensures that those who have made the investment in EMV chip technology will not bear responsibility or cost from fraud from another stakeholder who has not made their system more secure. The goal of the liability shift is to encourage both issuers and merchants to move to EMV technology at the same time so that fraud is removed from the system, not shifted from one party to another.

Status of U.S. EMV Migration

The U.S. payments industry is approximately two years into the planned four-year migration to adopt EMV chip technology. Industry stakeholders have been meeting regularly at Smart Card Alliance conferences and EMV Migration Forum meetings and within other industry organizations to address issues that require coordination and cooperation among multiple payments industry participants to ensure a timely and cost effective industry-wide migration to chip technology in the U.S.

The migration to chip cards in the U.S. is complex, expensive and difficult to coordinate. The U.S. market is the largest individual market to convert to chip cards. With over 12,000 financial institutions that issue cards, an estimated 1.2 billion cards in the market, over 10 million POS devices in retail stores, and another 100,000 ATMs installed, the United States payments market is larger than all of Europe's payments markets combined. To date, an estimated 10 to 15 million chip cards have been issued to U.S. consumers, mostly to those who travel frequently outside of the U.S. and who benefit from having the same chip cards that are used in those countries' retail outlets and ATMs. This progress represents less than 2% of the total number of cards in the market. Retailers have replaced approximately 1 million of the more than 10 million POS terminals in stores, but nearly all of these are still operating only as magnetic stripe accepting devices until the software is tested and certified by the acquirers and the stores are ready to begin accepting chip cards.

Implementing EMV chip technology for U.S. debit is also very complex. Complexities result from having 19 debit networks for PIN debit card transactions and the need for compliance with the 2011 Federal Reserve Rulemaking, "Regulation II, Debit Card Interchange Fees and Routing[6]," interpretation of the Durbin Amendment under the Dodd Frank Act. The rulemaking requires that there be at least two unrelated debit card networks supported on each card issued and that merchants have the option to decide which network to route those transactions to each time a debit card is used.

[6] "Regulation II (Debit Card Interchange Fees and Routing)." Federal Reserve System. Web, July 2012.

Accommodating these debit routing rules through agreements among all of the debit networks and the global brands, as well as determining the impact of recent court decisions challenging the Federal Reserve rules, have created uncertainty among issuers and merchants about how to implement EMV chip technology for debit transactions. Today the industry is working on ways to comply with the current rules and still be able to accommodate potential changes that may result from further decisions by the courts, and progress has been made.

How EMV Chip Cards Prevent Counterfeit Card Fraud

Chip technology in conjunction with the global EMV payments application standard has proven to be the most effective tool to prevent counterfeit card fraud and maintain the requirements for global interoperability of payment cards for issuers, merchants and consumers. The counterfeit fraud protection comes from two aspects of this technology:

1. The secure storage of the cardholder data inside the chip rather than on a magnetic stripe
2. The dynamic payment transaction data generated by the chip when it is presented to the payment reader for processing the card in a physical retail setting.

The chip itself is a powerful microcomputer with active defenses that prevent tampering with the application and the information it stores inside its memory. Even if chip data were to be copied, it could not be used to create a usable copy onto another chip card because each chip is programmed with a secret key known only to the issuer. The less secure magnetic stripe has no defenses to prevent a criminal from reading the stripe and reprogramming that same card data onto another magnetic stripe, creating an undetectable copy of the original card.

Chip-enabled terminals in retail stores are programmed to pass dynamic security information to the chip before the chip will pass the uniquely generated cryptographic electronic signature to the terminal to complete a payment transaction. This feature is the first line of defense against the use of counterfeit cards that is possible today with magnetic stripe cards.

Figure 3: Chip-enabled POS terminal with an EMV chip card inserted

The chip generates a one time, unique security code, called a cryptogram, for each chip payment transaction that is passed through the chip terminal and through the retailer's POS system and payments processing network. The security cryptogram is verified by the issuer processor to determine that the card used to start the transaction is authentic and that the transaction data was unique to that card. Therefore, a counterfeit copy of that card or a second transaction with the same unique card data would be detected by the issuer and the message normally sent back to the retailer to complete the transaction would deny the transaction.

In addition, EMV chip transactions do not include other data needed for magnetic stripe transactions. This means that any stolen data cannot be used to create a fraudulent transaction in an EMV chip or magnetic stripe environment.

The dynamic data generated by EMV chip cards and the omission of data used in magnetic stripe transactions greatly devalue any payment data that is present in the retailer's or third party processor systems since the chip data cannot be made into counterfeit cards to commit fraud. For example, if EMV chip data had been present in the retailers' systems that were recently victimized by a POS malware attack that extracted card transaction data, the impact of the data breach would have been significantly lessened for the merchant, the card issuers and the consumers through greatly reduced risk of counterfeiting and the resulting card fraud.

The EMV standard also supports additional security mechanisms including the manner with which consumers verify their identities, called Cardholder Verification Methods (CVMs). The EMV standard supports signature, PIN and/or no CVM. Chip-based payment cards that use signature as a CVM have all of the security benefits that the chip and the EMV transaction data provide for protection from counterfeiting and resulting fraud. Chip-based payment cards that use PINs as a CVM provide an added layer of security that prevents the physical card from being used if it is lost or stolen. In the U.S., card issuers will decide which CVMs they want to support based on customer profiles and card management considerations. Merchants can decide which CVMs available on each card they will accept in their retail outlets. As a result, it is likely we will see EMV chip cards issued with a mix of signature, PIN and no CVMs in the U.S.

The issuance of chip cards in the U.S. does not mean the elimination of the magnetic stripe altogether. Financial institutions will continue to issue chip cards with a magnetic stripe on the back for the foreseeable future in order to enable consumers to continue to use these cards at merchant locations that haven't yet upgraded to chip, or in some countries who have not yet adopted the EMV chip standard.

These magnetic stripes that will remain on the backs of bank-issued EMV chip cards do not pose a fraud threat to card issuers or consumers when chip-enabled merchant terminals are widely deployed. When issued on a chip card, a magnetic stripe has different information stored, so when swiped at an EMV chip-accepting terminal, it signals to the terminal that the card was issued with a chip. The terminal will then force the card to be used as a more secure chip card rather than as a less secure magnetic stripe card at that device.

Another scenario is where that chip card's magnetic stripe is copied and a card is created with that card's data written to another magnetic stripe on an unauthorized second card. When that counterfeit card is swiped at a merchant terminal that can process a chip transaction, the terminal would also direct the customer to use the chip. Because the chip doesn't exist on this counterfeit card, the transaction will be declined. If the counterfeit card is used at a terminal that does not support a chip, the card would be accepted unless the issuer flags the transaction based on certain usage analytics or if the cardholder reported the card lost or stolen.

After the fraud liability shift date, if the copied card made with the magnetic stripe data of a chip card is used at a terminal that does not support a chip, and the card is accepted even though it is a copy, the merchant would be responsible for that fraud because it did not have the more secure EMV chip handling capability that would have detected the card was a counterfeit. This is the reason for the liability shift discussed earlier; it's important for both the issuance and acceptance infrastructures to move to chip at the same time to provide the most protection from counterfeit card fraud.

In a third scenario where chip payment card data is intercepted and used to make an online purchase, there are additional security measures that online merchants use, including the three or four digit card security code printed on the card (and which is not available from either the magnetic stripe or the chip), the cardholder's billing address information, or both. Online purchases where the EMV chip is not used in the payment transaction, called Card-Not-Present (CNP) transactions, are not protected by the issuance of EMV chip cards. However, there are other ways to manage CNP fraud risk that are being used today and new technologies that are being developed to address this problem.

To summarize, the security features that EMV chip cards provide to the market in conjunction with the chip reading terminals and advanced payments processing upgrades to support dynamic data are a powerful set of tools to take counterfeit fraud out of the payments system. These security features reduce the likelihood of, or the resulting damage from, any future data breaches against retailers, processors and financial institutions.

Conclusion

In summary, the U.S. reliance on magnetic stripe payment cards has made the country a target for fraud. Evidence to support this are: the increasing attacks on U.S. retailers, of which the FBI found at least 22 instances in the past year[7], and the fact that the U.S. is the only region where counterfeit card fraud rises consistently. Hackers are motivated by the big profits that they can make from selling U.S. magnetic stripe payment data on the black market to criminals to make and use counterfeit magnetic stripe cards.

Joining more than 80 countries and implementing EMV chip technology will greatly devalue U.S. payment card data in the eyes of criminals because it cannot be used to create counterfeit chip or magnetic stripe cards. Other countries that implemented EMV chip payments saw fraud decrease by as much as 67%.

While the move to EMV chip payments in the U.S. is a complex and expensive undertaking, it is a critical one that will benefit our entire payments system. I am encouraged by the payments industry's recognition that we need to move EMV chip technology. I am even more encouraged by the fact that many of the largest financial institutions are now issuing EMV chip cards and big retail chains are moving

[7] "Recent Cyber Intrusion Events Directed Toward Retail Firms." FBI Cyber Division. Web, 17 Jan. 2014.

quickly to put in place the chip-enabled terminals and working with their acquirer processors to enable those devices to begin accepting chip transactions by the October 2015 targeted completion dates.

Contact Information:

Randy Vanderhoof
Executive Director
Smart Card Alliance
191 Clarksville Road
Princeton Junction, NJ 08550
www.smartcardalliance.org
609-587-4208
rvanderhoof@smartcardalliance.org

Randy Vanderhoof, Director
EMV Migration Forum
www.emv-connection.com/emv-migration-forum/

Appendix 1: About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Alliance invests heavily in education on the appropriate uses of technology for identification, payment and other applications and strongly advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart card technology, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.

The Alliance is comprised of more than 220 member companies worldwide, including participants from financial, government, enterprise, transportation, mobile telecommunications, healthcare and retail industries. A mix of issuers and adopters of smart card technology work in concert with leading industry suppliers of the full range of products and services supporting the implementation of smart-card based systems for secure payments, identification, access and mobile communications.

The four main priorities of the Alliance are:

- To influence standards that are relevant to smart card adoption and implementation;
- To maintain a voice in public policy that affects smart card adoption and implementation;
- To serve as an educational resource to its members and the industry; and
- To provide a forum for cutting edge discussions and projects on issues surrounding smart cards.

Within the Smart Card Alliance organization, members have addressed the market requirements and technical applications for smart cards in specific industry verticals by forming industry councils. Six active councils in 2013 each worked from a specific charter and mission statement. Over 500 individuals from 127 organizations supported these councils, with many participating in more than one council. The Identity Council, Access Control Council, and Health and Human Services Council attend to the identity management and security uses of smart cards including security badges, digital log in credentials, and approaches to secure networks and Internet services. The Payments and Transportation Councils serve the payments markets for bank cards, prepaid cards, and transit fare payment systems. The Mobile and NFC Council has the most cross-industry role, since mobile technology and NFC are affecting payments, identity and access applications across many new mobile platforms.

Smart Card Alliance

Appendix 2: About the EMV Migration Forum

Launched in August 2012, the EMV Migration Forum – a cross-industry organization that is separate but affiliated with the Smart Card Alliance – focuses on supporting the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants and consumers to help ensure a successful introduction of more secure EMV chip technology in the United States. The Forum mission is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States. By establishing a professional, collaborative environment for engaged discussion and debate among all industry stakeholders, the organization is harnessing the collective expertise of the U.S. payments industry to guide migration to more secure EMV technology.

The Forum now has more than 150 member organizations, with representatives from all industry stakeholder groups – payment brands, issuers, acquirer processors, merchants, debit networks and industry suppliers.

Over 400 individuals from more than 100 member organizations are involved in the Forum's six Working Committees, which are chaired by industry leaders and meet via regular conference calls and at in person member meetings.

In 2013, Forum members met a total of nine times in person, from two-day all-member conferences to one-day in-person Working Committee meetings. Each participating organization sends it top payments experts and managers to share information and collaborate on creative solutions to the challenges ahead for the U.S. migration to EMV.

The Forum has been successful in dealing with such challenging issues as EMV debit routing, certification testing, and changes impacting ATM operators, merchants, and card issuers in a congenial, courteous and professional environment for the benefit of all involved.

EMV®
Migration Forum

Appendix 3: References/Resources

"Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?," Smart Card Alliance Payments Council white paper, January 2013, http://www.emv-connection.com/card-payments-roadmap-in-the-u-s-how-will-emv-impact-the-future-payments-infrastructure/

Card-Not-Present Fraud: A Primer on Trends and Transaction Authentication Processes, Smart Card Alliance Payments Council white paper, February 2014, http://www.emv-connection.com/card-not-present-fraud-a-primer-on-trends-and-transaction-authentication-processes/

EMV Connection web site, http://www.emv-connection.com

"The EMV Ecosystem: An Interactive Experience for the Payments Community," Smart Card Alliance resource, February 2013, http://www.emv-connection.com/the-emv-ecosystem-an-interactive-experience-for-the-payments-community/

EMV Frequently Asked Questions, Smart Card Alliance publication, http://www.emv-connection.com/emv-faq/

"EMV 101: Fundamentals of EMV Chip Payment," EMV Migration Forum webinar, January 2014

"EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community," EMV Migration Forum white paper, July 2013

"Large Scale Payment Data Breaches Highlight Need for U.S. Card Issuers and Retailers to Move More Quickly to Smart Chip Payment Technology," Smart Card Alliance brief, January 2014

Smart Card Alliance web site, http://www.smartcardalliance.org

"Standardization of Terminology," EMV Migration Forum publication, February 2014, http://www.emv-connection.com/standardization-of-terminology/