First Annapolis

CSCU
CARD SERVICES FOR CREDIT UNIONS

EMV: Background and Implications for Credit Unions

November 2012

TABLE OF CONTENTS

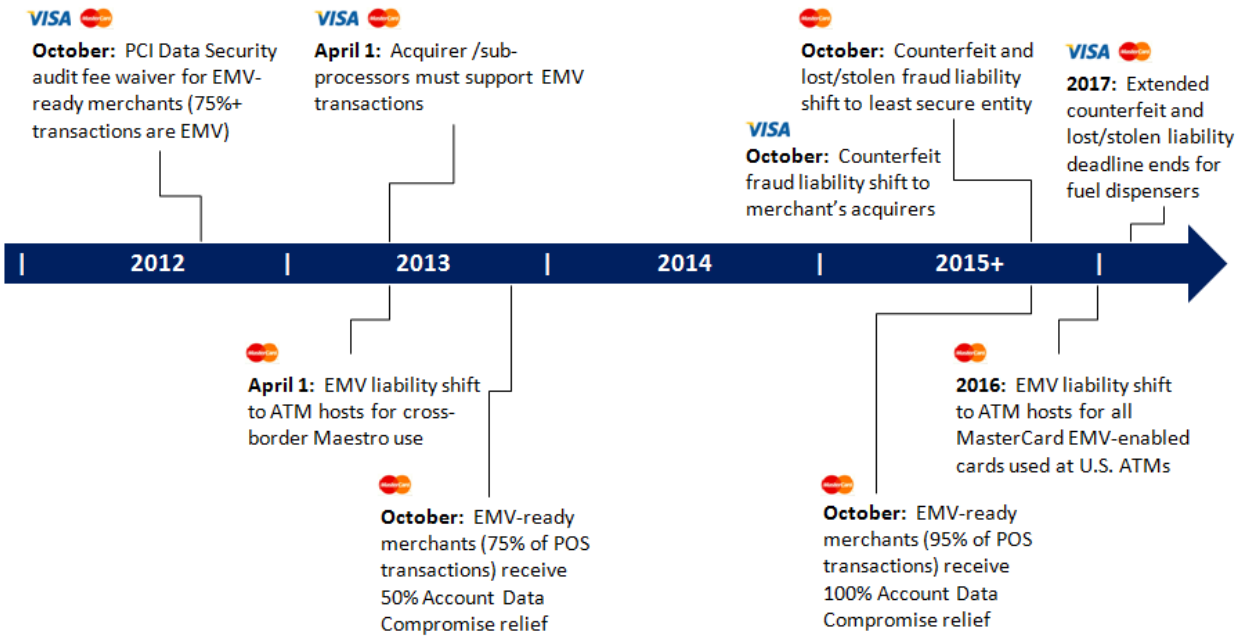
EXECUTIVE SUMMARY

EMV is payment card industry standard developed by Europay, MasterCard and Visa that utilizes integrated circuit chip technology to reduce counterfeit fraud in a card present environment. EMV was developed in the 1990s to improve the security of card transactions. The United States is the last major card market to begin adopting EMV. Converting an entire market of cards and terminals, in addition to ensuring that the necessary back-office, processing, and customer service changes are in place, is a significant undertaking. The payment networks have described a conversion timeline, or set of guidelines that include a timetable for EMV adoption.

Whereas mag-stripe cards transmit a 'static' or constant CVV/CVC value each time it is swiped at a POS terminal, EMV chip cards generate a 'dynamic' or a different value each time it is presented at an EMV-enabled POS terminal. When mag-stripe card account information is compromised as a result of data breaches, skimming or phishing, the compromised information can be used to make counterfeit cards ultimately leading to fraudulent transactions. Conversely, the dynamic nature of EMV chip makes them more difficult to counterfeit, thus reducing fraud in card-present transactions.

Credit union executives should keep in mind that counterfeit fraud is one of the largest components of total card fraud (40% by some estimates). While EMV is a solution to address counterfeit fraud, it does not address fraud from other sources such as phishing or card-not-present. In order for EMV to be effective at reducing counterfeit card present fraud, all stakeholders, issuers and their cards, merchants and their terminals, processors and their authorization systems, must be EMV-compliant. Some of the major card brands have developed migration timelines and incentives for issuers, merchants and processors to become EMV-compliant. The first key date is October 1, 2015; at that time if an EMV- enabled card is presented at a non-EMV-enabled POS terminal, then any fraud resulting from a counterfeit card transaction will be the responsibility of the merchant. This liability shift applies to all card-present transactions with the exception of transactions at automated fuel dispensers, which have a liability shift date of October 1, 2017.

Figure 1: Visa and MasterCard EMV Timeline



Source: payment network press releases

While the adoption roadmap has been defined, there are still a number of unresolved questions concerning the EMV migration. First is how transactions on EMV cards will be verified, which could occur via PIN, signature, or both. The payment networks have slightly different preferences on this topic and a standard has yet to emerge. Another key decision will be whether or not EMV deployments will be for contact, contactless transactions, or both. Regardless of the outcome, the transaction experience for consumers will change as a result of EMV; the card will either be inserted into a reader instead of being swiped or tapped to pay with contactless depending on individual cards and the terminal's capabilities.

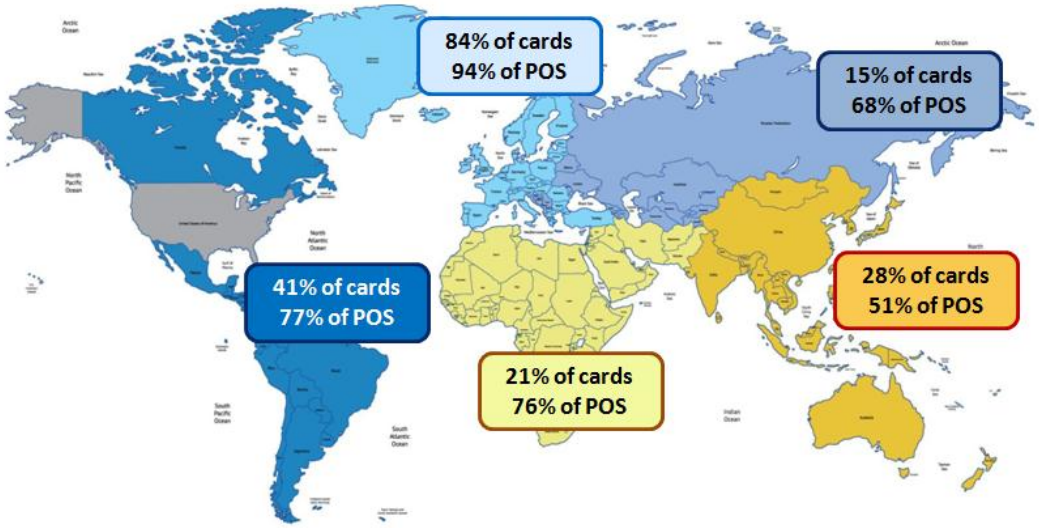
Credit unions will have several implications to consider as they begin their EMV planning process. In addition to deciding to verify by PIN vs. signature and whether to issue contact, contactless cards, or both, credit unions will have to determine when and how to re-issue payment cards and for whom. An important consideration will be the characteristics of their payment card portfolios (credit, debit, prepaid) and the needs of their members, specifically international travelers and affluent segments. This includes the level of fraud, where transactions occur (by geography and sales channel), and the types of fraud incurred. The EMV capabilities and experience of the credit union's processor and other service providers will also be a key consideration, as the conversion process will be a joint effort. Credit unions will have options on when and how to convert. This decision process will require managers to weigh incremental costs against the benefits of EMV. Some may opt to convert their entire portfolio before the liability shift, or wait until after 2015. For all credit unions, a complete understanding of the dynamics of EMV is paramount for success.

CSCU and First Annapolis jointly authored this paper to help explain what EMV is, the timeline and roadmap for conversion, and how EMV impacts the industry and credit unions. The whitepaper will be updated periodically as developments occur.

INTRODUCTION

Earlier this year, the major payment networks announced that the U.S. would join the rest of the major card markets around the world and begin adopting EMV, or "Europay, MasterCard, Visa," a global card standard meant to improve the security of payments over the next several years, with a transition roadmap that includes a fraud liability shift set for October 1, 2015.

Figure 2: Global EMV Deployment of Cards and Physical POS Terminals*



*Cards include credit, debit and ATM
Sources: EMVCo, First Annapolis Consulting analysis

The primary objective for EMV is to create a more secure environment for card payments transactions in the physical environment, which represents over $3.5 trillion in consumer retail sales in the U.S. per year. Another goal is to lay the groundwork for greater mobile payments adoption based on near field communications technology (NFC). Contactless EMV/Chip cards and smartphones would utilize NFC to execute payments. Thanks to the proliferation of smartphones, which now represent almost half of all handsets in the U.S., mobile has emerged as a new channel that financial institutions, retailers, and other payments constituents are utilizing to enable payments and account management, deliver offers, build loyalty, and interact with customers and members on a deeper level.

EMV and mobile enablement both require planning on the part of financial institutions. The purpose of this whitepaper is to provide credit unions with a better understanding of the EMV roadmap. In addition, the whitepaper will address the implications of EMV to credit unions, present options for response, and outline potential actions that credit union managers can take to prepare.

EMV OVERVIEW

EMV is a global card standard launched in the 1990's by the payment card networks to improve card transaction security and global interoperability. This year, the major networks announced similar roadmaps that provide a guide to the industry on how to adopt the technology in the U.S. over the next few years. EMV differs from mag-stripe in several important ways:

1. Data Storage and Card Authentication/Encryption: Information is kept on the integrated circuit, or secure chip on the card. To date, copying data from the chip to a fraudulent card has been difficult for fraudsters in major card markets that have adopted EMV. Mag-stripe data can be copied to counterfeit plastics if the potential fraudster has access to the physical plastic through skimming. Payment account numbers can be copied through phishing or from data compromises. Once a copy is made, the POS reader cannot differentiate between the counterfeit and the original card, and fraud prevention relies on back-end functionality or shutting down the account. With EMV, the card credentials are accompanied by a dynamic cryptogram that verifies the card and the transaction details.

2. Interaction with the POS: With EMV, cards are inserted into a reader or tapped at a contactless terminal instead of being swiped. Regardless of whether contactless becomes part of EMV adoption or if consumers choose to use it, the payment process for the consumer will change slightly. In a contact EMV transaction, the consumer would give the card to the employee at the POS to briefly be inserted into the reader, or do so themselves. Once EMV reaches full adoption, swiped mag-stripe transactions will decrease in frequency, though they will still occur in some circumstances. The form of the payment product may also change. EMV-enabled plastics can be contact, contactless, and/or utilize NFC technology.

3. Cardholder Verification: Transactions can be completed or verified via signature, (as is the case in the U.S., most Asian and Latin markets) but most EMV implementations involve the use of a PIN that is entered for credit or debit transactions (as is the case in most European markets and Canada). This will differ from the mag-stripe environment today, where after a card is swiped, the authentication method depends on the type of card product, and not the underlying technology.

This section will outline the details of the proposed timeline, examine fraud in the U.S. today, evaluate lessons learned from other countries that implemented EMV, discuss the impact of EMV on the payments value chain, the implications for credit unions, and recommendations for response.

Background and Technology

EMV was designed to improve security over the standard mag-stripe card. Mag-stripe cards transmit "static" or the same credential with each authorization. If mag-stripe information is compromised, it is relatively easy for fraudsters to create counterfeit cards. Conversely, EMV utilizes an integrated circuit (IC), or chip, to generate dynamic data, or changing cryptograms that are unique each time the card is used to authorize a transaction and decrypted by an EMV-enabled POS terminal. Dynamic cryptograms are new to the payments transaction process and do not occur via mag-stripe today. There are several options for implementing EMV technology and the networks have specified these options in their U.S. standards for EMV. The areas below are flexible, allowing credit unions to find the balance between cost and complexity.

1. Cardholder Verification: Cardholders will verify with Chip & Signature, Chip & PIN, or have the option for either, depending on what methods individual issuers support. No Signature Required (NSR) may also be an option for transactions below a certain limit for select merchant categories. Visa has advised issuers that signature is their preferred method because it maintains the cardholder experience status quo for the majority of transactions, but will let issuers decide which to implement and will support either. MasterCard has provided guidance stating that Chip & Signature is considered less secure. Cards without support for an offline PIN will work abroad for most, but not all transactions. An offline PIN may be required for unattended terminals that are not connected to a host-based online authorization environment. This can include independent terminals like those found at kiosks at gas or train stations, or in areas where terminals cannot be connected to a phone line network for other reasons. These transactions will likely make up a limited number of transactions and credit unions should consider the cost and benefits when deciding whether or not to support an offline PIN. Issuers can choose to enable one or more verification methods, but must consider cost and customer experience.

   While issuers could theoretically allow two separate PINs for online and offline transactions, it is likely a better member experience to select a single PIN. No signature required is likely to continue for small-ticket transactions, but it is not clear how this would apply to Chip & PIN cards. Updated standards may be necessary to maintain quicker transactions for small-ticket purchases.

2. Contact and/or Contactless: EMV cards will be contact, or contactless, or both (dual interface). For the foreseeable future, EMV plastics will continue to carry a mag-stripe for non-converted terminal transactions. Regardless, EMV will change the physical payments experience. In a contact EMV transaction, the card is inserted into the reader and then removed, not swiped. Contactless transactions involve tapping the reader within a close proximity to enable the reading of credentials. Dual-interface cards are capable of contact or contactless transactions. In other markets, contact cards have typically been part of the first conversion cycle, with dual-interface cards becoming standard in subsequent card issuance (though this occurred in markets where contactless terminal deployment lagged, which is less likely in the U.S.).

3. Authorizations: Online authorization is the U.S. standard for mag-stripe transactions and will be part of the EMV implementation. Both mag-stripe and EMV authorizations are required to be verified in real-time from a network-connected terminal where the transaction can be evaluated for possible fraud in the U.S. Card use at some international acceptance points (e.g., some kiosks in Europe) will require that cards also be able to support an offline authorization environment, where the terminal is not connected to the network and transactions are verified between the POS and the secure data on the card. Transactions can be authenticated using static data authentication (SDA), dynamic data authentication (DDA), or combined data authentication (CDA), where all of the data is encrypted.

Timelines, Guidelines, and Changes

The four network brands in the U.S. have released similar EMV roadmaps, guidelines, and timetables. However, Visa and MasterCard are the key players in driving EMV adoption. Each has slight differences in specific aspects of their guides. The key items are as follows:

1. Incentives: Visa and MasterCard are offering to waive the audit fee for PCI compliance for merchants when 75% or more of their transactions are EMV-compliant, or originate from contact/contactless-accepting EMV terminals. MasterCard is offering the additional benefit of 50%-100% in financial relief for account data compromises (data breaches) for merchants that process 75% and 95% EMV terminal-originated transactions in 2013 and by 2015, respectively.

2. Merchant Processor/Acquirer Readiness: Visa and MasterCard have identified the start of Q2 2013 as the timeline for acquirer processor readiness to handle EMV transactions. Neither network has identified a mandate or guidelines for issuer card processors, only a liability shift date. Issuers may incur incremental costs associated with EMV, including expenses for the additional data that is handled in the authorization information flow and scripting / personalization fees for EMV cards.

3. EMV Terminals: Visa and MasterCard are backing different cardholder verification measures at the POS. Visa recommends Chip & Signature or Chip & Choice while MasterCard has created a liability hierarchy with greatest preference to awarded to Chip & PIN. Chip & PIN is likely to provide superior security, but will require that the terminal being used has a PIN pad. In addition, although one of the goals of the EMV guidelines is to help advance the necessary infrastructure for mobile payments, there are no requirements that EMV terminals must be able to support contactless transactions.

The key motivating factor for conversion to EMV is the liability shift in fraud. In 2015 (and 2017 for fuel merchants), acquirers with merchants that accept an EMV card using a non-EMV enabled POS terminal will accept losses associated with counterfeit fraud (and in the case of MasterCard, lost/stolen fraud). This is a material change from today's environment where issuers largely hold the liability for card-present fraud. The liability shift has been introduced in other countries and is meant to encourage POS terminal conversion ahead of the start date of October 1, 2015.

The conversion dates have been upheld by the networks in the other major payments markets worldwide. In terms of adoption, the majority of financial institutions, acquirers, and merchants have met the established EMV timelines in their respective markets by converting cards to EMV and terminals to accept EMV, and enabling the ability to process the transactions. In Canada, several instances of market cooperation complemented the suggested conversion process. Five of the largest financial institutions met to coordinate conversion strategies for their card portfolios. Interac, the Canadian debit network, separately required that mag-stripe transactions would not be accepted for purchases or ABM (ATM) use by 2015. Public transportation systems in Waterloo and Kitchener began EMV pilots and converted their terminals early. Working groups coordinated conversion between banks and merchants, held forums, and prepared best practices materials. In the U.S., similar working groups have been formed. For instance, several

industry constituents, including MasterCard, The SmartCard Alliance, Ingenico, First Data, TSYS, and FIS will provide guidelines for technical issues and consumer experience to aid in the conversion process and provide thought leadership.

The EMV timeline could be extended for a variety of reasons, though these delays have not led to timeline extensions in other markets. These delays may include:

1. Delay by Issuers: Due to several unknowns in the market concerning EMV, coupled with the lack of clarity around potential benefits as well as the incremental costs associated with processing and plastics.

2. Infrastructure Delays: Even if one form of verification becomes the preferred method, it is possible that some lag or fragmentation in merchant terminal adoption and the kinds of terminals that are adopted may delay full conversion.

3. Regulatory: The merchant-controlled routing provision of the Durbin Amendment may also be a source of delay. The industry is still debating whether or not the technical design of EMV will comply with the Durbin regulations as implemented. Changes will be required if does not.

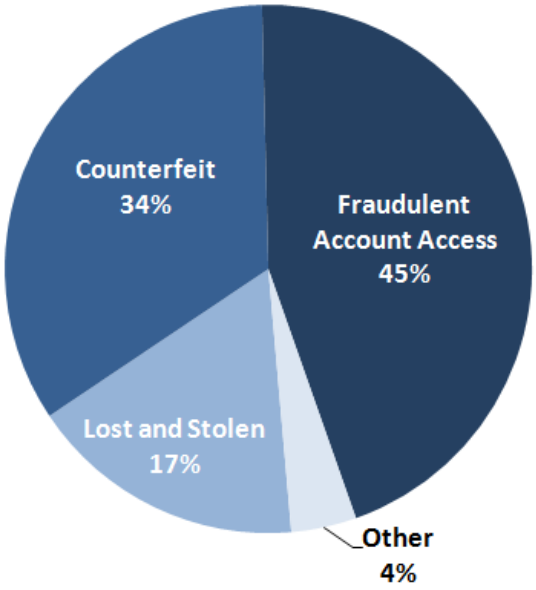
4. Terminal Replacement Delays: Not all merchant terminal replacement cycles fit within the roadmap timing and some may find the costs of early replacement outweigh the benefits.

Fraud in the U.S. and Lessons from Abroad

The primary rationale for converting to EMV is reducing payments fraud, specifically counterfeit. Other markets that have converted to EMV, such as the UK and France, experienced reductions in card-present transaction fraud of up to 25% when EMV adoption reached scale. This reduction originates from card-present fraud from data breaches, ID/application theft, phishing, counterfeit/skimming, and lost/stolen (the details of which are included below). This is typically accompanied by a material increase in card-not-present fraud after an EMV conversion. The U.S. is the last major market where mag-stripe transactions are the primary standard. While it is reasonable to expect that it will experience some reduction in fraud levels post-EMV, it should be noted that the U.S. already maintains stronger anti-fraud practices than most other markets employed prior to their respective EMV conversions. Therefore, fraud reduction in the U.S. may be smaller than the reductions experienced by other markets.

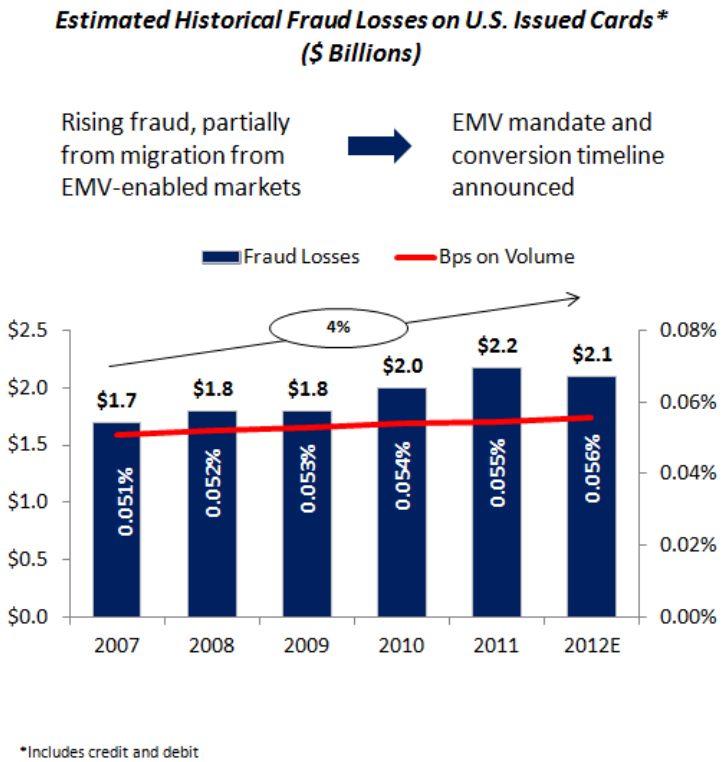
U.S. deployment of EMV cards and POS terminals is currently less than five percent. Today, card fraud (credit and debit) in the U.S. is estimated at $2.2 billion, or 5.5 bps on volume. Since 2007, card-related fraud has grown at 4% per year. It is important to note that the figures reported above do not include merchant fraud, or the fraud related to chargebacks that is borne by the merchant, which is not uniformly reported and can be difficult to estimate because of overlap in estimates and segmentation among other fraud types.

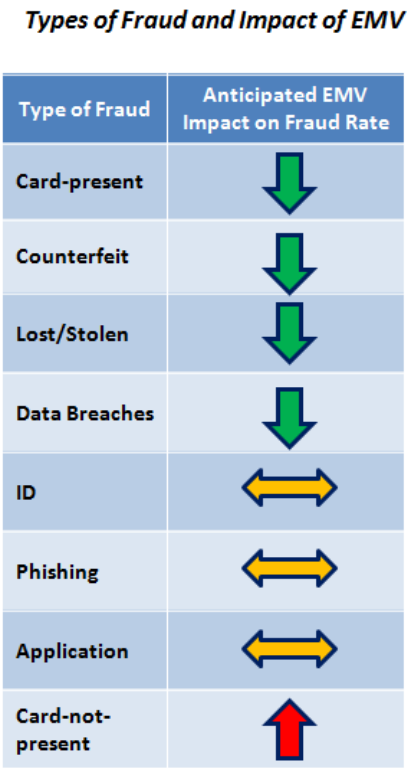
Figure 3: U.S. Fraud by Type (excludes cash)



Source: Visa

Figure 4: Fraud Losses and Types of Fraud*





*Includes credit and debit

Sources: Federal Reserve Bank of Atlanta, First Annapolis Consulting analysis

There are two main channels where fraud occurs:

1. Card-Present: Refers to fraud at the POS. EMV directly addresses this form of transaction fraud because the data in the chip is encrypted as it is transmitted to the terminal, reducing the likelihood that fraudsters can steal card credential information. How much card-present fraud decreases in the U.S. is in part a function of the verification method that becomes the industry standard. Chip & PIN would add an additional layer of security over the status quo today for credit and signature debit transactions because it requires that the user not only have the card plastic, but also know the associated PIN. Card-present fraud in the U.S. was about $2.2 billion in 2011. This includes issuer-related fraud losses only.

2. Card-Not-Present (CNP): EMV does not address CNP fraud, which typically results from e-commerce, m-commerce, and mail/telephone order (MOTO) transactions. It is possible that an online PIN utilized in the CNP environment may help reduce this fraud in the long-term, but U.S. deployments of PIN debit for remote purchases have largely been unsuccessful to date. CNP transaction fraud typically rises in EMV-enabled countries as fraud migrates to the weakest link. CNP fraud has increased anywhere from 20%-50% as a percent of total fraud (card-present and CNP) before EMV was implemented in some European markets because of the migratory effect. It is unlikely that this includes merchant fraud.

Card credentials are stolen by fraudsters in a variety of ways:

1. Data Breaches: Fraud that is the result of a breach of secure data from the entity that holds payments card credentials. This typically occurs when the database of one of these companies is hacked. It is unclear how large fraud losses that originate from data breaches are because of the difficulty in tracking fraudulent transactions back to a data breach itself. Data breaches often result in other kinds of fraud like counterfeit, which EMV will reduce because it uses dynamic data, making it more difficult to copy. PINs and verification measures can protect against some data breach fraud. For instance, a PULSE network study revealed that 34% of signature debit fraud can be traced back to data breaches, but only 14% of PIN debit fraud is a result of similar breaches. In some cases, card-not-present fraud that results from online-stored data breaches will not be affected by the EMV roadmap because the payment account number(s) may be compromised.

2. ID Theft / Application: EMV does not solve for fraud resulting from identity theft. Fraudsters can still utilize an individual's personal data to apply for and gain access to a card. ID fraud is difficult to track and often results in other kinds of fraud.

3. Phishing: EMV does not stop fraudsters that get cardholders to reveal card numbers, CVVs, and other information needed to utilize the card. Phishing can result in CNP / e-commerce-related fraud because it involves gaining access to the card credentials, but not the underlying data from the physical card that is taken by skimming and is used to make

counterfeit plastics. It is not expected that the EMV conversion will have an impact on phishing.

4. Counterfeit / Skimming: EMV will reduce counterfeit fraud by employing dynamic and encrypted payments credentials. However, it is possible that fraudsters will eventually adapt to the technology changes.

5. Lost / Stolen: An issuer that implements Chip & PIN would make it more difficult to use a card if it is lost or stolen, even in the case of mailed card fraud, because the PIN is set independently by the cardholder. Friendly fraud or fraud associated with a card that is taken from a family member, friend, or otherwise authorized user and misused is included in this category.

It is important to note that even though a card may be EMV-enabled and terminals may be capable of handling an EMV transaction, counterfeit fraud in the card-present environment may persist until EMV deployment reaches critical mass among issuers, merchants, and processors. Cards will still have mag-stripes for several years, and this means that card data can still be skimmed like it is today. Therefore, fraud reductions will be dependent on the speed upon which EMV becomes fully implemented.

Payments Value Chain Implications

EMV affects every constituent in the payments value chain to some degree. The level of impact varies depending on several factors. Broadly defined, these can involve changes to product functionality, card features, technology/equipment, trends in fraud, the liability shift, operations, and financial impacts. These factors are detailed below by constituent.

Cardholders / Members

Members will be exposed to some immediate changes as a result of the shift to EMV. Specifically, these may include:

1. A New Card: While EMV-enabled cards will continue to have mag-stripes for some time, the chip will also be visible. Credit unions should plan for a member education and communications campaign (see below).

2. A New Transaction Experience: Transactions will be completed by inserting the card into the reader or tapping, not swiping it. Cardholders may also begin entering a PIN for credit and all debit transactions if Chip & PIN becomes the standard for verification.

3. A New PIN: EMV cardholders may need to create up to two PINs— an online PIN and an offline PIN. Issuers can streamline the process and have cardholders use the same PIN, but the data storage and management of each PIN will be separate on the back-end. Or, the host could store one PIN that is used for online (connected to a network) and offline (non-connected terminals such as mass transit and gas stations in Europe) environments. It is not clear whether the cost of supporting an offline PIN will justify the limited number of use cases and likely transactions requiring it. Regardless, issuers should only allow

management of the PIN (i.e., changing it, resetting) in connected locations (e.g., ATMs, branch locations, etc.).

4. New Fees or Higher Costs: EMV will be more expensive to support than the current mag-stripe standard. Issuers will need to decide whether to pass these costs on to their cardholder base in the form of new fees, like a separate charge for an EMV-enabled card, or increase costs elsewhere to account for the new costs that the issuer will bear.

Figure 5: EMV Technology and Cardholder Payments Experience at the POS

	Contact EMV	Contactless EMV	Chip/PIN	Chip/Signature
				
What Would Be Familiar	• Very little	• Similar for cardholders already utilizing contactless cards or mobile NFC	• Similar process to PIN debit today	• Similar process to signature today • No signature required rules would likely still apply
What Would Change	• Card is inserted into the reader and read by the terminal, then removed	• Typically faster than swiping a mag-stripe • Cards could be dual-interface, confusing some cardholders about when to tap vs. insert	• Credit and signature debit transactions could require a PIN • No-PIN required rules may develop • Some cards may have a separate online and offline PIN (unlikely for issuers that synch PINs)	• Some cards could be enabled to handle both PIN and signature, potentially confusing cardholders

Source: First Annapolis Consulting analysis

Issuers

Financial institutions are immediately impacted by the EMV timeline, though it is unclear how some of these factors may play out in the long-term:

1. Card Reissuance: Card portfolios that are converted to EMV before October 1, 2015 could benefit from improved card-present security, being market-competitive with other issuers that have made the change to EMV, and possibly benefiting from the liability shift where fraud losses occur from transactions with merchants that have not converted in time.

2. Verification Method Management: Chip & PIN is the most likely verification method for EMV. This means issuers may need to manage a PIN for every credit and debit card. There is also the potential for confusion among cardholders or members. Travelers may need an offline PIN for use abroad or in other cases where terminals are not connected for real-time authorizations. Issuers can synchronize the online and offline PIN so that cardholders need only remember one PIN, but may need to educate them on the differences so they understand how to manage and use them appropriately.

3. Member Service / IVR Calls: As a result of the new transaction experience, verification methods, and reissuance, credit unions can expect more calls from their members in response to the initial confusion at the point of sale. This underscores the need for member education in coordination with any EMV card reissuance.

4. Costs: EMV conversion entails complex changes throughout the production, card management, transaction processing, and IT functions. Issuers can expect to pay more for card plastics, transaction processing, member support and servicing, and staff education and training. These costs will be more clearly defined as the market becomes more EMV-ready.

5. Fraud: In the longer-term, issuers can expect lower card-present fraud as EMV nears full adoption and mag-stripes are phased out. The exact timing and degree of fraud reduction is presently unclear.

6. Liability Shift: After October 1, 2015, if a merchant accepts an EMV card, but is unable to process it as an EMV transaction, the liability for fraud losses on that transaction shifts to the merchant, instead of the issuer.

Issuers that own and service providers that manage ATMs will also need to consider hardware and software changes. Visa has to date excluded counterfeit fraud at U.S. ATMs, but MasterCard has more specific requirements. Specifically, the owner of the ATM will be responsible for fraud resulting from EMV cards on non-EMV-compliant ATMs after October 1, 2013 for Maestro ATMs and all MasterCard cards after October 1, 2015. The Smartcard Alliance has outlined the following required changes. To be compliant, ATMs must have:

- An EMV-capable chip card reader
- An EMV software kernel installed by the manufacturer, with update messaging infrastructure to handle EMV data fields
- Tested end-to-end (hardware and software)

Some credit unions will have members that want an EMV-enabled card sooner rather than later. These "early adopters" likely include international travelers, corporate cardholders, and those people living in states near international borders (e.g., Canada, Mexico). Illustrated in Figure 5 below is a sample of EMV offerings in market today. As an interim solution, some issuers are offering EMV-enabled prepaid cards to these cardholders. Others have begun the process of permanently replacing their cardholders' debit and credit cards.

Figure 6: Announced Issuer EMV Conversions

	Financial Institutions	Card Type	EMV Auth Method
Banks	Bank of America	• Most corporate cards (Visa) • Available on several consumer cards upon request (Visa)	PIN
	CHASE	• Select Visa Signature • Palladium Visa Signature • British Airways Visa Signature • Hyatt Visa Signature	Signature
	citi	• All MasterCards by request • Automatic on Executive / AAdvantage World Elite cards	Signature
	Travelex	All Prepaid Debit (MasterCard)	PIN
	usbank	All FlexPerks Travel Rewards Cards (Visa)	Consumer – Sig. Corporate – PIN/Sig.
	WELLS FARGO	Wells Fargo Platinum (being tested with a pilot group – not available to the general public)	Signature & PIN
Credit Unions	Andrews	All GlobeTrek Rewards cards (Visa)	PIN
	State Employees' Credit Union	All Debit Cards (Visa)	PIN
	UNFCU	All Consumer Credit Cards (Visa)	PIN

Sources: financial institution press releases, First Annapolis Consulting research

Networks (Visa, MasterCard, and PIN-Debit Networks)

Payment networks may need to adjust their platforms to adjust for EMV, but will likely require minimal changes to switch infrastructure. There are a limited number of direct implications to the networks from the EMV conversion. Signature-verified payments products may need to be adapted to PIN-based verification if PIN becomes standard. It is possible that the payment networks might change the pricing structure to reflect the new standards imposed by EMV.

Acquirers and Merchants

Merchant processors/acquirers have until 2013 to be ready to support EMV transactions. There are no mandates for merchant conversion, but the incentives and the liability shift are relevant to these players. Incentives become available October 2013 and 2015. The liability shift occurs in October of 2015. It is possible that acquirer processors will pass on the costs associated with EMV readiness to merchants. In the other markets that converted to EMV, major merchants typically met the specified timelines, or did so shortly thereafter. Smaller merchants typically follow behind, making them more exposed to fraud that occurs on EMV cards that are used at non-EMV terminals.

Some of the key impacts to acquirers and merchants include:

1. Requests for EMV Terminals: Some merchants will want to convert as soon as possible. As a result, acquirers will need to be prepared to address merchants that have an upcoming terminal replacement cycle within the EMV timeline and specifically, the fraud

liability shift. Terminals will likely need to be equipped to handle both signature and PIN transactions until an industry standard emerges. It is not clear what percentage of terminals will be converted by 2015, but it is typical in other markets for the largest merchants to convert before or around the liability shift, with lag in adoption typically concentrated among smaller merchants, typically small-to-medium enterprises. In addition, merchants and acquirers will need to consider terminals capable of both contact and contactless enablement.

2. Readiness for EMV by April 2013: The roadmap notes that acquirers should be prepared to process EMV transactions by this date. However, penalties for non-compliance are unclear.

3. Liability Shift: In 2015, merchants that are not enabled to handle EMV transactions at the POS will be responsible for fraud losses on an EMV card.

4. Employee Education: Merchants will need to ensure their checkout process in the physical environment is aligned with the changes to the payment process as a result of EMV.

Acquirers may charge merchants new fees as a result of the liability shift. These fees may be used to increase revenues, cover additional costs, or mitigate any increases in risk.

Credit Union Implications and Considerations

As previously mentioned, EMV will have a wide range of impacts on credit unions. Issuers of all sizes must address several business changes stemming from the EMV guidelines. This section highlights the considerations credit unions may want to take into account as they make decisions concerning their respective EMV approaches.

Card Functionality

Credit unions, like other issuers, will have a say in whether Chip & PIN or Chip & Signature becomes the industry standard in the U.S. Most industry constituents support the migration to all Chip & PIN because of the fraud protection benefits of two-factor verification over the current signature verification for credit and signature debit. Financial institutions may weigh the fraud benefits of having all credit and debit transactions verified via PIN with the burden of educating members on the new payment process.

The decision to offer contact, contactless, or dual-interface plastics should also be considered. EMV contact terminals are likely to also be contactless-enabled to accept NFC mobile payments. In the meantime, it is unclear, given the changes in the consumer experience, whether cardholders will begin to utilize contactless payment methods. Issuers should therefore weigh member convenience vs. the additional costs for dual interface functionality. Contactless adoption has closely followed EMV conversion in other markets because of the minimal incremental cost to cards once the market matures, and the preference among issuers to steer the transaction process to a tap vs. inserting the card into the reader. These trends are likely to continue in the U.S.

The U.S. is likely to remain an online-authorization environment. However, travelers may require cards that are enabled with an offline PIN as well. It will be the credit union's responsibility to ensure that its cards are capable of conducting transactions under a variety of acceptance circumstances.

Product and Member Segmentation

Credit unions may also consider member and product portfolio characteristics when approaching the EMV conversion planning process and evaluate priorities for issuance. Most credit unions will not need to convert all cards at once and might instead prioritize high value members or those that would benefit the most from the conversion to EMV. Issuers should consider the fraud rates on each card product (credit, debit, and ATM) and may want to focus on re-issuing higher fraud cards first.

Closely related to the product segmentation is the member base. International travelers, corporate cardholders, and residents of border cities will be the first to benefit from EMV-enabled cards for use abroad. Credit unions should determine how big this base is and prioritize appropriately. All credit union members will need to be educated on how EMV affects the payments process at the physical POS so they can transition smoothly. Finally, credit union managers should think about how to announce these changes to the member base and conduct ongoing education about how to use the cards at the POS and manage their EMV PIN.

Service Provider / Processor Capabilities

Credit unions should understand what their service provider and/or processor's capabilities are around EMV as they consider what features to enable and for which members. If the credit union has the option to utilize an interim solution, it may want to consider offering a prepaid EMV card before fully converting key member segments.

In addition, the credit union may also consider its card processor's abilities relative to the EMV roadmap. The roadmap specifies that acquirer processors must be ready by April, 2013, but makes no mention of issuer processors. The credit union will need its issuer processor to be capable of handling the additional authorization data and the scripting of EMV plastics. The card producer's capabilities will also need to be evaluated, specifically around the EMV plastics offered and the associated costs.

Fraud

The key consideration related to EMV for fraud is weighing how impactful the conversion will be, particularly in the early years of the timeline. Every EMV-enabled card will still carry a mag-stripe until EMV terminal deployment is near 100%. Fraudsters will continue to search for new ways to exploit the encryption and security measures of EMV, and may eventually be successful. Again, it is important to note that EMV primarily addresses select types of card-present fraud (about 60% of all card volume is card-present, according to FIS Fraud Management). As such, credit unions should be careful in developing expectations for reductions in fraud resulting from the EMV conversion.

Costs

Credit unions will incur new costs from processors and other service providers as a result of EMV. Member education and other marketing costs are incremental and important to consider, but the primary costs will

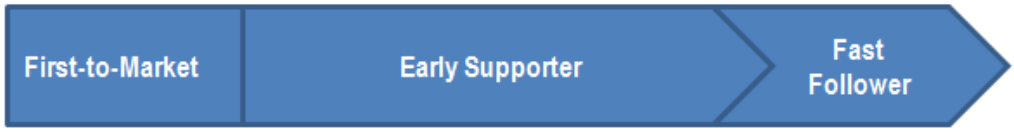
likely be increased processing and plastics costs. The other measurable cost may be an increase in member service/IVR calls due to the increase in PIN changes and associated EMV calls. Back-office cost management will need to be taken into consideration.

EMV transactions carry more information in the data stream and as a result, processors may charge a higher EMV authorization fee. In addition, credit unions will need to pay a scripting, or writing fee, for each EMV card that is created. This scripting process involves the writing of the secure data (card credentials, PIN, transaction size or velocity limits, etc.) to the chip on the card during personalization.

EMV Card Issuance Approach

Timing is perhaps the most important consideration for credit unions as they approach their EMV decision-making process. The biggest timing decisions are when to convert the payment product portfolios and how. Credit unions have several options for EMV conversion dependent upon their individual priorities.

Figure 7: EMV Issuance Options



Approach	Convert All Cards at Once	Stagger Conversion	Convert or Use Interim Solution	Wait to Convert
Description	Convert all cards to EMV in one conversion event prior to the 2015 deadline	Convert cards in accordance with normal reissuance cycle (~3 years)	Convert some cards or offer prepaid cards for higher priority members (e.g., international travelers)	Wait until 2015 or later to convert their cards
Pro	Exposes the credit union to the least fraud risk	Readies the portfolio for the liability shift date	Addresses immediate needs of members	Mitigates investing early for little gain while fraud liability remains status quo
Con	Larger up-front costs and tech commitments amidst several industry unknowns	May imply moving slightly ahead of most of the market, which may bring inherent risks	May risk slipping past liability shift date	May become a target for fraudsters as large issuers move to EMV

Note: Mag-stripes are typically replaced every three years in the U.S., but some issuers reissue EMV cards every five to seven years. This is done because of cost; timing needs associated with all-at-once conversions, and because EMV chip cards are typically more durable than mag-stripes.

When considering the timing and approach, credit unions may look to several internal characteristics that may help guide their selection of an approach.

1. Limited Transactions that Benefit from EMV (International / Cross-border or CNP): These credit unions can likely delay their conversion process should they be comfortable with the potential for increased domestic fraud risk. Mag-stripe acceptance will likely persist for some time after the 2015 conversion date. As such, members are unlikely to experience domestic acceptance problems. Issuers with lower exposure to card-not-present transactions may not see as high a rise in overall fraud, as their portfolio is not as exposed to the major source of fraud that EMV does not address.

2. A Small Member Base: For credit unions with less than 1,000 cards, a staggered conversion cycle may not be feasible. The credit union's size may lend itself to an all-at-once conversion because of the limited batch size. This conversion can be completed at any time, depending on issuer processor readiness.

3. Limited-to-No Credit Cards and Good Fraud Management: Credit card fraud is higher relative to debit, and credit unions without exposure to credit fraud may be able to lengthen their conversion time. Similarly, credit unions with lower-than-average card penetration may also wish to wait, given their lower exposure to any fraud changes that result from the conversion process.

Planning Process

As described above, credit unions have much to consider when it comes to EMV. That being said, the EMV process can be effectively managed through thoughtful planning, which may include:

1. Issue Cards that can be used in Various EMV Deployments: Since there are still several unknowns regarding EMV, early adopters should consider the incremental cost of additional features (e.g., contactless). Credit unions may want to consider adopting a card that can be programmed for any form of EMV verification. Dual-interface capabilities should also be considered, depending on the issuer's individual costs and complexity associated with conversion. Cards should also have enough data storage space to store an offline PIN or transaction size limit programming if necessary. Chips with 4K to 8K in memory size will be sufficient for most EMV features. Issuers deciding between one or the other should select contact and consider if and when products need to be migrated to contactless or dual-interface, keeping in mind that EMV cards have a longer "life" and are not replaced as often as mag-stripe plastics.

2. Stagger Card Reissuance: For some credit unions, a staggered re-issue approach will be best. Credit unions can begin re-issuing in accordance with the approach identified above as part of the normal re-issue cycle. High-priority members and international travelers may be converted before card expiration dates; prepaid may make sense as an interim solution for some credit unions. Credit cards should be considered for conversion first due their higher fraud rates.

3. Communicate with Your Members: Credit unions will need to provide educational materials to their members about the differences presented by the new cards and instructions on use. This can best be accomplished through enclosures with the card mailer. Branch and call center staff should also receive educational training so that they can address member questions and concerns.

4. Understand your Processor's Capabilities: Credit unions must determine whether processing and card production partners will be ready to issue EMV by the desired conversion timeline. Credit unions must determine what incremental costs they will experience as a result of the EMV conversion.

Figure 8: Suggested EMV Preparation Steps

2012: Begin Partner Discussions and Initial Planning

Step	Possible Actions
1	Get educated on EMV, with a focus on the technology and timelines. This includes educating employees on EMV and the upcoming impacts to their respective departments. Appoint EMV Transition Project Manager to coordinate the process if appropriate. Develop a timeline of EMV milestones.
2	Begin conversations with all partners (processors, networks, card producers) to learn more about EMV and required changes. Obtain partner EMV timelines and understand related impacts.
3	Monitor news surrounding EMV to understand key developments, potential changes to the timeline, and lessons learned from larger issuers that have converted or are converting.
4	Consider prioritizing key member segments for conversion. This may include international travelers, high-value members, etc.
5	Evaluate EMV-enabled prepaid card options as interim solutions. Evaluate which EMV-related features the card should have and when to replace them (i.e., 4-7 years vs. current average of 3).
6	Evaluate reissuance timeframes for existing mag-stripe cards.
7	Seek an update from key partners on EMV readiness.

2013 - 2014: Determine Conversion Strategy and Approach

Step	Possible Actions
1	Continue monitoring EMV developments and how changes may impact credit unions.
2	Confirm when partners will be prepared for EMV.
3	Finalize re-issue approach (convert all at once, on normal re-issue cycle, wait to convert, etc.).
4	Estimate the associated incremental costs of EMV based on partner discussions.
5	Begin to develop and deliver EMV training for call center and branch staff in-line with overall conversion strategy.
6	Develop and begin to implement an initial member education plan and continue to clarify how EMV may change the payments process.
7	Begin re-issuing cards as appropriate or confirm when conversion will begin.
8	Expedite EMV conversion for key member segments if necessary.

2015 and Beyond: Ongoing Conversion and Monitoring

Step	Possible Actions
1	Begin, continue, or complete conversion process based on overall strategy.
2	Monitor benefits from fraud liability shift and overall changes in fraud profile.
3	Continue to distribute member education materials.
4	Determine whether costs associated with EMV are in-line with market competitive rates.

Regardless of the credit union's size or characteristics, managers should exercise caution and be proactive in determining EMV strategies. It is unclear how the market will react, whether fraud will increase, decrease, or stay the same, and how mobile payments will play a role in the EMV conversion. While there are still many unknowns, careful planning, a thorough evaluation of EMV considerations and related impacts will optimize the go-to-market strategy for credit unions and ultimately members.

Summary

Every credit union has different fraud characteristics, membership, and products that need to be considered in the EMV planning process. In addition, each credit union needs to factor in its internal financial and human resources that can be committed to an EMV implementation. As a result of these variables, credit unions will need to appropriately identify and plan for EMV to achieve a successful implementation. Though not intended to be an exhaustive list, below is a summary checklist of recommendations and considerations:

1. Identify and give responsibility and accountability to a key manager/executive for overall EMV planning and execution; this role will be increasingly important as we get closer to the October 1, 2015 liability shift date.
2. Consider further EMV oversight such as an EMV committee of key executives to ensure a smooth roll out to employees and members.
3. Begin employee education on EMV. Understand what it is, how it works, and the types of fraud it does/does not address.
4. Monitor industry communications, progress, and trends. There are still significant decisions to be made by industry leaders that may require credit unions to modify their plans.
5. Consider whether to issue contact and contactless (dual interface) cards initially or contact only. Also consider the deployment of EMV enabled terminals when considering when to begin EMV card issuance.
6. Create a timeline of milestones and update and track progress against this timeline.
7. Analyze the credit union's fraud history to determine priorities for EMV card issuance that will have the greatest impact in reducing fraud. Determine where the credit union's fraud comes from, the split of card-present and card-not-present, and remember that EMV primarily addresses card-present counterfeit fraud. Think about fraud in overall dollar and percentage terms. Consider how fraud differs by payment products and member segments.
8. Determine which verification method(s) will be supported. Work with your processor to make sure they are prepared to accommodate these changes.
9. Develop a member education program. Focus on what the new cards will look like, how the POS interaction will change, why the change is occurring, and when it will occur. Utilize all channels available (e.g., in-branch, online, newsletters, messages, inserts, etc.).
10. Adjust product offerings as necessary to accommodate EMV.

There are many variables to consider and key decisions to be made in the near future. Continue to follow CSCU's communications on EMV as we lead up to October 1, 2015.

GLOSSARY

Key Terms	Definition
Authorization	A verification that the account being accessed for a transaction is in good standing and the transaction does not meet certain criteria associated with possible fraud.
Card Encryption	The process by which payments credentials are "locked", or encoded before being transmitted from the card to the POS terminal, where they are decoded with a "key", or decryption process.
Cardholder Verification Method	The process that occurs during the transaction after authorization, where the cardholder either signs a receipt or pad, enters additional card information like a card security code on the plastic for card-not-present transactions, or enters a PIN to verify identity and complete the payment.
Card-present	A transaction made where the card is present and interacts with the physical POS terminal to transmit payments credentials, either from an EMV Chip or mag-stripe.
Card-not-present (CNP)	A transaction occurring in an environment where the card cannot be used and card credentials (card number, card security code, expiration date, etc.) are entered manually, typically in an e-commerce, m-commerce, or MOTO (mail order/telephone order) transaction.
Chip (Integrated Circuit)	A circuit, or electronic chip, that is included on all EMV cards and stores encrypted payments data like credentials, offline PINs, and transaction limit data.
Chip & PIN	A verification method where the cardholder enters a PIN at the POS to complete an EMV transaction.
Chip & Signature	A verification method where the cardholder signs a receipt or POS pad to complete an EMV transaction.
Chip & Choice	An option provided to issuers by the networks that allows them to support Chip & PIN, Chip & Signature, or both.
Combined Data Authentication	EMV authentication method where a unique encryption key is given to data on the card and the transaction. A separate verification code is given, which is then decoded by the POS terminal when card credentials are transmitted.
Contact	Transactions that occur with a card plastic that makes physical contact with the POS terminal (either by a mag-stripe that is swiped or an EMV card that is inserted) to transmit payments credentials from the card to the POS.
Contactless	Transactions that occur with a card plastic or other properly enabled device that transmits payments credentials via a radio signal using Near Field Communication (NFC) technology, when in proximity (1-3 inches) of a properly-enabled POS terminal.

Key Terms	Definition
Dual-interface	A card that is enabled to transmit payments credentials by either contact (EMV or mag-stripe) or contactless methods.
Dynamic Data Authentication (DDA)	EMV authentication method where a unique encryption key is given to the data on the card and is unique to each transaction, which is then decoded by the POS terminal. The DDA is what renders compromised card data useless to fraudsters and counterfeit fraud.
EMV (Europay, MasterCard, Visa)	A global card standard that enables more secure payments transactions by encrypting data during transactions at the point of sale.
EMV Timeline	A timeline set by the major payments networks that details how and when issuers, acquirer processors, merchants, and other payments industry constituents should convert the U.S. market to EMV over the next few years.
Fraud Liability	The entity along the payments value chain responsible for the losses associated with a fraudulent transaction. Typically the issuer, but sometimes the merchant.
Fraud Liability Shift	A shift of the fraud liability from the issuer to the merchant. As part of the EMV roadmap, acquirers (and by relation, the merchant) will be responsible for fraud losses associated with EMV cards that are utilized at a non-EMV-enabled POS terminal after October 1, 2015 (October 1, 2017 for fuel dispensing merchants).
Fraud Migration	The process by which the fraud from countries that have adopted EMV moves to countries that have not adopted EMV. Can also be defined as fraud that moves from a source that EMV increases the security of (card-present) to one that it does not (card-not-present).
No Signature Required	A credit or signature debit transaction that is below an identified ticket size (set by the merchant individually, with a ceiling set by the networks) and does not require a signature to complete the transaction.
Offline Authorization	An authorization that occurs between credentials stored in the card and an offline, or standalone POS terminal.
Online Authorization	An authorization that occurs between credentials stored in the card and a network-connected POS terminal.
Personalization	The process by which cardholder name, account, and other data is coded to the mag-stripe or the chip.
Scripting	The process by which secure card credentials are written to the chip on the card at the time of personalization.
Static Data Authentication (SDA)	Authentication method where a single encryption key is given to the data on the card and the transaction, which is then decoded by the POS terminal.

SOURCES

Cisco Online Survey, May 2012.

Cybersource Online Fraud Report, 2012.

EMVCo, "A Guide to EMV" May 2011.

EMVCo, Worldwide EMV Deployment and Adoption, updated as of Q4 2011.

Euromonitor 2011: U.S. Cards Report.

Federal Reserve Bank of Atlanta 2011 Risk Forum White Paper.

FIS 2012 Client Conference, EMV and Fraud Reduction- Learning from Canada and Europe.

PULSE Card Fraud Study, 2008.

Smartcard Alliance, "Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?" September 2012.

The Nilson Report, Issue 987, January 2012.

VeriFone 2012 EMV Webinars.