# The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options

*By Richard J. Sullivan*

Debit and credit card payments are convenient for consumers, widely accepted by merchants, and more efficient than paper forms of payments. But as cards have become the primary payment instrument in retail transactions, awareness of identity theft and concerns over the safety of payments has increased. For example, a recent data breach at Heartland Payment Systems compromised 130 million records of payment cards—the largest in a succession of security failures that have compromised growing numbers of payment records.

Like all forms of payment, cards have security vulnerabilities. Traditional forms of card payment fraud are still an important threat, but fraud resulting from unauthorized access to payment data appears to be rising. Payment providers are exploring options to protect sensitive data, such as the recently implemented payment card industry data security standard. But the damage from card payments fraud is a rising concern, and we are only beginning to get a sense of the dimensions of the problem.

As the central bank of the United States, the Federal Reserve has responsibility to ensure that payments are safe, efficient, and accessible.

---

*Richard J. Sullivan is a senior economist in Payments Systems Research at the Federal Reserve Bank of Kansas City. This article is on the bank's website at* ***www.KansasCityFed.org.***

Confidence in the safety of payments is particularly important. Thus far, the role of public policy has been to encourage the card payment industry to develop its own standards and procedures that limit fraud. Whether this policy stance is sufficient depends on the effectiveness of industry efforts to limit fraud in light of the dramatic shift towards card payments.

This article provides an overview of card payment fraud in the United States. The process for approving card payments depends to a large extent on information. Thus, criminals have a strong incentive to steal that information, leading to attacks on computer systems, data breaches, and ultimately payment fraud. Such criminal efforts are increasing in organization and scale. To assess the resulting damage, this article presents a preliminary estimate of the rate of card payment fraud in the United States. According to the estimate, card fraud is higher in the United States than in several other countries for which data are already available. While the U.S. payment industry is taking steps to combat payment fraud, progress has been slowed by conflicts of interest, inadequate incentives, and lack of coordination. The principal conclusion is that policymakers should monitor the card payment industry to see if it better coordinates security efforts, and if not, consider actions to help the industry overcome barriers to effective development of security.

The first section examines the information-intensive card payment approval process and the security vulnerabilities that emerge as a result of shifting to electronic forms of payments. The second section explores what we know about how criminals gather and use payments information to commit fraud. The section also addresses the monetary harm that fraud inflicts on participants in the payment system. The third section reviews several important initiatives, in the United States and elsewhere, designed to combat card payment fraud. It goes on to discuss the limited effectiveness of industry efforts to establish payment security standards on its own and the resulting policy concerns.

## I. EMERGING VULNERABILITIES OF CARD PAYMENTS

The primary aim of card payment security is to ensure that only payments authorized by the account holder are allowed. Vulnerabilities exist in the card payment approval process, however, that enable criminals to make fraudulent card payments. These vulnerabilities are related

to an information-intensive payment approval process. Criminals have begun concerted efforts to collect and exploit this information, especially targeting electronic records.

While traditional forms of card payment fraud (such as from lost or stolen cards) remain important, this section will focus on newer forms of payment fraud, which are often a result of breaches of personal information.[1] Large data breaches are especially damaging, and many of these breaches expose payment-related data. Criminals are specializing in activities to gather sensitive information (such as writing malevolent software or establishing fake Internet sites), to commit fraud, and to launder associated funds. These groups are international in scope and organize themselves in underground online markets where they can buy and sell services that aid in stealing data or perpetrating payment fraud.

## *Card payment approval and fraud*

Payment fraud occurs when someone gains financial or material advantage by using a payment instrument, or information from a payment instrument, to complete a transaction that is not authorized by the legitimate account holder.[2] In this definition, the lack of an account holder's authorization is the crucial distinguishing characteristic of payment fraud.[3] A card payment approval system screens transactions to limit fraud. The system authenticates the card, identifies the cardholder, and determines whether the transaction satisfies certain limits set by the card issuer or merchant.

Card issuers and merchants face numerous challenges in making a correct approval decision. The payment cards that issuers provide are not sufficiently difficult to counterfeit.[4] To accommodate merchants and consumers, card issuers continue to allow payments via mail order, the telephone, and now the Internet, with only the information from a payment card. Some merchants do not properly check payment cards for counterfeits or review signatures of cardholders. Some consumers write their personal identification numbers (PINs) on their payment cards or do not sufficiently protect their personal computers. Criminals take advantage of these and other vulnerabilities either to gather or to exploit information that lets them commit fraud.

The common underlying cause of these vulnerabilities is an information-intensive payment approval process.[5] Criminals have incentives

to gather and use the information to commit fraud. Because more information will generally lead to a more accurate approval decision, card issuers (and merchants) have an incentive to continuously expand the data on which they rely (Roberds and Schreft 2008). The result appears to be an escalating cycle of card issuers adding information to their databases and criminals devising ways to gather the information.

The recent transition to electronic payments processing has opened new avenues for gathering payment card data. Small handheld card readers are used in locations such as restaurants to read and save card information.[6] A disguised card reader can be fit over a legitimate slot on ATMs or other payment terminals to electronically capture card information (skimming). Video cameras placed in hard-to-detect locations can capture PIN numbers.[7] Criminals also exploit the Internet by, for example, sending out millions of e-mail messages that trick a small number of recipients into revealing sensitive account or card information (phishing). On a larger scale, hackers can penetrate computer systems and steal information where it is stored and transmitted.

Stolen data circulate among criminals in underground Internet markets. Evidence shows that stolen credit card information is most commonly available at a cost of $.85 to $30 per card number (Symantec). Bank account information is the second most common type of data available, at a cost of $15 to $850 per account number. Other information, such as full identities, online auction accounts, email accounts, and passwords are also for sale.

More broadly, a specialized electronic payment fraud industry appears to be growing. Security experts argue that since 2004 "criminals who were carrying out card fraud and attacks on electronic banking got organized, thanks to a small number of criminal organizations and a number of chat-rooms and other electronic fora, where criminals can trade stolen card and bank account data, hacking tools and other services" (Anderson and others). Elements of this industry specialize in activities such as writing malware, hacking databases, organizing underground electronic marketplaces, and laundering money.

### *Data breaches*

Criminals exploit card information from any source to commit card payment fraud. But data breaches deserve special attention be-

cause electronic processing of payments provides new means of accessing data and can substantially increase the amount of data that is compromised. Organizations do not always report data breach incidents but recently the public record has become more complete as states have implemented laws that require disclosure.[8]

Data breaches occur when individuals gain unauthorized access to digitized information. Until recently, insiders of an organization were mostly responsible for data breaches, but with the arrival of the Internet, outsiders gained access to this information. The majority of publicly disclosed data breaches are committed by outsiders, although insiders account for a significant share (Table 1). Most incidents are a result of stolen laptops or desktop computers, followed by exposure of information on the Internet or e-mail and by hacking.

Since 2005, at least 2,221 data breaches have been made public. The number of breaches rose until the middle of 2006, which can be partly attributed to data breach notification laws (Chart 1). The number of publicly announced breaches fell, then rose, and fell again from mid-2006 to mid-2009. For about a year it has been fairly steady at a relatively low level of about 30 per month. The recent decline in breaches may have multiple causes, such as increased difficulty in tracking the data breaches due to waning news organization interest or better security of data.[9]

A recent example shows the damage that can result from a data breach. In November 2008, computer hackers broke into RBS Worldpay, a U.S. payment processing subsidiary of the Royal Bank of Scotland, and gained access to data on 1.5 million cardholders (Gorman and Perez). They distributed the information to a worldwide network of confederates. While these "cashiers" counterfeited payment cards, the hackers modified computer systems at RBS Worldpay to raise the available funds on the cards and the limits on the cash that could be withdrawn at ATMs. Then, over the course of just 12 hours, the cashiers went on a cash withdrawal spree, obtaining $9 million from 2,100 ATMs in some 280 cities.

While this is a large-scale example, lesser attacks occur on a regular basis. According to one law enforcement official, more money is stolen from banks by data breaches than by robbery (Gorman and Perez).

*Table 1*

## CHARACTERISTICS OF PUBLICLY DISCLOSED DATA BREACHES IN THE UNITED STATES

| | | |
|---|---|---|
| Source | Outsiders | 64% |
| | Insiders-accident | 21% |
| | Insiders-malicious | 7% |
| Type | Stolen laptop or computer | 27% |
| | Exposure on Internet or e-mail | 17% |
| | Hack | 16% |
| | Documents lost in mail or on disposal | 9% |
| | Scams and social engineering | 8% |

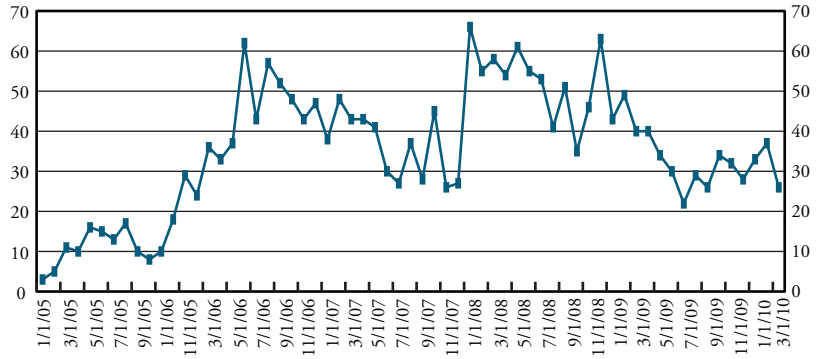
Notes: Statistics based on 2,318 incidents since 2000 tracked by the Open Security Foundation (datalossdb.org, accessed on March 25, 2010). The incidents compromised personally identifiable information such as credit card numbers, social security numbers, names and/or addresses, financial account information, financial information, date of birth, e-mail addresses, medical information, and miscellaneous.

Sources other than those listed above include insiders and unknown.

Types other than those listed above include lost media, stolen documents, lost tapes, lost documents, lost computer drives, stolen media, stolen computer drives, lost laptops, virus, disposal of computer tapes, missing laptops, disposal of computer drives, lost computers, disposal of computers, and unknown.

*Chart 1*

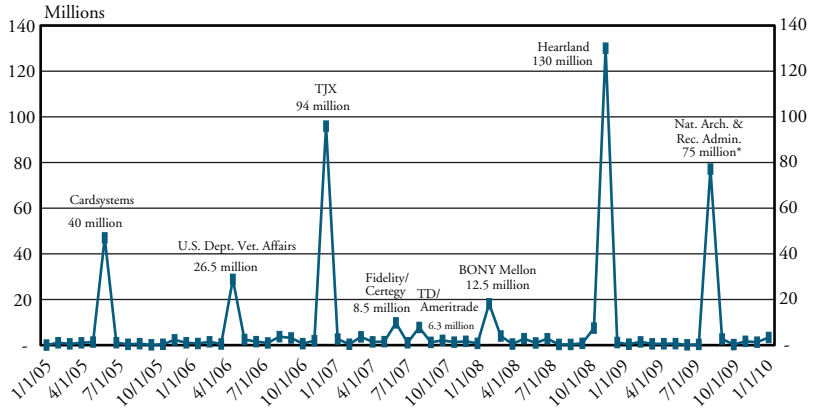
## PUBLICLY DISCLOSED DATA BREACH INCIDENTS IN THE UNITED STATES




Notes: Statistics based on 2,221 incidents that compromised personally identifiable information since 2000 tracked by the Open Security Foundation (datalossdb.org, accessed on April 21, 2010).

*Chart 2*

## RECORDS COMPROMISED FROM PUBLICLY DISCLOSED DATA BREACHES IN THE UNITED STATES




Notes: Statistics based on 2,221 incidents that compromised personally identifiable information since 2000 tracked by the Open Security Foundation (datalossdb.org, accessed on April 21, 2010).
*Data at the National Archives and Records Administration may have been compromised when a defective hard drive was sent to be recycled without first being destroyed. The hard drive contained 70 million records of sensitive information of veterans (Singel). It is not clear that the information reached unauthorized individuals. While some may not consider this a data breach, it is included in Chart 2 because it is in the Data Loss Database.

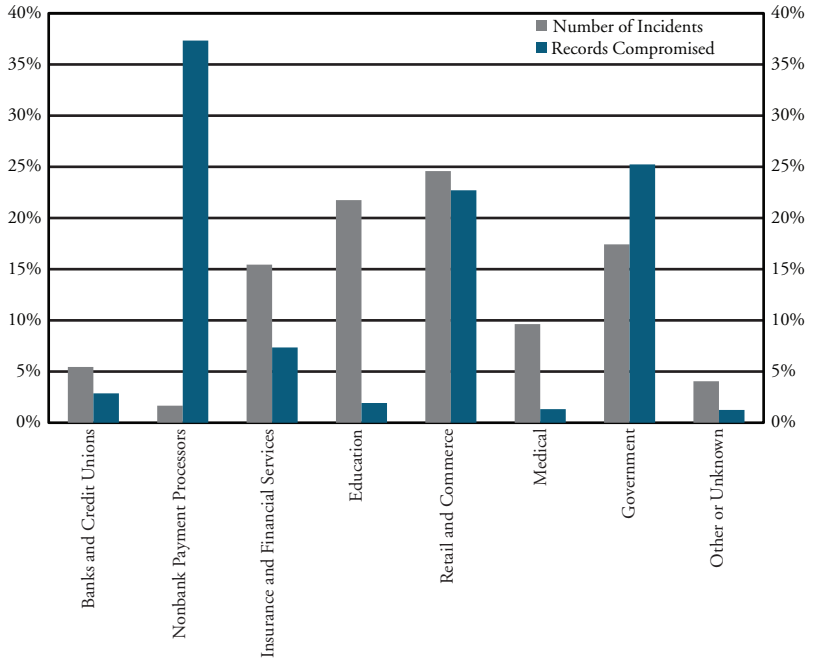
The damage resulting from a breach may relate more to the records compromised than to the number of breaches. Since early 2005, at least 494 million records of sensitive information have been compromised in publicly announced data breaches. Just eight large data breaches have accounted for 79 percent of the compromised records (Chart 2). Because large incidents occur infrequently, it will take time to know if their occurrence has slowed.

A closer look at the origin of data breaches shows that the distribution of incidents and records compromised varies considerably across sectors of the economy. Among the sectors shown in Chart 3, nonbank payment processors account for a small share of breach incidents but are responsible for the largest share of records compromised. Retail and commerce account for the largest share of incidents and the third-largest share of records compromised. The education sector stands out with a significant share of incidents but few compromised records. Government entities have a significant share of both. Banks and credit unions have a good record by comparison.

*Chart 3*

## SHARE OF INCIDENTS AND RECORDS EXPOSED

*Publicly disclosed data breaches, U.S., Jan. 2005 to March 2010, by sector*




Notes: Statistics based on 2,221 incidents that compromised personally identifiable information since 2005 tracked by the Open Security Foundation (datalossdb.org, accessed on April 21, 2010), and author's calculations.

Some tentative conclusions can be made from the record of publicly announced data breaches. First, much exposure results from a relatively few large breaches. Second, sectors that process or store payment data, such as nonbank payment processors and retailers, are major targets. Third, nonbank payment processors have avoided a large number of potential attacks, but when their security systems are successfully penetrated, exposure can be extensive.[10] Fourth, the relatively good record of banks and credit unions, despite their storage of data useful for payments fraud, suggest they have done a good job protecting sensitive data.

### *Links from stolen data to fraud*

It is challenging to track stolen data to its misuse. After a data breach, determining what information has been compromised is difficult. In the case of large breaches involving millions of payment records, criminals

may not be able to take advantage of the data quickly and may exploit it over a period of time. As a result, consumers may not be aware that a data breach has led to fraudulent use of their payment card.[11]

Two common ways to use stolen data for card payment fraud are to purchase goods from Internet, mail order, or telephone merchants or to counterfeit a payment card and use it in an ATM cash withdrawal or in a face-to-face transaction at a point-of-sale (POS). Internet, mail order, or telephone transactions, referred to as card-not-present (CNP) transactions, are vulnerable to stolen data because payment cards cannot be inspected.

A recent study of banks found that, between 2006 and 2008, fraud losses from counterfeit cards rose on each of signature debit, PIN debit and ATM transactions (American Bankers Association 2009). Costs related to online payments fraud (lost sales, direct payment fraud losses, and fraud management) rose steadily from 2000 to 2008 (Cybersource 2010). The 2009 costs declined somewhat, to $3.3 billion (1.2 percent of sales revenue), in part due to the economic slowdown. Unfortunately, we do not have good statistics on sources of credit card fraud, which is twice as likely as debit card fraud (Javelin).

These statistics are only suggestive because the information used for the fraudulent transactions do not necessarily come from data breaches. More direct information is available from a 2008 survey of banks. The survey reports that 43 percent of respondents suffered payment fraud losses due to data breaches, up from 22 percent in 2006 (American Bankers Association 2009). The increase is significant because, as shown below, banks bear the largest share of card payment fraud loss.

There is also some evidence on what characteristics of data breaches are more likely to lead to payment fraud. Misuse of data was more likely if it was identity-level information, such as Social Security numbers, and obtained through deliberate hacks or stolen computer hardware (ID Analytics). The potential for fraudulent use of stolen data was less related to the size of a data breach than to the resources available to hackers.

An indirect consequence of stolen data and associated fraud is public concern over the safety of payments. News reports of data breaches and identity theft have become routine. To protect themselves, consumers and businesses must use security software (firewall and antivirus software, etc.) on their personal computers to prevent criminals from

stealing personal information directly or from installing malware that allows secret control of the computer.[12] These attacks on personal computers contribute to consumer anxiety and suspicion about the safety of some forms of payment.[13]

In short, attention has turned to new threats to card payment security, such as stolen payment data obtained in data breaches and other sources. Stolen data is linked to card payment fraud by a complex and developing chain. Preventing hackers from breaching computer security and committing fraud is widely viewed as a major challenge. The bottom line, however, is that payment participants bear a significant loss. The next section reviews the evidence on losses caused by card payment fraud.

## II. HOW LARGE ARE PAYMENT CARD FRAUD LOSSES?

To gauge the extent of debit and credit card fraud, this section examines the direct monetary losses. It first reviews two alternatives for measuring card fraud losses and the comparability of the measurement. It then presents a new estimate of the fraud loss rate (total fraud losses divided by the value of total card payments) in the United States for 2006. The estimate suggests that the loss rate was higher in the United States than in Australia, France, Spain, and the UK. Finally, the section discusses factors that explain the international differences. For the United States, significant factors include continued reliance on older payment card technology, the use of signatures to identify the cardholders, and a highly developed Internet economy.

### *Alternatives for measuring fraud losses*

One measure of the damage caused by card payment fraud is the value of associated losses for all participants in various card payment networks.[14] In recent years, several countries around the world have begun to regularly publish such statistics (Sullivan 2009). The data that feed these statistics originate in financial institutions when account holders report fraudulent transactions. The financial institution puts a marker in the computer record of the transaction, indicating that it was reported fraudulent. Periodic summary statistics on the number and value of fraudulent payments can then be easily generated from computer records. Typically, an industry organization gathers data from

card issuers and networks to calculate aggregate statistics. Often, information on the sources of payments fraud is also reported.

These statistics are unavailable for payment card fraud in the United States, but an alternative method can provide comparable statistics. The estimate of U.S. fraud presented here is based on the sum of direct losses borne by card issuers, POS merchants, and merchants in Internet, mail order, and telephone transactions.[15] This estimate should be comparable to those from other countries because the value of a fraudulent payment when first reported should approximate the sum of the losses of payment participants who ultimately bear the loss.

The person or merchant who first reports a fraudulent payment will not necessarily bear all or even part of the loss. For example, a merchant typically receives a payment guarantee by the card issuer for a properly approved payment where the card is present at the time of purchase. In this case, the loss is borne by the financial institution that issued the payment card. While the merchant may first report the fraudulent transaction, it does not bear the loss.[16]

Some merchants, however, do bear losses due to card payment fraud. Merchants who accept CNP payments cannot inspect cards for authenticity or confirm that a customer has possession of the card. As a result, CNP transactions are not generally guaranteed. Relative to their sales, card payment fraud losses fall most heavily on Internet, mail order, and telephone merchants because nearly all of their payments are CNP transactions.

Another important example concerns consumer payments. A consumer might find a $200 fraudulent debit card payment on his monthly account statement. U.S. regulations say that if the consumer reports the transaction to his financial institution in a timely manner, the consumer would be responsible for no more than $50 of the value of the transaction, and the financial institution would lose the remaining $150.[17] In practice, however, consumers often avoid any of the cost of a fraudulent card payment. All of the major credit card networks provide zero liability to cardholders in cases of fraudulent payments.[18] As a result, consumer losses are excluded from the estimates in this section.

Finally, the estimated fraud losses for the United States reported here relies on the best sources available and informed assumptions. By comparison, other countries have developed and refined their methods

for collecting data and reporting fraud statistics over several years. As a result, the U.S. statistics should be viewed as preliminary and may be subject to change as more information becomes available.

### *Fraud losses in the United States and other countries*

In 2006, total U.S. fraud losses are estimated at $3.718 billion (Table 2). Card issuers paid the largest dollar cost, followed by POS merchants and Internet, mail order, and telephone merchants. Internet, mail order, and telephone merchants had the lowest cost of card payment fraud, but the annual sales volume of POS merchants was approximately 30 times that of Internet, mail order, and telephone merchants. Fraud as a share of sales volume was much higher for Internet, mail order, and telephone merchants than for POS merchants.[19]

The shares of fraud losses in the United States in 2006 were divided between card issuers (59 percent) and merchants (41 percent). For comparison, losses in France are shared more equally. In 2007, 51 percent of French losses were attributed to issuers and acquirers and 46 percent to merchants (Observatory for Payments Card Security 2007). This comparison is tentative, however, because of the preliminary nature of the estimate of U.S. losses. Additional research will be needed to further refine the distribution of fraud losses.

Table 3 compares loss rates on payment card transactions in the United States to losses in Australia, France, Spain, and the UK.[20] The United States had the highest rate of fraud losses in 2006; Australia and Spain had the lowest; and France and the UK were in the middle. The extent of the difference is significant: The highest rate of fraud is almost four times that of the lowest.

While there is some uncertainty in the calculations, the difference between U.S. fraud rates and those in other countries, shown in Table 3, is sufficiently large that added accuracy would not close the gap—but probably increase it. First, the U.S. statistics are based on net losses for those who bore the loss, while other countries use the gross losses when the fraudulent transaction is reported. The difference between net and gross is the amount of funds recovered or prevented from being fraudulently transferred. If the estimate for the United States were based on gross losses, the difference would be greater. Second, conservative as-

*Table 2*

## FRAUD LOSSES ON DEBIT AND CREDIT CARD PAYMENTS UNITED STATES, 2006

| Card issuers | *billions* | Share of total loss |
|---|---|---|
| PIN debit | $0.028 | |
| Signature debit | $0.337 | |
| Credit cards | $1.240 | |
| ATM withdrawals | $0.397 | |
| **Total issuer losses** | **$2.002** | **59%** |
| Merchants | | |
| POS | $0.828 | |
| Internet, mail order, and telephone | $0.568 | |
| **Total merchant losses** | **$1.396** | **41%** |
| Total losses | $3.718 | |

Note: See Appendix for sources and details.

*Table 3*

## FRAUD LOSS RATES ON DEBIT AND CREDIT CARD PAYMENTS, 2006

| | Loss per $100 |
|---|---|
| Australia | $0.024 |
| France | $0.050 |
| Spain | $0.022 |
| UK | $0.086 |
| U.S. | $0.092 |
| U.S. card issuers only | $0.054 |

Note: See Appendix for sources and details.

sumptions are generally used to calculate the losses of U.S. merchants. More realistic assumptions would likely widen the gap as well.

### *Why fraud loss rates differ*

The cross-country differences in fraud rates are due to a number of factors, including the mix of payment cards in use, transaction authorization systems, the types of payments made using cards, evolving security standards, and the use of older card technology that has relatively weak security features.

The rate of fraud is lower on PIN debit cards than on signature debit cards (Pulse). As a consequence, countries that rely more heavily on PIN codes to authenticate payment cards will have less payment fraud. In Australia, for example, approximately 90 percent of debit transactions in 2006 used PIN codes, compared to only about 40 percent in the United States.

The quality of transaction authorization systems is also important. Both the Spanish and Australian payment networks have strong reputations for the use of transaction history analysis to help identify and avoid fraudulent transactions.

Another factor contributing to the difference in fraud rates is the extent of Internet, mail order, and telephone shopping, where relatively risky CNP transactions are necessary. A recent European Commission study showed that only 20 percent of individuals ordered goods over the Internet in Spain, compared to 57 percent in the UK (EC Staff Working Document). A 2008 survey of U.S. consumers found that 83 percent of them made purchases on the Internet (Hitachi). Thus, the relatively high rate of card fraud in the United States and in the UK is likely due, in part, to more fully developed online commerce.

Yet another factor contributing to cross-country differences in fraud rates is evolving security standards that help to prevent debit and credit card fraud. For example, "chip-and-PIN" payment cards have an embedded computer chip and require use of a PIN to initiate a transaction. These cards are more secure because they better protect data used to authorize a payment, and they make it difficult to counterfeit a payment card. These cards are being adopted in many countries around the world. Chip-and-PIN cards have been successful at reducing fraud

in face-to-face transactions, ATM withdrawals, and from lost or stolen cards (UK Cards Administration).

In countries that adopt chip-and-PIN cards, experience shows that fraud will migrate to payment types with relatively weak security. This occurs because issuers of chip-and-PIN cards also add magnetic stripes to their cards to allow backward compatibility with older transaction equipment. The magnetic stripe allows fraudsters to use information from a chip-and-PIN card to counterfeit cards for use in locations that continue to accept such cards. Prior to the adoption of chip-and-PIN cards, about 18 percent of fraud on counterfeit cards of UK issuers occurred on transactions outside of the UK, but today it is over 80 percent (APACS). Much of this growth has been on transactions in the United States, where magnetic stripes are still used on payment cards.

To sum up, the United States has a higher card fraud loss rate than Australia, France, Spain, and the UK. International differences are due to a number of factors, including underlying card payment technology and security standards. For the United States, important factors that lead to a relatively high fraud loss rate include a comparatively weak approval process for debit and credit card transactions and a highly developed Internet economy.

## III. THE WAY FORWARD

Led by various segments of the industry in the United States and elsewhere, several initiatives to further protect card payments are under way. Outside the United States, card issuers and networks are implementing new card technology and publishing payment fraud statistics. Projects in the United States include enhancing data security standards, supplementing approval systems of contactless payment cards, developing methods to encrypt payment data, and disguising card numbers. While these are positive steps, barriers remain, such as conflicts of interest, inadequate incentives, poor governance, and potential redundancy. U.S. policymakers face mixed signals on how well the card payment industry controls payment fraud. On one hand, considerable efforts are aimed at reducing fraud. On the other, some initiatives appear redundant, new security standards are adopted slowly, and the rate of card fraud losses is relatively high.

### *Industry initiatives*

A major initiative occurring in other countries is the implementation of the EMV standard for payment cards. EMV is an acronym for the card schemes Europay, MasterCard and Visa, but the standard has also been accepted by American Express, Discover, and JCB.

The EMV standard defines technical rules and protocols for payment cards that use computer chips. The standard has some flexibility, allowing card issuers to adopt various configurations for their cards that best fit their business needs. The chip-and-PIN card mentioned above is an example and is currently the most common implementation of the EMV standard. Chip-and-PIN cards are fully implemented in a few countries, but many other countries, including Canada and Mexico, are either in transition to chip-and-PIN or plan to adopt it in the near future. Chip-and-PIN payment cards have proven to be very good at preventing certain types of fraud, such as on lost or stolen cards. In countries where merchants will only accept these cards, counterfeit fraud has fallen as well.

Another initiative that other countries are pursuing is the collection and publication of payment fraud statistics. These statistics provide guidance for the card industry in its efforts to combat fraud. After implementation of chip-and-PIN, for example, statistics revealed to UK issuers that fraud on their cards was migrating to areas of relative security weakness. Specifically, CNP fraud in the UK and counterfeit card fraud outside of the UK grew rapidly. The information helped the industry take steps to counter these sources of fraud, and it appears the efforts have had some success. Total fraud losses on UK-issued payment cards fell 28 percent in 2009 over the previous year, a decline partly attributed to sophisticated fraud detection screening and to fraud prevention tools applied to online shopping (UK Cards Association).

In the United States, the major credit card companies are leading the most significant recent initiative to improve security and control fraud in card payments. While the card companies have long maintained their own security standards, a cooperative effort in 2004 between Visa and MasterCard led to a common standard. Other card companies joined the effort, and in 2006 the group formed the Payment Card Industry (PCI) Security Standards Council to oversee the

standard. Card companies themselves manage compliance validation and enforcement.

The PCI Council oversees several industry-wide standards. The most important is the PCI Data Security Standard (PCI DSS), which helps merchants and payment processors protect sensitive data. This goal is accomplished by creating secure networks, strong access controls, data encryption, computers protected with firewalls and antivirus programs, and security policies designed to establish an effective internal control environment.[21]

Data breaches and their consequences have led elements of the U.S. payment industry to explore ways to improve card payment security. Card issuers have been deploying contactless payment cards, which have a small radio to transmit card information to a payment terminal. Because it is difficult to counterfeit these cards, they are considered more secure than magnetic stripe cards. Issuers are considering an upgrade to EMV-compliant contactless cards, which will use a cryptogram (an encrypted identifying number for the transaction) to allow the card issuer to check the authenticity of the payment card and the uniqueness of the transaction.

Two initiatives are being developed in the merchant community in cooperation with payment service providers. One initiative targets a weakness in the PCI DSS, which requires encryption of sensitive card data when it is transmitted over public networks, but not when transmitted over private networks. Merchants are investigating "end-to-end encryption," which would encrypt payment data over the entire communications channel from the point-of-sale terminal to the card issuer (Hernandez). Another initiative disguises a card account number by replacing it with a token number. This "tokenization" would occur after a card payment has been authorized so that a merchant can store the transaction information without having to store the card account number (Taylor). Merchants can retrieve the card account number for later processing, if needed. Both of these options could make merchant and processor computer networks less of a target because they would not store or transmit sensitive payment card information in forms that would be useful to hackers.

### *Barriers to improving card payment security*

For the private market to find a socially optimal level of security, it must first overcome significant barriers (Roberds and Schreft 2009). Efforts to improve card payment security by one member of the network may benefit other members, just as one member's security breach may harm others.[22] But because one member of the network has no incentive to take account of the external benefits or costs of others, security for the network is less than optimal. Further, conflicts of interest can arise over the appropriate level of effort to enhance security. Some members will prefer relatively little effort, leaving the security of the entire network subject to its weakest links.

An answer to this dilemma is to pursue security efforts in a collective and comprehensive manner. Payment networks, for example, require membership to access network services. The threat of fines or expulsion makes members more likely to abide by rules regarding security and other operational matters (Braun and others).

Conflicts of interest can also complicate the development of security standards. Technically, standards would be more effective if members of the network determined them cooperatively. For example, security engineers recommend finding the most effective control points in the network to provide adequate security (Moore and others). But if each member of the payment network "goes it alone" and works only with its own control points, then it may be passing up effective security options that lie elsewhere in the network.

Research on standard-setting has found that governance is a key to success. Success is more likely if the governance structure includes all of the various interests in the network. The standards themselves need to be effective yet flexible enough to satisfy competitive interests. If done correctly, the process will promote compliance because all participants have a stake in the outcome (Steinfeld and others). Even then, the governance structure must also address issues such as intellectual property rights and provide a way to lessen the tendency of vested interests to block progress (Greenstein and Stango).

The International Organization for Standardization (ISO) uses a model of cooperation to coordinate international security standards for payments. In the United States, the affiliated American National Standards Institute's (ANSI) X9 committee is responsible for standards

in the payments industry (Sullivan 2008). The PCI DSS and EMV standards are not developed in these standard-setting organizations. Instead, they use a centralized model controlled by the card issuers and networks. The centralized model may allow security standards to be developed rapidly, but perhaps at the expense of adoption.[23] Only half of the largest U.S. merchants met the PCI compliance deadline of September 30, 2007.[24] Similarly, many European retailers have been slow to achieve PCI compliance (Leyden).

Implementing the PCI DSS has also been controversial. Merchants and processors face significant costs of compliance and question the benefits they receive (Mott).[25] The standards themselves have been criticized because they do not address card network rules that require merchants to store card information to resolve disputed transactions or facilitate refunds.[26] In addition, some merchants who have been certified as compliant have still been the victims of successful security breaches, raising concerns about the quality of the standard.[27]

### *Considerations for policymakers*

An important question concerns how well the payments industry as a whole can meet the challenge of protecting sensitive information. Policymakers can take some comfort that a significant amount of private sector activity is trying to find a solution to data breaches and associated payment fraud. By exploring several alternatives, the market may be able to sort out the most effective and efficient ways to protect sensitive card data.

Barriers to improving card payment security, however, may be higher in the United States than in many other countries. Coordination is particularly difficult, with over 18,000 federally insured depository institutions that offer deposit services and over 1 million retail establishments. In addition, the United States has a history of depending on paper checks for retail payments, which has a different security profile than electronic payments. The major shift to electronic payments is relatively recent, and developing appropriate security standards is in its first stages. The PCI Council is a framework for coordination, but it is too early to know whether its practices effectively balance the interests of cardholders, merchants, processors, and card issuers (box).

## GOVERNANCE OF THE PCI COUNCIL

The PCI Council is owned by the five major credit card companies, and its executive committee consists of representatives from each of the companies. The executive director and chief technology officer of the council each have extensive experience in credit card companies.*

The council's membership consists of over 500 companies, including financial institutions, payments associations, merchants, equipment manufacturers, software developers, and payment processors. These members can vote for representatives on a board of advisors. But whether this broad membership provides meaningful influence is unclear. A letter sent by several merchant groups to the PCI Council in June 2009 that recommended several changes to the PCI DSS suggested that many merchants in the United States would like to have more influence on the design of card payment security standards.**

The PCI Council is a step forward because it has standardized security across the five major card companies. Whether it can also incorporate the interests of the wider payment community is unclear. The council is currently directing a revision to the PCI DSS (expected to be released at the end of September 2010). Participating organizations and stakeholders provided feedback on the current standard through October 31, 2009, which the council has been reviewing. The extent to which the PCI Council balances the interests of all stakeholders in the credit card industry will go a long way toward determining the success of the revised standard.

* See *https://www.pcisecuritystandards.org/index.shtml* for more information about the PCI Council.

** "Merchant Trade Groups Come Together to Advocate for Changes to Data Security Standards," *Smart Card Trends*, June 10, 2009.

Regardless of the reasons, several signs suggest that lack of coordination in the payments industry has impeded security improvements. First, once fully developed, end-to-end encryption, tokenization, and payment messages augmented by cryptograms may all provide more security. But, to the extent that they each make attacks on card networks less attractive, they appear to be redundant (Smart Card Alliance). If so, they are competing technologies that are expensive to develop and implement. The potential payoff to effective coordination of standard-setting is the ability to choose what may be the best option for all members of the payment network and to accomplish common goals before considerable investment is made in unneeded technology.

Second, slow adoption and disputes over the design of the PCI DSS suggest that development of the standard is one-sided, favoring issuers over merchants. This should concern policymakers because effective payment security has two parts: the security standard and its adoption. If members of the payments industry do not feel it is in their self-interest to adopt a new security standard, they may adopt it slowly, and thus overall protection of payments suffers.

Third, the rate of fraud on U.S. card payments is relatively high. Lower rates of card payment fraud have motivated the payments industry in other countries to take the major step of adopting payment smart cards. But a high rate of fraud has not led to U.S. adoption of payment smart cards. It may be that payment smart cards are not the best solution for U.S. fraud prevention, but an alternative, comprehensive, and coordinated solution is not being considered.

Finally, reining in payment fraud in the United States is hampered by a lack of detailed, consistent, and periodic data. In a time of profound changes to the retail payment system, such information is crucial. Existing data have quality issues and inconsistent availability, making it difficult to identify what strategies the industry and policymakers should pursue. Producing better statistics would require some effort and cost, but most of the basic data already exist in the information systems of payment providers. Set-up costs would be required to standardize reporting and to establish an entity to compile data and regularly report statistics.[28] Other countries have not found this system to be overly burdensome.

## IV. SUMMARY

In the United States, fraud loss rates on debit and credit card transactions are higher than in Australia, France, Spain, and the UK. The main vulnerability is that fraudulent payments can be made with just a few pieces of information that the payment card industry uses in its payment approval process. Hackers have strong incentives to gather this information, leading to serious data breaches. The industry is moving to improve card payment security, but there are indications that their efforts could be more effective.

To guard against excessive fraud losses and to ensure confidence in card payments, policymakers need to monitor developments in card payment security. First, will card payment security continue to evolve without the benefit of industry-wide statistics on the level and sources of fraud losses? These statistics would help to determine whether the industry continues to tolerate a relatively high rate of fraud. Second, will the card payment industry move toward more coordination of security efforts? Such coordinated efforts have been successful in the Automated Clearing House system, another electronic payment system that has grown rapidly in recent years (Braun and others). If not, policymakers might consider a more active role to help the payments industry overcome barriers to effective coordination of security development.

## APPENDIX: SOURCES AND METHODS

### *Calculation sources and details*

The goal of the calculations is to obtain comparable estimates of fraud losses to all payment participants on payment cards issued by domestic institutions.

**Australia:**

Fraud rate = (ATM and debit card fraud losses+credit card fraud losses) / (ATM and debit card transaction value+credit card transaction value)

.000239 = ($14.4 million+$85.3 million)/($186.3 billion+$230.7 billion)

= 2.39¢ per $100 transaction value

**Source:**

Australian Payments Clearing Association (APCA) Media Release, "Payments Fraud in Australia," December 15, 2008.

**France:** .

Fraud rate = Total fraud losses/Total transaction value (see table below)

.000500 = €186.1 million / €372.5 billion

=5.0¢ per $100 transaction value

**Source:**

Observatory for Payment Card Security (OPCS), Annual Report, 2006.

| | | Debit, ATM, and credit | |
|---|---|---|---|
| Scheme | Transaction type | Fraud losses | Transaction value |
| Four party | French issuer, French acquirer | €100,475,400 | €331,270,000,000 |
| Four party | French issuer, Foreign acquirer | €73,835,500 | €15,140,000,000 |
| Three party | French issuer, French acquirer | €9,147,180 | €24,340,000,000 |
| Three party | French issuer, Foreign acquirer | €2,593,910 | €1,720,000,000 |
| Total | | €186,051,990 | €372,470,000,000 |

**Spain:**
.000224=2.24¢ per $100 transaction value
**Source:**
ServiRed, *Annual Report*, 2007.

**UK:**
POS retailer fraud losses=total fraud losses in 2004*(APACS fraud on POS transactions for 2006/ APACS fraud on POS transactions for 2004)
= £14 million*(£72.1 million/£218.8 million)
= £4.6 million
Online retailer fraud losses=total fraud losses in 2004*(APACS fraud on CNP transactions for 2006/ APACS fraud on CNP transactions for 2004)
= £14.1 million*(£212.7 million/£150.8 million)
= £19.9 million
Fraud rate
= (fraud losses reported by APACS + POS retailer fraud losses + Online retailer fraud losses)
/ (card purchase transaction value + value of ATM withdrawals)
.000912= (£427 million+£19.9 million+£4.6 million)/(£315.5 billion+£179.8 billion)
=9.12¢ per $100 transaction value

**Notes:**

APACS reports only provide the value of fraud; the value of transactions is taken from separate reports on payment clearing and settlement. Levi, et al. (2007, p. 24) states that losses for transactions not fully authorized by card issuers are excluded from APACS data. They also report that in 2004 retail fraud losses not included in the APACS data amounted to £14.1 million for POS merchants and £14 million for CNP transactions. Because of the transition to chip-and-PIN payment cards, POS merchant card fraud declined and CNP fraud increased from 2004 to 2006. To get an estimate for 2006, the 2004 figures are adjusted using APACS data (from 2004 and 2006) for fraud on face-to-face and CNP transactions.

**Sources:**

Association for Payment Clearing Services (APACS), "Quarterly Statistical Release," May 15, 2009.

APACS, "2008 Fraud Figures Announced by APACS," Press Release, March 19, 2008.

Michael Levi, John Borrows, Mathew H. Fleming, and Matthew Hopkins, "The Nature and Economic Impact of Fraud in the UK," Report for the Association of Police Officers' Economic Crime Portfolio, February 2007.

**United States:**

Card issuer losses on credit card transactions are the total value as reported by issuers. For other transactions, losses are calculated from loss rates on categories of payments (PIN debit, signature debit, and ATM transactions) multiplied by the total value of these transactions.

**Card issuers:**

Credit card losses: $1.24 billion

Debit and ATM cards:

total losses=(PIN debit losses+signature debit losses+ATM withdrawal losses)

$762 million = (.000085*$333 billion)+(.000505*$666 billion) +(.000686*$579 billion)

Total credit, debit and ATM card loss=$2.0 billion=$1.24 billion+$762 million

**POS merchants:**

total losses=(PIN debit losses+signature debit losses+credit card losses) *share of card payments on cards issued by domestic financial institutions

$0.829 billion = [(.0001*$333 billion)+(.0003*$666 billion)+(.0003* $2.1 trillion)]*0.96

**Internet, mail order, and telephone merchants:**

Total losses=Total Internet, mail order, and telephone fraud loss* proportion of loss due to chargeback transactions

$0.9 billion=$183 billion*.014*.35

**Loss rate:** (Fraud losses reported by card issuers+POS merchant fraud losses+Internet, mail order, and telephone merchant fraud losses)
/ total value of debit and credit card transactions

.000924= ($2.0 billion+$0.829 billion+$0.9 billion)/$3.1 trillion = 9.2¢ per $100 transaction value

**Notes:**

Loss rates are for actual debit and credit card fraud losses at domestic card-issuing financial institutions; at POS retail establishments; and at Internet, mail order, and telephone merchants. Issuer credit card losses are from "Credit Card Fraud—U.S.," (2007). Debit card losses are based on a survey of debit card issuers (Pulse 2008). Debit card loss rates are an average of statistics reported for 2005 and 2007. The loss rates are applied to estimates of the value of PIN and signature debit card transactions for the United States (Gerdes 2008) to obtain total losses.

Losses for Internet, mail order, and telephone merchants are found by applying a reported 1.4 percent loss rate on Internet sales (CyberSource 2007) to the overall sales for these merchants reported by the U.S. Census Bureau (2007). This results in $2.567 billion in payment fraud losses to Internet, mail order, and telephone merchants. The CyberSource loss rate includes sales that the merchants did not accept because the transactions were suspicious. To obtain actual losses, the author included 35 percent of the $2.567 billion, which represents the value of chargeback transactions. Losses for POS merchants are taken based on estimates of loss rates provided to the author by Steve Mott,

the principal of BetterBuyDesign and an expert on payments who provides consulting services to merchants. Other sources of loss rate are similar but result in higher total losses than the rates provided by Mott (see McGrath and Kjos, footnote 22, p. 13; Mott 2007; and Taylor).

The estimates are for payment cards issued by domestic financial institutions, but some sales by U.S. merchants will be on payment cards issued by foreign financial institutions. According to the Bureau of Economic Analysis, foreign travelers in the U.S. spent $108 billion in 2006, which represents 4 percent of total card payments. Accordingly, the estimate for losses by POS merchants is reduced by 4 percent. This assumes foreign tourism and travel is purchased on payment cards and that the fraud rate for foreign and domestically issued cards is equal.

**Sources:**

CyberSource. 2007. *Online Fraud Report.*

Gerdes, Geoffrey R. 2008. "Recent Payment Trends in the United States," *Federal Reserve Bulletin*, October, pp. A75-A106.

McGrath, James, and Ann Kjos. 2006. "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges," Federal Reserve Bank of Philadelphia, Payment Cards Center.

Mott, Steve. 2007. "Why POS Merchants Don't Buy in to Payment Security," *Digital Transactions News*, September 7, available at *www.digitaltransactions.net/ newsstory.cfm?newsid=1503.*

Nilson Report. 2007. "Credit Card Fraud—U.S.," *The Nilson Report*, issue 876, March.

Office of Travel and Tourism Industries. 2006. "Annual 2006 U.S. Travel and Tourism Balance of Trade," at *http://tinet.ita.doc.gov/outreachpages/download_data_table/BalanceofTrade_1996-2006.pdf.*

Pulse. 2008. "2008 Debit Issuer Study," May.

Taylor, Gray. 2009. "Card Payments: Global Key Data," presentation to the Association for Convenience and Petroleum Retailing, p. 25.

U.S. Bureau of the Census. 2007. *Annual Retail Trade Survey.*

## ENDNOTES

[1]Traditional methods include stealing payment cards, intercepting mail with cards or account information, and spying cards as they are used. Forty-one percent of debit card fraud is a result of lost and stolen cards (Tedder).

[2]Identity theft is special case of this type of payment fraud. Identity theft occurs when a criminal takes information about a person to create a new deposit, credit card, or non-deposit (cell phone, utility, and so on) account. In each of these cases, the identity of a person is misrepresented and any transaction with the account would be payment fraud.

[3]Illegal activities, such as terrorist financing or gambling, are not considered payment fraud if they involve a payment that is properly authorized by the account holder (Braun and others, p.145).

[4]Issuers began to add magnetic stripes to payment cards in the 1970s and since then have struggled with their vulnerability to counterfeiting (Mandell, 1990, pp. 64-69, ch. 9 and ch. 10).

[5]Examples of such information include card account number, card security code, expiration date, card issuer phone number, cardholder name, address, zip code, merchant or transaction characteristics, and personal information such as high school or mother's maiden name.

[6]Card information skimmed at Florida restaurants sells for as much as $50 (Poulsen).

[7]PIN transactions are less prone to fraud, but the PIN is now another piece of information targeted by criminals ("Losses Mount As Fraudsters Evade UK Chip Card Protections," *Cards & Payments*, July 1, 2008, p. 14). Because it is difficult to monitor and detect, most compromises of PINs occur at pay-at-the-pump terminals (Tedder, p. 9).

[8]In 2003, California was the first to enact a notification law. Other states followed, and at least 42 states now have such laws (Perkins Coie).

[9]On less press coverage, see *datalossdb.org/where_did_it_go*. Other explanations include more effective law enforcement and better acquaintance with requirements of notification laws so that companies are less likely to announce minor incidences.

[10]See Sullivan (2007) for an analysis of the risk that nonbanks pose for payments and a discussion of the supervisory structure over nonbanks in payments. Bradford and others (2009) describe the extent of and risks posed by nonbanks in the payments systems of the United States and Europe.

[11]A study of identity fraud found that 45 percent of consumers did not know how their data was accessed (Javelin).

[12]Criminals put together groups of compromised computers into "botnets" and use them, for example, to send phishing e-mails to large numbers of recipients.

[13]Respondents to a 2008 survey of consumers most commonly chose security as the most important characteristic of payment instruments (Foster and others, 2009, p. 37)

[14]These direct losses are only part of the cost of payment fraud. Others include costs of fraud prevention and costs of pursuing perpetrators. Social costs include law enforcement activities to investigate and prosecute payment fraud.

[15]Another major participant in the card payment network is acquirers, who process payments for merchants. Losses reported to acquirers would typically be passed on to the merchants for whom they process payments.

[16]Merchants pay for the guarantee in their payment processing fees.

[17]The rule for what is "timely" and the $50 limit is determined in the United States by Regulation E, written by the Federal Reserve to implement a provision in the 1978 Electronic Funds Transfer Act.

[18]Industry practice is less consumer friendly in cases of fraud on PIN debit transactions. But the resulting losses to consumers would be limited because it has been estimated that 88 percent of major banks apply zero liability to consumers in cases of fraudulent PIN debit transactions (Tedder 2009, p. 7).

[19]For credit card transactions, Table 2 assumes that fraud losses as a percent of sales was .03 percent for POS merchants and .49 percent for Internet, mail order, and telephone merchants.

[20]Data limitations allow estimates only for the year 2006. Details on sources and calculations of these estimates are provided in an appendix.

[21]Two other standards concern software and hardware used to process payments (see *www.pcisecuritystandards.org*).

[22]Banks have had to reissue many of their debit and credit cards as a result of data breaches. See, for example, *www.bankinfosecurity.com/articles.php?art_id=1200*.

[23]Chip-and-PIN rollout in the UK was coordinated by the Association for Payment Clearing Services, which consists of financial institutions and payment clearing and settlement companies. The Groupement des Cartes Bancaires, a clearing and settlement network, guided France's switch to EMV payment cards.

[24]"Key PCI Deadline Passes With Half of Big Merchants Compliant," *Digital Transactions News*, October 2, 2007 (*www.digitaltransactions.net/newsstory.cfm?newsID=1533*). As of September 30, 2009, large merchants, who process about half of Visa transactions, were 97 percent compliant (Visa).

[25]Similarly, in 2003, the British Retail Consortium expressed concern that the cost of shifting to chip-and-PIN may reach €500 million but estimated that retailers would save only €25 million in card payment fraud losses (Simpson).

[26]"Merchant Trade Groups Come Together to Advocate for Changes to Data Security Standards," *Smart Card Trends*, June 10, 2009 (*www.smartcardstrends.com/det_atc.php?idu=9557*).

[27]Hackers attacked the computers of Heartland Payment Systems, Inc., in December 2007 and went undiscovered until October 2008 (Zetter). A reported 130 million records were compromised. Heartland was compliant in April 2008. Some argue that the security standards are inadequate, while others allege that Heartland's security efforts were deficient (Wolfe). A June 2009 breach at Network Solutions occurred despite PCI compliance (McGlasson).

[28]This is often an industry-controlled entity to ensure confidentiality. Examples are the Australian Payments Clearing Association or the UK Payments Administration.

## REFERENCES

American Bankers Association. 2007. *ABA Deposit Account Fraud Survey Report*, 2007 ed.

_____. 2009. "ABA Deposit Account Fraud Survey Highlights of Survey Results."

Anderson, Ross, Rainer Böhme, Richard Clayton, and Tyler Moore. 2008. "Security Economics and the Internal Market," Report to the European Network and Information Security Agency.

APACS. 2009. *Fraud: The Facts*

Bradford, Terri, Fumiko Hayashi, Christian Hung, Simonetta Rosati, Richard J. Sullivan, Zhu Wang, and Stuart E. Weiner. 2009. "Nonbanks and Risk in Retail Payments: EU and U.S.," in Eric M. Johnson, ed., *Managing Information Risk and the Economics of Security*. New York: Springer Publishing.

Braun, Michele, Jamie McAndrews, William Roberds, and Richard J. Sullivan. 2008. "Understanding Risk Management in Emerging Retail Payments," Federal Reserve Bank of New York, *Economic Policy Review*, vol. 14, no. 2, September, pp. 137-59.

CyberSource. 2007. "8th Annual Online Fraud Report."

_____. 2010. "11th Annual Online Fraud Report."

EC Staff. 2009. "Report on Cross-Border E-Commerce in the EU," EC Staff working document, May 3.

Foster, Kevin, Erik Meijer, Scott Schuh, and Michael A. Zabek. 2009. "The 2008 Survey of Consumer Payment Choice," Federal Reserve Bank of Boston, Public Policy Discussion Papers, no. 09-10.

Gerdes, Geoffrey. 2008. "Recent Payment Trends in the United States," *Federal Reserve Bulletin*, October, pp. A75-A106.

Gorman, Siobhan, and Evan Perez. 2009. "Hackers Indicted in Widespread ATM Heist," *Wall Street Journal*, November 11, p. A10.

Greenstein, Shane, and Victor Stango. 2007. "Introduction," in S. Greenstein and V. Stango, eds., *Standards and Public Policy*. Cambridge: Cambridge University Press, pp. 1-17.

Hernandez, Will. 2009. "Debate Lingers Over Definition Of 'End-To-End' Encryption," *ATM & Debit News*, August 20, p. 1.

Hitachi Consulting. 2008. "2008 Study of Consumer Payment Preferences," September.

ID Analytics. 2006. "National Data Breach Analysis."

Javelin Strategy and Research. 2010. "2010 Identity Fraud Survey Report," February.

Kwang, Kevin. 2009. "Signature Makes Cards 'Less Secure'," ZDNet Asia website, November 23, at *http://www.zdnetasia.com/news/security/0,39044215,62059517,00.htm.*

Leyden, John. 2008. "Merchants Call Credit Card Industry's Bluff on Compliance," *The Register*, June 24, at (*www.theregister.co.uk/2008/06/24/pci_dss_compliance*).

McGlasson, Linda. 2009. "Top 9 Breaches of 2009," CU Info Security website, December 14, at *www.cuinfosecurity.com/articles.php?art_id=2001&pg=1.*

Mandell, Lewis. 1990. *The Credit Card Industry: A History*. Boston: Twayne Publishers.

Moore, Tyler, Richard Clayton, and Ross Anderson. 2009. "The Economics of Online Crime," *Journal of Economic Perspectives*, vol. 23, no. 3, September, pp. 3-20.

Mott, Steve. 2007. "Why POS Merchants Don't Buy into Payment Security," *Digital Transactions News*, September 7, at *www.digitaltransactions.net/newsstory.cfm?newsid=1503.*

Observatory for Payment Card Security (OPCS). 2007. *Annual Report.*

Perkins Coie. 2009. "Security Breach Notification Chart," at *www.perkinscoie.com/files/upload/LIT_09-09_Security_Breach_Notification_Law_Chart.pdf.*

Poulsen, Kevin. 2009. "Credit Card Skimming Survey: What's Your Magstripe Worth?" Wired Magazine Threat Level blog, October 2, at *www.wired.com/threatlevel/2009/10/ florida_skimming.*

Pulse. 2008. "2008 Debit Issuer Study," May.

Roberds, William, and Stacy Schreft. 2008. "Data Breaches and Identity Theft," Federal Reserve Bank of Atlanta, working paper 2008-22, September.

_____. 2009. "Data Security, Privacy, and Identity Theft: The Economics Behind the Policy Debates," Federal Reserve Bank of Chicago, *Economic Perspectives*, First Quarter, pp. 22-30.

Simpson, John. 2003. "Security of Payments: A Retailer's Viewpoint," British Retail Consortium, at *ec.europa.eu/internal_market/payments/docs/fraud/2003-conference/secure-pay-retailers_en.pdf.*

Singel, Ryan. 2009. "Probe Targets Archives' Handling of Data on 70 Million Vets," Wired Magazine Threat Level blog, October 1, at *http://www.wired.com/threatlevel/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/.*

Smart Card Alliance. 2009. "End-to-End Encryption and Chip Cards in the U.S. Payments Industry," September, at *www.smartcardalliance.org/resources/pdf/End-toEnd_Encryption_Position Paper_090809.pdf.*

Steinfeld, Charles W., Rolf T. Wigand, M. Lynne Markus, and Gabe Minton. 2007. "Promoting E-business Through Vertical IS Standards: Lessons from the U.S. Home Mortgage Industry," in S. Greenstein and V. Stango, eds., *Standards and Public Policy.* Cambridge: Cambridge University Press, chapter 5, pp. 160-207.

Sullivan, Richard J. 2009. "The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States," Federal Reserve Bank of Kansas City, *Payment System Research Briefing*, October.

_____. 2008. "Can Smart Cards Reduce Payments Fraud and Identity Theft?" Federal Reserve Bank of Kansas City, *Economic Review*, vol. 93, no. 3, Third Quarter, pp. 35-62.

_____. 2007. "Risk Management and Nonbank Participation in the U.S. Retail Payments System," Federal Reserve Bank of Kansas City, *Economic Review*, vol. 92, no. 2, Second Quarter, pp. 5-40.

Symantec. 2010. "Global Internet Security Threat Report," April, at *http://www4.symantec.com/Vrt/wl?tu_id=SUKX12717112825031262O2.*

Taylor, David. 2009. "Data Security Slugfest: Tokenization Vs End-to-End Encryption," Storefront Backtalk website, April 15, at *www.storefrontbacktalk.com/supply-chain/data-security-slugfest-tokenization-vs-end-to-end-encryption/#comments.*

Tedder, Krista. 2009. "Now You See It, Now You Don't: A Review of Fraud Costs and Trends." First Data Corporation White Paper 2009, at *http://www.firstdata.com/downloads/thought-leadership/ fd_fraudcostsandtrends_whitepaper.pdf.*

UK Cards Association. 2010. "New Card and Banking Fraud Figures," press release, March 10, at *www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/.*

Visa. 2009. "U.S. PCI DSS Compliance Status," September 30.

Wolfe, Daniel. 2009. "New Security Focus Goes Beyond PCI," *American Banker*, March 24, p. 1.

Zetter, Kim. 2009. "TJX Hacker Charged With Heartland, Hannaford Breaches," Wired Magazine Threat Level Blog, August 17 at *http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/.*