Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud

A Smart Card Alliance White Paper

Publication Date: October 2009

Publication Number: CMPC-09004

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

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. 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 cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

TABLE OF CONTENTS

1 Introduction

The global payments industry has implemented a wide variety of techniques to combat card-based fraud. Outside of the United States, the payments industry has moved or is moving to EMV[1] technology to combat increasing fraud rates. The U.S. has historically addressed fraud in a different manner, relying on magnetic stripe cards and online authorizations as well as other online techniques to detect and react to fraud. The U.S., however, is now issuing contactless payment cards based on smart chip technology that secure transactions by generating a unique dynamic cryptogram (an encrypted code) with each transaction.

The payments industry is undergoing a significant change with the move to EMV outside of the U.S. and increasing use of contactless payments in the U.S. This white paper was developed to discuss how the resulting changes to the payments infrastructure are expected to affect card-based fraud in the United States and how different technologies can address this fraud.

The white paper provides an overview of current fraud levels in the U.S. and of projected trends based on anticipated changes to the payments infrastructure. It focuses on credit and debit card fraud, which accounts for the vast majority of payment fraud in the U.S. Based on a cross-section of industry research and estimates, approximately 77% of payment fraud derives from these two payment types.[2]

The different approaches used by the U.S. payments industry to combat fraud are described, including both preventative measures and mitigating measures. The white paper also examines the opportunity presented by new technologies and processes, particularly chip card-based technologies and processes, to help mitigate card-based fraud losses.

The white paper concludes with a discussion of U.S. contactless payments deployment and its impact on increasing the security of the U.S. payments infrastructure and reducing fraud, and describes how contactless chip technology can eventually lead to the deployment of globally interoperable EMV cards and terminals in the United States.

[1] Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals. EMVCo members now include American Express, MasterCard, JCB, and Visa.

[2] American Bankers Association and Tower Group.

2 U.S. Payment Fraud Today: What Is the Issue?

The payment card industry has been subjected to fraud losses for as long as cards have been in general use. However, acquirers and issuers are currently taking a closer look at the issue of fraud, as they begin to recognize that the cost of fraud is higher than the actual dollar amount of losses. Acquirers and issuers understand that losses affect card usage rates, authorization parameters, operational processes, and staffing while also decreasing profit margins. Furthermore, these losses can endanger the most valuable asset acquirers and issuers have—their relationships with business partners and consumers.

It follows that the industry should give serious consideration to new technologies and processes that may prove to be effective in combating fraud. Chip-based payment is one of those technologies. It would move the industry away from reliance in many markets (the U.S. market in particular) on magnetic stripe technology and its limitations. In addition, contactless payment introduces new processes that can move the industry from a reactive, loss identification and remediation mentality to a proactive posture of loss prevention.

The exploration of chip card-based technologies and processes comes at an opportune time. The United States may eventually become the weakest link in the payments industry and, thus, both the region to which fraud could migrate and a source of counterfeit fraud for issuers outside of the U.S. As European countries migrate to more secure chip card technology, criminals change their behavior and seek to exploit less secure technologies (the magnetic stripe) and locations outside of the region.[3]

2.1 Payment Fraud Statistics and Examples

News about credit card cloning, data breaches, and online fraud is becoming all too familiar to American consumers. Fraudsters have devised so many inventive attacks that even the most careful of consumers and reputable businesses can become victims. The recent breach at Heartland Payment Systems compromised millions of credit card accounts that could potentially be used to create counterfeit cards.[4] Consumers were not even aware that their cards had been cloned, because the original card was still in their possession. Similar breaches occurred at TJX[5] and RBS WorldPay[6], and in 2008, investigators linked many breaches to international crime rings. Some of the fraudsters were eventually caught when they began to use counterfeit cards and were discovered by bank fraud detection mechanisms.

Modern fraud detection mechanisms are vulnerable, however, because they rely on identification of an unusual pattern in purchasing habits before blocking subsequent purchases ("post-fraud"). Fraudsters leverage the delay in pattern detection, among other things, to give themselves a head start—a fraud "grace period" of from several hours to several days—when they can purchase items that are easily converted to cash or simply withdraw cash from an ATM.

There are no reliable, precise, consistent statistics for U.S. payment fraud. Rather, the industry relies on surveys and extrapolations to gauge the levels and trends for payment fraud. By any account, however, the losses are significant.

At a global level, the Nilson Report estimated card fraud of $5.5 billion on $11.8 trillion in purchases of goods and services and cash advances in 2007, the most recent year for which data is available.[7] Based

---

[3] APACS, *Fraud: The Facts 2008,* http://www.cardwatch.org.uk/images/uploads/publications/Fraud%20the%20Facts%202008_links.pdf; SouthportVisitor.com.uk, "Fraud on U.K.-issued cards down 23%," October 7, 2009, http://www.southportvisiter.co.uk/southport-news/southport-breaking-news/2009/10/07/fraud-on-uk-issued-cards-down-23-101022-24870875/

[4] "Three Indicted in Major Hacking Case," Kim Zetter, *Wired*, August 17, 2009, http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/

[5] "TJX Customer Data Hacked, Fraud Reported," CBS News, January 24, 2007, http://www.cbsnews.com/stories/2007/01/24/business/main2396258.shtml

[6] " RBS WorldPay Data Breach Hits 1.5 Million," internetnews.com, December 24, 2008, http://www.internetnews.com/security/article.php/3793386/RBS+WorldPay+Data+Breach+Hits+15+Million.htm

[7] *The Nilson Report*, Issue 915. November 2008

on a review of several sources, the Smart Card Alliance estimates total U.S. card fraud losses in 2007 at $1.7 billion,[8] although Mercator Advisory Group reports that fraud losses are probably dramatically underreported and may actually be as high as $16 billion, especially when all of the associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses are considered.[9]

The true cost of fraud, however, exceeds the actual dollar amount of losses. Financial services companies incur damage to their reputations, higher overall operating costs for increased vigilance (including transaction monitoring), reduced productivity, and higher staff expenditures; they also bear the cost of reissuing cards after a fraud incident.

An often overlooked and less well understood cost is the impact fraud has on card usage. As fraud events overwhelm the industry, many organizations use a "block and reissue" policy that can have considerable adverse effects.

A recent analysis of 56,000 reported debit card fraud incidents identified a number of other costs associated with fraud, including the following:[10]

- Reissuance costs: The cost of reissuing cards, providing consumer correspondence, reactivation campaigns, and other associated activities averages $25 per event. Based on the average of four transactions per event, approximately 14,000 consumers were affected at a cost of $350,000.
- Reduced reactivation rates: Due to the increase in fraud events and decrease in consumer confidence in financial institutions over the past 12 months, approximately 20% of affected consumers (2,800 consumers) did not reactivate their accounts. The increased expense of obtaining new cardholders meant issuers spent $560,000, at a rate of $200 per consumer, to recoup the lost business.
- Decreased transaction volumes: Approximately 30% of consumers used their card less frequently, decreasing the revenue realized by the financial institutions. Additional revenue associated with a consumer's demand deposit account (DDA) is also typically lost as consumers end their relationships with the financial institution.

Financial institutions also experience significant lost revenue opportunity due to fraud. Attempts to reduce fraud by deploying unduly stringent authorization strategies that target perceived high risk activity can lose millions of dollars of potential revenue. Paired with the ever-increasing cost of originating a new account and decreasing interchange revenue, fraud events have a significant, if not always explicit, cost to issuers.

2.2 Emerging Technologies and Global Impact

As new technologies to thwart fraud and improve margins emerge, the United States can look to the experience of other countries to assess potential risks and rewards.

Chip cards based on EMV specifications have made inroads in Europe, Latin America, Canada and Asia Pacific, with countries reporting benefits from the adoption of EMV.[11] In Europe and some other markets,

---

[8] According to a PULSE survey in 2008 (http://www.remittancedirectory.com/pdfReader.jsp?document=/docs/PULSE050208.pdf), issuers lost 5.40 basis points (0.054%) per dollar spent through signature debit transactions in 2007 and 1.09 basis points (0.0109%) through PIN debit transactions. According to *The Nilson Report* (May 2008), U.S. signature debit transaction volume in 2007 was $1,101.98 billion. *Cards & Payments* reported in May 2009 that the U.S. fraud rate for consumer bankcards in 2008 was $1.1 billion (7% of total charge volume). Combining these statistics, estimated U.S. fraud in 2007 is $1.7 billion.

[9] http://www.remittancedirectory.com/pdfReader.jsp?document=/docs/PULSE050208.pdf; *The Nilson Report*, Issue 902, May 2008; *Cards & Payments*, May, 2009; Mercator Advisory Group, "Fraud to the Left of Me, Risk to the Right," October 2008

[10] First Data, "The True Cost of Fraud" (March 2009)

[11] APACS, *Fraud: The Facts 2008*

the adoption of EMV has been coupled with a personal identification number (PIN) stored on the chip. The PIN replaces the cardholder's signature, significantly improving protection against loss and theft.[12]

These higher security cards appear to be effective at reducing some types of fraud. In the United Kingdom, mail non-receipt and lost and stolen card fraud has decreased. Counterfeit fraud within the geographic footprint of the issuer has also declined. U.K. issuers are now focusing authorization strategies on transactions from high risk, non-EMV-enabled markets as a means of further reducing their exposure.[13] ATM skimming fraud losses have also been reduced by up to 55% due to the increasing proportion of EMV-compliant ATMs.[14]

While EMV has clearly helped to reduce payment card fraud where it has been deployed, e-commerce fraud continues to be a concern. In 2008, according to the 10th Annual CyberSource Survey, criminals stole $4 billion from online merchants, up from $3.7 billion in 2007, for a loss of 1.4 percent of online revenue, a rate that has held constant for 3 years.

The payment card industry will need to build on the progress of EMV and look forward to new means of addressing e-commerce fraud loss (for example, MasterCard's Chip Authentication Program (CAP) and SecureCode™[15] and Visa's Dynamic Passcode Authentication and Verified by Visa[16]).

2.3 Payment Fraud: What Does the Future Hold?

The U.S. payments industry needs to determine whether it is prepared for the potential of significantly higher payment card fraud if fraud migrates to the U.S. from EMV-enabled locations.

Based on the APACS report "Fraud, The Facts 2008," United Kingdom issuers have seen fraud committed in the United States increase by 8 basis points in the past year. Counterfeit fraud in the UK decreased by 32% year-over-year, but international fraud, most of which occurred in the United States, increased by 114%. (See Figure 1.)

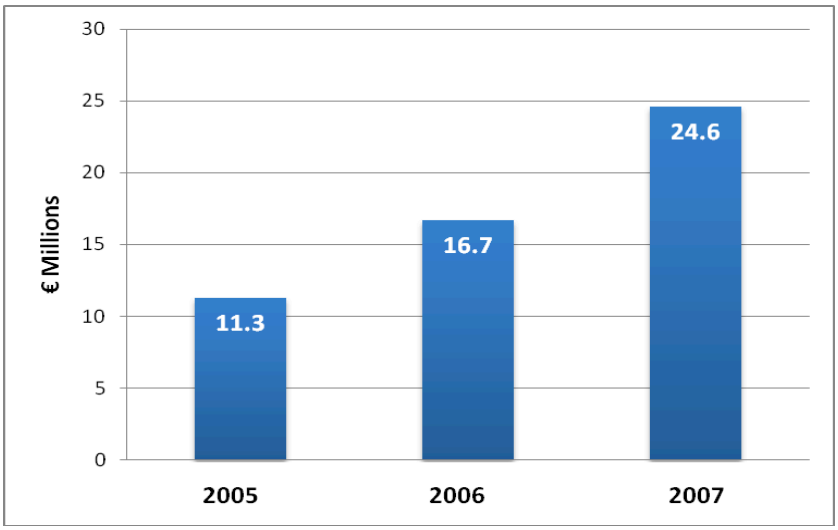

Figure 1. U.K. Issued Cards: Counterfeit Fraud Committed in the U.S. (Source: APACS)

[12] This is commonly referred to as "chip and PIN."
[13] APACS, *Cheque Fraud*, http://www.apacs.org.uk/payments_industry/payment_fraud_2.html
[14] ATM Marketplace, "EMV adoption in Europe knocks ATM fraud losses down 55%," 1 November 2007
[15] MasterCard, *OneSMART Authentication*, https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/biz_opportunity/cap/index.jsp
[16] Visa, *Dynamic Passcode Authentication: Overview Guide*, http://www.visaeurope.com/documents/aboutvisa/dynamicpasscodeauthentication.pdf?d=070207

Criminals are known to exploit the weakest link, moving from locations where stronger authentication is present to those where it is not, or from financial institutions and merchants who have more sophisticated fraud detection and prevention tools to those with less. With issuers in the rest of the world moving to EMV, criminals are more likely to move counterfeit magnetic stripe card activities to the U.S., attacking both U.S. and international issuers. If the United States wants to avoid an incoming tide of higher loss, the industry must be willing and able to make the necessary investments in certain emerging technologies and processes, as discussed in Section 3.

The adoption of chip cards and POS terminals in the United States would have a dual benefit. Not only would American acquirers and issuers benefit from smaller losses and improved cost management controls, but all EMV-enabled issuers globally could experience reduced losses and decreased operational impact from payment card fraud.

3 How Can Fraud Be Addressed in the U.S. with Commercially Available Solutions?

A number of commercially available solutions can assist in dealing with fraud in the United States. Generally speaking, they fall into one of two categories: mitigating measures or preventative measures. Card authentication and cardholder verification are examples of preventative fraud measures, because effective authentication and verification mechanisms can prevent fraudulent transactions. If the preventative solutions are ineffective, then compensating controls (mitigating measures) are needed to reduce the impact of fraud.

3.1 Mitigating Measures or Compensating Controls

Fraud mitigating measures are in place today and are used to address security gaps that fraudsters can exploit. A common cause for these security gaps is the poor performance of the chosen authentication solution (see Section 3.2). A typical scenario involves using these mitigating measures to address a current fraud attack based on patterns seen in previous fraud attacks. Fraud mitigating measures use information on past fraud trends to reduce the impact of future fraud trends.

3.1.1 Neural Networks

Neural networks are one type of fraud detection system that is used to protect credit or debit card accounts. They are typically integrated into the issuer's authorization process. Neural networks develop a profile of "normal" behavior for each account and then compare the current transaction's characteristics to that profile, to produce a "score" that indicates the likelihood that the transaction is fraudulent.

Neural network performance is directly related to the quantity and quality of information presented to it. To build a better profile for a particular account, the neural network should "see" every transaction for the account. Because the U.S. market uses online authorization, neural networks are an ideal tool to support issuer operations. The performance of neural networks can be improved by including higher quality data in the transactions, such as by using dynamic authentication data as opposed to static authentication data.

3.1.2 Analytics

Analytics are another tool used to mitigate fraud during the issuer authorization process. Transaction activity for a portfolio is evaluated and used to develop a set of "expert rules" that are applied in the authorization process. These rules are applied to the transaction's characteristics, the account profile for transaction velocity (the speed at which the card is used by the consumer), known shopping patterns (stores, transaction size), and international activity.

Analytics also provide maintenance support for an issuer's neural networks. With proper maintenance, analytics will help improve the performance of the neural networks as the card portfolio spend patterns and fraud trends change over time.

3.1.3 Alerts and Out-of-Band Techniques

Alerts are notifications sent over e-mail or to a mobile device (typically using SMS) that allow a cardholder to track card transactions in near real-time. The cardholder can customize alerts by transaction amount, date and time at which the transaction occurred, and merchant name and location. Alerts may also include information about how to contact the issuer, either through a telephone number or a direct link to the issuer's customer support desk or website.

The primary purpose of alerts is to notify the cardholder of possible misuse of the card, with the intention of preventing any further misuse. Additional benefits include enabling the cardholder to monitor and track any card transactions in near real-time, which may be useful in managing spending on secondary or

linked accounts. However, alerts occur after the fact, and therefore are ineffective in preventing the first fraudulent transaction. In addition, if the alert is not received for some reason, the cardholder is unable to take action and mitigate further fraud.

3.2 Preventative Measures

Preventative measures use authentication mechanisms to validate that the payment card is authentic or that the person presenting the card is the genuine cardholder.

Three "factors" can be used for authentication: something you have (such as a card), something you know (such as a PIN), and something you are (such as a fingerprint). The more factors that are used to authenticate an individual in a transaction, the more reliable the authentication of an identity is. The financial services world typically uses the first two factors for authentication.

In addition, authentication can be either static or dynamic. Static authentication always uses the same credential or data for validation. Dynamic authentication uses a different credential each time, and the credential used is typically transaction-specific. As an example, in the case of magnetic stripe cards, the same static data is validated with every transaction, while chip cards support the generation of a different, dynamic security value for each authorization request, improving security.

The next sections describe the different types of authentication mechanisms currently used in the U.S. payments industry.

3.2.1 Authorization

Online authorization is the process by which merchants seek approval (authorization) for a transaction from the issuer. The authorization request is routed from the merchant to the issuer. When the request is presented, the issuer provides a response (approve or decline) based on available funds, customer service, and fraud management considerations. Authorizations in the U.S. market are processed almost exclusively online, due to the low cost of telecommunications.

In several markets outside the U.S., offline authorizations can take place up to the floor limit of the retail point-of-sale (POS) using chip cards and EMV-compliant terminals. For these transactions, the card is the issuer's agent and acts based on the issuer's preferences for the account. Offline authorizations are intended for markets or sectors where the cost of online authorization is high, due to costly telecommunications services, or where telecommunications service is not always reliable. Offline authorizations are also used where acceptance locations do not have a convenient telecommunications connection (e.g., with parking meters). Most EMV transactions continue to be authorized online.

3.2.2 Card and Cardholder Authentication with Static Authentication Data

For retail POS transactions using magnetic stripe cards, static authentication data is used to verify the card participating in the transaction. Since the data is static, it does not change from transaction to transaction. If static authentication data is captured, it can be used in fraudulent transactions in the retail POS environment or in the card-not-present environment. As a result, this valuable data must be protected.

3.2.2.1 Card Verification using the Card Security Code

A card is a token and therefore qualifies as a "what you have" authentication factor. A card security code[17] is encoded onto the magnetic stripe on the card. Validation of the card security code is intended to confirm that the card participating in the transaction is legitimate. The card security code on the magnetic stripe is read by the merchant's terminal and sent to the issuer, along with the transaction details, as part of the authorization request. The card security code is validated by the issuer's

[17] This value has different names depending on the payment brand. For example, Visa uses the term Card Verification Value (CVV) and Card Verification Value 2 (CVV2) and MasterCard uses the term Card Verification Code (CVC) and Card Verification Code 2 (CVC2).

authorization systems, using a cryptographic process. The issuer takes action based on the result of the card security code validation.

A different card security code is also printed on the back of the card. Although initially developed as a tool for mail order, telephone order, and e-commerce sales environments, the printed card security code has been used in retail POS environments to provide an additional card verification mechanism. Like the card security code written on the magnetic stripe, the printed code entered at the POS is validated by the issuer's authorization systems, using a cryptographic process, and the issuer will take action based on the result of the validation.

3.2.2.2 Cardholder Verification using Online PIN and AVS

Cardholder verification is different from card authentication in that it attempts to validate that the cardholder is legitimate. A physical signature is the most common, yet least secure, cardholder verification method. A PIN represents a secret shared between the issuer and the cardholder. The PIN therefore qualifies as a "what you know" authentication factor. By verifying a shared secret, the issuer can be assured to a much higher degree than with a signature that the correct cardholder is participating in the transaction. The PIN is validated by the issuer's authorization system using a cryptographic process. The issuer takes action based on the result of the PIN validation.

An additional mechanism, the address verification service (AVS), was initially developed as a tool for mail order, telephone order, and e-commerce sales environments. However, it has been used in retail POS environments to provide additional cardholder verification. The cardholder is requested to enter the billing zip code into the merchant's terminal so that it can be sent with the authorization request. Although AVS relies on information that is not necessarily a shared secret, it does constitute an additional mechanism that issuers can use to add confidence that the valid cardholder initiated a transaction.

3.2.3 Contactless or Chip Card with Dynamic Authentication Data

A person's credit or debit card number has two important roles in a transaction. First, the number is a pointer to the account holding the cardholder's funds, providing a unique identifier for that account. Second, the number provides routing information from the POS to the bank where the account is held. When combined with an authorization to release funds from the account to a merchant, this data becomes useful for payment purposes. Unfortunately, it also becomes useful to criminals who intend to commit fraud.

It is very difficult to prevent the data on a magnetic stripe from being copied, or skimmed. Since the data is static, it can simply be read, using a low cost reader, and transferred onto a counterfeit card or used fraudulently over the Internet.

The obvious approach to preventing unauthorized use of the card number is to "hide" the data, or encrypt it. However, since the information is needed both by the merchant (for payment) and by the network (for routing), encryption is very difficult. A more intuitive and effective approach is to render the data useless to criminals by adding a dynamic element to the transaction record so that every transaction is unique and transaction record cannot be used to create a fraudulent card or transaction. The dynamic element would be generated with each transaction using a secure cryptographic technique.

Chip cards and secure contactless devices play a significant role in generating dynamic data. The card or device is capable of securely storing a unique derived key that can generate a dynamic cryptogram with each transaction. Two types of cryptograms are in use today, both of which protect cardholder account data from skimming.

The first type of cryptogram entails the use of a dynamic card security code, which changes for each contactless transaction and replaces the magnetic stripe-based card security code before the transaction is read at the POS. Securing the data before it leaves the payment card (the initial end-point of a transaction) secures the entire transaction. Attempts to secure the transaction later in the process without considering data on the card leaves a significant vulnerability for counterfeit card fraud. Use of

dynamic card security codes not only makes the transaction more secure, it also renders any captured data valueless for use on a counterfeit magnetic stripe card.

Contactless transactions today generate dynamic cryptograms with each transaction. The dynamic cryptograms protect cardholder data in all payment transactions, because they make each payment transaction unique. The chip card must be present to generate a valid cryptogram, which is verified online when the transaction is authorized. Expanding use of contactless cards throughout the U.S. payment system would lower fraud over time because stolen payment card information could not be used to make fraudulent cards. In the future, it may be necessary to implement a stronger, EMV-based cryptogram to stay one step ahead of fraud.

3.2.4 EMV/Chip

Increasing counterfeit card fraud led the financial 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 bank cards.

EMVCo developed its specifications to ensure global interoperability – so that any EMV-compliant card can be accepted at any EMV-compliant point-of-sale anywhere in the world. The EMV specifications not only define how chip cards can be used for fraud prevention but how they can be used by issuers to offer additional features to cardholders such as multiple payment applications on the same plastic card. Chip cards can carry security credentials that are encoded by the card issuer at personalization. These credentials, or keys, are encrypted and impervious to access by unauthorized parties. These credentials therefore prevent card cloning, one of the common ways magnetic stripe cards are compromised and used for fraudulent activity. In practical terms, this means that chip card-based payment account information cannot be skimmed, which increases the level of security to the point where it can actually be thought of as fraud prevention.

Fraud prevention technology in chip-based EMV payment cards (which can be contact, contactless or dual-interface cards) complements post-fraud detection mechanisms by providing an additional layer of intelligence to protect consumers. Issuers, acquirers and merchants in a large number of markets around the world have decided to implement full EMV technology. Some programs are signature-based and others use a PIN, commonly known as "chip and PIN," to combat fraud.

In short, chip cards, which can be used in contact or contactless mode, provide a high level of security based on their ability to compute ever more secure cryptograms using dynamic transaction data or provide additional information as required by the issuer. The end result is that an authorization request cryptogram is calculated and sent with each authorization request, and this value is always unique.

Combining the state-of-the-art in post-fraud detection with the stronger prevention mechanisms provided by using chip cards will help the payments industry stay ahead of international fraud rings. Banks will profit from fewer losses due to fraud; merchants will profit from fewer chargebacks; and consumers will profit from improved service and security levels.

3.3 Fraud Measures Summary

Authentication solutions that employ dynamic credentials provide performance for combating fraud that is superior to that provided by solutions using static credentials. Static credentials can be compromised, as shown by the rash of data security incidents throughout the United States. These compromised credentials can be used in counterfeit fraud at a retail POS, at ATMs or over the Internet at e-commerce merchants. As a result, static credentials must be protected by all participants in the payment transaction, from merchants to processors to banks, and authentication solutions that are dependent upon them must be reinforced with additional fraud mitigating measures.

In contrast, if a dynamic credential is compromised, it has no value in any transaction except the original one. Using a more robust authentication solution will improve the performance of current authorization systems and fraud mitigating measures. If issuers can be assured to a higher degree that it is their

cardholder who is participating in the transaction, they can make better, more effective authorization decisions. This would in turn improve transaction approval results, creating a better yield of transactions – that is, higher sales volumes at lower fraud rates.

4 Contactless Payments in the United States: Benefits for Addressing Fraud

4.1 Current Status of U.S. Contactless Payments Deployment

Contactless cards have been issued in the United States since 2004. As of June 2009, more than 90 million contactless cards, fobs, and tags have been issued by multiple card issuers under the brand names American Express, MasterCard, and Visa. More than 130,000 merchant locations accept contactless payments today, including a broad cross-section of merchants in a wide variety of merchant categories.

4.2 Measures to Combat Potential Fraud

The primary sources of credit and debit card fraud are card cloning, card skimming, and transaction replay. Each of these forms of fraud is possible because static data can be copied from one source and reproduced on fraudulent cards or used in an Internet purchase transaction. Current magnetic stripe technology is highly susceptible to data copying, and it is equally easy to encode fraudulent magnetic stripe cards using inexpensive encoding devices. For this reason, in many countries terminals are brought to restaurant tables to process a debit or credit card transaction so that the card never leaves the cardholder's sight. Allowing the server to take the card to the cash register provides all the time required to copy magnetic stripe data.

There are other sources for criminals to obtain this data as well. The data can be obtained from a retailer's or acquirer's database, a line tap on a terminal, a fraudulent terminal, or a compromised reader attached to an ATM. Once the static data is captured, it is easy to produce a fraudulent card quickly and difficult for issuer systems to identify a fraudulent transaction. Typically the fraud is discovered only after a pattern of unusual transaction behavior is detected or when the cardholder reviews a statement.

Branded contactless payment programs being implemented in the U.S. market address the fraud issues associated with the current magnetic stripe card-based payment infrastructure. These programs provide a security solution that is similar to EMV in three areas:

- Counterfeiting chip cards is virtually impossible, and any attempt at counterfeiting is detected by the issuer system.
- Any stolen card data cannot be replayed in a successful transaction.
- Risk management data can be sent from a card to its issuer.

Branded contactless payment cards address these issues by leveraging the logic and security provided by the microprocessor chip embedded in the cards. U.S. and EMV contactless cards use identical construction and communication protocols (ISO/IEC 14443). As a result, the physical contactless reader interface is the same for both U.S. and EMV contactless cards. It is the logic within the card application that is different.

4.3 The First Step in Fighting Fraud: U.S. Contactless

The first layer of fraud protection in contactless cards is the method by which data is loaded onto the chip, which is referred to as the personalization process. Before any data can be loaded, a special key, or set of keys, must be submitted to the chip to gain access to memory. This security feature protects cards between manufacturing and personalization and distribution to the cardholders. Once the card has been personalized, it becomes virtually impossible to get access to the chip's secret keys. This feature alone makes contactless cards less susceptible to fraud than magnetic stripe cards, because it is extremely difficult to produce a counterfeit contactless card.

The second layer of protection is additional security logic that can be programmed into the chip. Currently, the United States has adopted an implementation of contactless cards to achieve a high level

of security with the least impact on the current payment system infrastructure. U.S. contactless cards use dynamic data elements from the card and the terminal to produce a dynamic cryptogram that can only be authenticated by the card issuer or its agent. Use of dynamic data and a cryptogram component is the principle underlying EMV security; however, the U.S. dynamic cryptogram is not EMV compliant. The difference is in the type and amount of data used in the cryptograms, the amount of data that is passed to the host system, and additional risk management parameters that can be defined in an EMV card for offline transactions or authentication failure. Where EMV transactions require message modifications to the terminal, acquirer, and issuer host systems, the U.S. contactless implementation leverages space already available in the message protocol and only the contactless card reader or terminal needs to be changed. In some cases, an intelligent contactless reader can simply be added to an existing magnetic stripe POS terminal, and the additional reader can perform the functions required to accept a U.S. contactless card without having to change the terminal application.

Each payment brand uses a slightly different naming convention for their U.S. contactless cards and the dynamic cryptogram. However, in all cases, certain data on the card and the terminal change with every transaction to facilitate generating a unique cryptogram for every transaction. The authentication of the cryptogram assures the issuer that the card presented is authentic. If data is copied or intercepted at the reader, the data is already obsolete for future transaction attempts. If an attempt is made to use the data to produce counterfeit cards or replay a transaction, the dynamic cryptogram validation fails and the transaction is refused.

There have been reports in the media that sufficient sensitive data can be intercepted or captured from a contactless card to put the cardholder at risk of fraudulent transactions. Some data is passed in the clear and can be captured, but the dynamic data component that is linked to each card and each transaction guards against misuse of the data. In addition, the data stored on the chip is different from that stored on the magnetic stripe. As a result, data captured from a contactless chip cannot be used to produce a counterfeit magnetic stripe card.

Although the contactless approach used in the U.S. is different from that used in many EMV markets, the security features on U.S. contactless cards can also be leveraged when the cards are used outside the United States. This is ensured by the contactless POS terminals that have been deployed in EMV markets that also support the U.S. version of contactless. Due to the low infrastructure impact of the contactless technology deployed in the U.S., adding the U.S. contactless feature has virtually no impact on cost and complexity of the readers deployed outside the United States. The implication of this approach is that U.S. contactless issuers benefit from additional security on all transactions, including those taking place outside the U.S. It is therefore beneficial in the short- to medium-term that U.S. issuers and merchants continue to invest in deploying current contactless technology in order to maximize the security benefits for both domestic transactions and for those made overseas.

4.4 Logical Next Steps: Migration to EMV Cards

One significant advantage of contactless chip technology over magnetic stripe technology is that security can be incrementally increased over time. This is not the case for magnetic stripe cards. Contactless chip technology is based on a microprocessor which provides the flexibility to enhance security and makes possible a logical progression of increased security to combat ever more sophisticated attacks as they emerge.

Indeed, industry stakeholders (e.g., payment brands, industry bodies, issuers, processors) have launched several initiatives to define the next logical approaches necessary to further combat fraud. These efforts range from enhancement to the card as well as to terminal technologies, and further leverage important benefits from EMV. Given the scope and potential impact to issuers, acquirers, processors and merchants that some of these initiatives suggest, however, it begs the question of whether the U.S. payments industry should now consider a concerted effort to move the market to full, globally-interoperable EMV-compliant dual-interface chip cards and terminals. While moving the U.S. to full EMV-compliant cards and terminals is a long-term proposition, the timing may be right to stem growing concerns related to fraud and to reap the benefits of fully interoperable chip payment cards around the world.

4.5 Comparison of Security Features: U.S. Contactless Payments, EMV, and Magnetic Stripe Infrastructures

Table 1 compares the security features provided U.S. contactless payments with EMV payment cards and the existing magnetic stripe infrastructure and outlines the benefits of contactless payments.

Table 1. Comparison of U.S. Contactless Payments Security Features with EMV and Magnetic Stripe Cards

U.S. Contactless Payments Security Feature/Behavior	Comparison with EMV Implementation	Comparison with Magnetic Stripe Infrastructure	Contactless Payments Security Benefits vs. Magnetic Stripe
Cardholder typically maintains possession of a contactless payment card and taps the card on the reader, never relinquishing the card to a sales clerk.	EMV contact chip card is inserted into the reader slot by cardholder or handed to a sales clerk. Cardholder retains possession of contactless EMV chip cards and taps the card on a reader.	Magnetic stripe card is swiped by consumers in a multi-lane retailer or is inserted in a gas pump or ATM. Cardholders typically give their cards to a sales clerk in all other POS environments. The potential for skimming data from the card increases when the card leaves the cardholder's possession.	Provides better security to cardholders—no risk of skimming chip data by the sales staff. Provides a more hygienic way of payment—no physical contact.
Card is based on highly secure smart chip technology. Contactless chip card is extremely difficult to counterfeit.	Card is based on highly secure smart chip technology. EMV chip card is extremely difficult to counterfeit.	Magnetic stripe data can easily be skimmed from a card or stolen from non-PCI-DSS-compliant data network or storage. Skimmed card data can be used to create a counterfeit card.	Contactless chip card is extremely difficult to counterfeit.
Contactless card transaction produces unique data for every transaction that is a function of a secret key resident on the card and placed there by the card issuer.	EMV chip card transaction produces a unique transaction code that does not allow reuse or replay of transaction data.	Magnetic stripe card carries static data, which, if skimmed or stolen, can easily be used to make a counterfeit magnetic stripe card.	Transaction data cannot be reused/replayed for fraudulent transactions. Card data from contactless transactions cannot be used to create a fraudulent magnetic stripe card that can be used for a successful transaction.

U.S. Contactless Payments Security Feature/Behavior	Comparison with EMV Implementation	Comparison with Magnetic Stripe Infrastructure	Contactless Payments Security Benefits vs. Magnetic Stripe
Contactless card allows online card authentication.	EMV chip card allows authentication of the payment card for both online and offline transactions.	No card authentication is possible for ISO-standard magnetic stripe cards.	Fits well into the U.S. infrastructure (where almost all transactions are authorized online).

5 Conclusions

Fraud is a growing and ever-changing problem for the payments industry. As new payment technologies are introduced and new fraud prevention and detection techniques are implemented, criminals look for the new weakest point in the system to exploit. The current weakest link for card fraud is the magnetic stripe payments infrastructure, which, as other countries implement EMV-compliant chip cards and infrastructure, is increasingly being attacked in the U.S.

The industry has implemented a variety of both preventative and mitigating measures to deal with card fraud. Unfortunately, the vast majority of U.S. payment transactions still move the same static account numbers, authorization codes, and transaction information across the industry's private and semiprivate networks. While the networks that carry those data elements have changed—from dial-up to IP communications to wireless—the data hasn't.

The solution to the fraud problem is not better protection of data nor better fraud detection techniques alone. The solution is to incorporate dynamic data into payment transactions, so that stolen account or transaction information is rendered useless.

The U.S. payments industry has already made a major first step in this direction. Contactless payments, as currently implemented in the U.S., help reduce card-based fraud. Current contactless payment devices generate dynamic cryptograms, similar to those generated by EMV payment cards, and the existing payment network infrastructure—as it is—can handle the current cryptogram. Merchants, acquirers, processors, payment brands, and issuers have all implemented the changes needed to accept the current generation of contactless payment cards and dynamic data. Generation and verification of dynamic data reduce the possibility of skimming, merchant server attacks, and use of counterfeit cards. Use of dynamic data, plus other existing fraud detection techniques, provides an effective solution to card-based fraud without any changes to the current infrastructure. Every additional contactless transaction reduces the possibility of fraud.

To further the momentum of current contactless deployments, the U.S. payments industry needs additional infrastructure investment. Merchants, acquirers, and issuers need to continue to invest in infrastructure that supports dynamic authentication. Contactless payments have been delivering benefit to payments process participants since their introduction in 2004 through improved convenience, faster throughput, increased number and size of transactions, and greater customer satisfaction. By also providing a solution to card-based fraud, contactless payments delivers an even more compelling business case for the industry.

Planning for these investments should be undertaken now to determine the optimal distribution of cost over time. These plans should also include the eventual migration of the U.S. to globally-interoperable EMV cards and terminals. Once EMV-enabled, the United States will benefit from the same highly secure and globally interoperable payments infrastructure as the rest of the world.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Contactless and Mobile Payments Council to discuss how changes to the U.S. and global payments infrastructure are expected to affect card-based fraud in the United States and how different technologies can address this fraud. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Contactless and Mobile Payments Council members for their contributions. Participants involved in the development of this white paper included: Dynamic Card Solutions, First Data Corporation, Gemalto, Giesecke & Devrient, IBM, INSIDE Contactless, KeyPoint Consulting, MasterCard Worldwide, Visa Inc., ViVOtech

Special thanks go to the following individuals on the project team that developed this white paper:

- **Deborah Baxley**, KeyPoint Consulting
- **Philippe Benitez**, Gemalto
- **Guy Berg**, Dynamic Card Solutions
- **Brent Bowen**, INSIDE Contactless
- **Andrew Chen**, Visa Inc.
- **Gwen Dido,** IBM
- **William Gostkowski**, Gemalto
- **William Haughney**, IBM
- **Simon Hurry**, Visa Inc.
- **Mohammad Khan**, ViVOtech
- **Jan Lundequist**, MasterCard Worldwide
- **Cathy Medich**, Smart Card Alliance
- **Ken Moy,** MasterCard Worldwide
- **JC Raynon**, ViVOtech
- **Rona Simmons**, IBM
- **Brian Stein,** Giesecke & Devrient
- **Krista Tedder**, First Data Corporation
- **Charles Walton**, INSIDE Contactless
- **Martin Zeisel**, First Data Corporation

About the Smart Card Alliance Contactless and Mobile Payments Council

The Contactless and Mobile Payments Council is one of several Smart Card Alliance technology and industry councils. The Council was formed to focus on facilitating the adoption of contactless and mobile payments in the U.S. through education programs for consumers, merchants and issuers. The group is bringing together financial payments industry leaders, merchants and suppliers. The Council's primary goal is to inform and educate the market about the value of contactless and mobile payment and work to address misconceptions about the capabilities and security of contactless technology. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

Trademark Notice

7 Glossary

Address verification service (AVS)
A fraud prevention measure that attempts to verify the identity of the cardholder by asking the cardholder to enter the billing address for the account. Initially developed as a tool for mail order, telephone order, and e-commerce sales environments, it has been used in retail POS environments (typically with the cardholder entering the zip code) to provide additional cardholder verification.

AVS
See address verification service**.**

Card security code
Codes either written on the payment card magnetic stripe or printed on the card that are used by the financial payment brands for credit and debit transactions to protect against card fraud.

Card verification code (CVC) / card verification value (CVV)
Terms used by MasterCard and Visa for the card security codes used for credit and debit transactions to protect against card fraud.

Chip card
A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, chip cards have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a card reader. Chip card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, key fobs, subscriber identity modules (SIMs) used in GSM mobile phones, and USB-based tokens.

Contactless payments
Payment transactions that require no physical contact between the consumer payment device and the physical point-of-sale (POS) terminal. In a contactless payment transaction, the consumer holds the contactless card, device or mobile phone in close proximity (less than 2-4 inches) to the merchant POS terminal and the payment account information is communicated wirelessly (via radio frequency (RF)).

Contactless chip card
A chip card that communicates with a reader through a radio frequency interface.

CVC
See card verification code.

CVV
See card verification value.

Dynamic card security code
A security code which changes for each transaction, replacing the magnetic stripe-based card security code before the transaction is read at the POS.

Dynamic authentication data
Information that is used during a transaction to verify the card or the cardholder participating in the transaction and that changes from transaction to transaction.

EMV
Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

EMVCo
The organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for

Payment Systems. EMVCo is currently owned by American Express, JCB, MasterCard Worldwide, and Visa, Inc.

Magnetic stripe card
A plastic card that uses a band of magnetic material to store data. Data is stored by modifying the magnetism of magnetic particles on the magnetic material and is read by "swiping" the magnetic stripe through a reader.

Personal identification number (PIN)
A secret that an individual memorizes and uses to authenticate his or her identity.

PIN
See personal identification number.

Smart card
See chip card.

Static authentication data
Information that is used during a transaction to verify the card or the cardholder participating in the transaction and that does not change from transaction to transaction.