Controlling Security Risk and Fraud in Payment Systems

By Richard J. Sullivan

In late 2013, a breach of the cashier system at a major retailer exposed information on 40 million debit and credit cards. That fraudsters can use the payment card numbers harvested in this breach to create fraudulent payments underscores one of many security weaknesses that can lead to payment fraud. The direct cost of fraud on automated clearinghouse (ACH), debit card, and credit card payments reached $6.1 billion in 2012. Investments and ongoing expenses for preventing, detecting, monitoring, and responding to payment fraud add considerably to direct costs. Fraud and security weaknesses in payments can have an indirect cost as well if they cause concerned consumers and businesses to choose less efficient forms of payment. More broadly, the public's loss of confidence in payments has had significant negative economic consequences in the past. A constant stream of news reports on data breaches, phishing attacks, spoofed websites, payment card skimmers, fraudulent ATM withdrawals, computer malware, and infiltrated retail point-of-sale systems should concern policymakers because it indicates weak payment security and undermines confidence in payments.

Richard J. Sullivan is a senior economist at the Federal Reserve Bank of Kansas City. Emily Cuddy and Joshua Hanson, research associates at the bank, helped prepare this article. This article is on the bank's website at ***www.KansasCityFed.org.***

Payment participants—end-users who make payments, financial institutions and nonbanks that provide payment services, and networks and service providers that process payments—all have considerable incentive to secure payments and deter fraud. They value the convenience of noncash payments and wish to avoid the inconvenience and losses of payment fraud. Under ideal conditions, these incentives would provide a level of payment security that best benefits society. Incentives do not work well, however, when accurate information about security solutions is unavailable, when the consequences of security failures spill over to innocent parties, or when effective security requires difficult coordination of many disparate parties.

Consequently, public and private institutions have evolved a "control structure" to ensure payment security and deter fraud. The control structure takes a variety of forms, such as setting rules that allocate losses resulting from payment fraud, regulating and supervising the activities of some payment participants, designing operational procedures that embed security protocols, and coordinating security efforts. Policymakers must assess how well a payment system manages fraud risks given constantly changing threats and complex interdependencies that can cause misaligned incentives. A proper assessment is crucial because improvements to payment security are costly and often in fixed infrastructure that is hard to change.

This article examines the problem of controlling payment fraud risk. The first section reviews methods of payment fraud, the levels and trends in the use of these methods, and the resulting losses. At various points, the section studies recent data breaches to illustrate how data useful to payment fraud is exposed and how a "virtual fraud factory" translates exposed data into payment fraud. The second section discusses how incentives influence payment security, describes the structures that networks and government have established to secure payments and control payment fraud, and reviews insights from recent research on defense strategies for computer networks. The third section presents examples of changes that would strengthen payment security and deter fraud.

The article finds the protection of sensitive data used to commit payment fraud is inadequate and payment participants should make immediate effort to improve data security. Medium-term priorities should target emerging weaknesses in check payment processing and

card payment authorization. In the long term, policymakers and industry leaders should seek to strengthen the control structure over payment security by making security standards more effective and creating appropriate incentives to protect payments.

I. THE PROBLEM OF PAYMENT FRAUD IN THE UNITED STATES

Fraudsters use a variety of methods leading to substantial direct losses to payment participants. These methods fall in and out of favor over time, as do attacks exposing sensitive data. Fraudsters use exposed sensitive data in a decentralized, worldwide production process translating stolen data into fraudulent payments. Direct losses in the United States from all methods of payment fraud do not show adverse trends. However, the number of data breaches has had an upward trend since 2009, and in 2013, the number of records exposed in data breaches significantly increased.

Methods of committing third-party payment fraud

One goal of strong payment security is to prevent third-party fraud—payment fraud perpetrated by individuals other than the legitimate account holder. Successful third-party fraud occurs when payment initiation (creating a payment order), authentication (confirming a payer's identity), or approval (screening the payment order for suspicious characteristics before granting approval) fail to prevent an unauthorized transaction. All payment participants have a role in preventing third-party fraud. In a check payment, for example, the account holder should ensure the checkbook is in the hands of authorized payers, the payee should verify the signature on the check, and the depository financial institution (DFI) should inspect the check to ensure it is not counterfeit.

Many methods of payment fraud occur in all payment channels. Forged signatures plague check as well as card payments.[1] Unscrupulous telemarketers obtain account information from prospective customers and improperly initiate ACH or check payments (Mallow and Thurman). Payment card numbers are sufficient to initiate an unauthorized payment in e-commerce transactions where the card is not present. Fraudsters may alter payment instruments by replacing a payee's name on a legitimately created check or recoding the magnetic stripe

Table 1

VALUE OF UNAUTHORIZED THIRD-PARTY FRAUD TRANSACTIONS, U.S. NONCASH RETAIL PAYMENTS, 2012

Payment type	Fraud value (billions)	Loss rate* (percent)
Check	$1.1	.0043
Automated clearinghouse	$1.2	.0009
Debit and credit cards	$3.8	.0921
All noncash retail payments	$6.1	.0035

*Fraud value per value of payment before recoveries and chargebacks, or the gross loss (or simply "loss").
Sources: Federal Reserve System (2014) and author's calculations.

of a payment card with data stolen in data breaches (Blank). Fraudsters also obtain raw payment cards and manufacture counterfeits with data stolen via card skimmers fit onto an ATM or gas pump, sometimes also with a remote camera installed to capture the cardholder's PIN (Digital Transactions News 2013a). Computer viruses infect personal computers with key loggers that harvest online banking credentials, which are then used to generate fraudulent wire, check, or ACH payments.[2]

The outcome of these methods in the United States is the loss of an estimated $6.1 billion on unauthorized third-party fraud transactions, or 0.0035 percent of total payment value, in fraudulent check, ACH, and card payments for 2012 (Table 1).[3] The highest losses are on debit and credit cards, totaling $3.8 billion, followed by ACH ($1.2 billion) and checks ($1.1 billion).

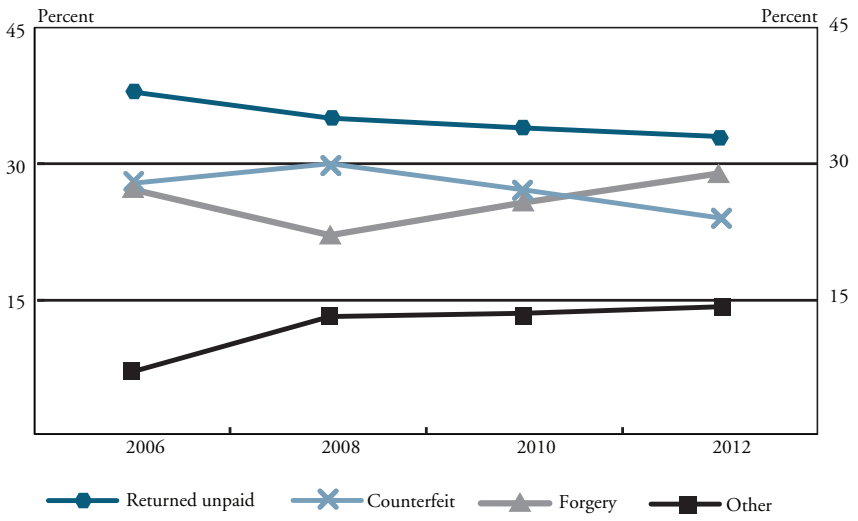
Changes in methods of fraud and attack vectors

Some methods of committing payment fraud are used consistently while others have changed in recent years. Methods used for check fraud have changed a modest amount since 2006 (Chart 1). Checks returned unpaid (insufficient funds, closed or fictitious accounts, stop payments, and so on) are the leading method of check fraud and have a slight downward trend since 2006. Since 2008, the share due to counterfeit checks has declined while forged checks have increased, becoming the second leading source of check fraud.

Fraud resulting from counterfeit cards has become the leading source of credit and debit card fraud, accounting for 51 percent of fraudulent debit and credit card transactions in 2012 (Chart 2). The

Chart 1

SHARES OF U.S. CHECK FRAUD BY METHOD OF COMPROMISE



Note: 2010 statistics are estimated.
Source: American Bankers Association.

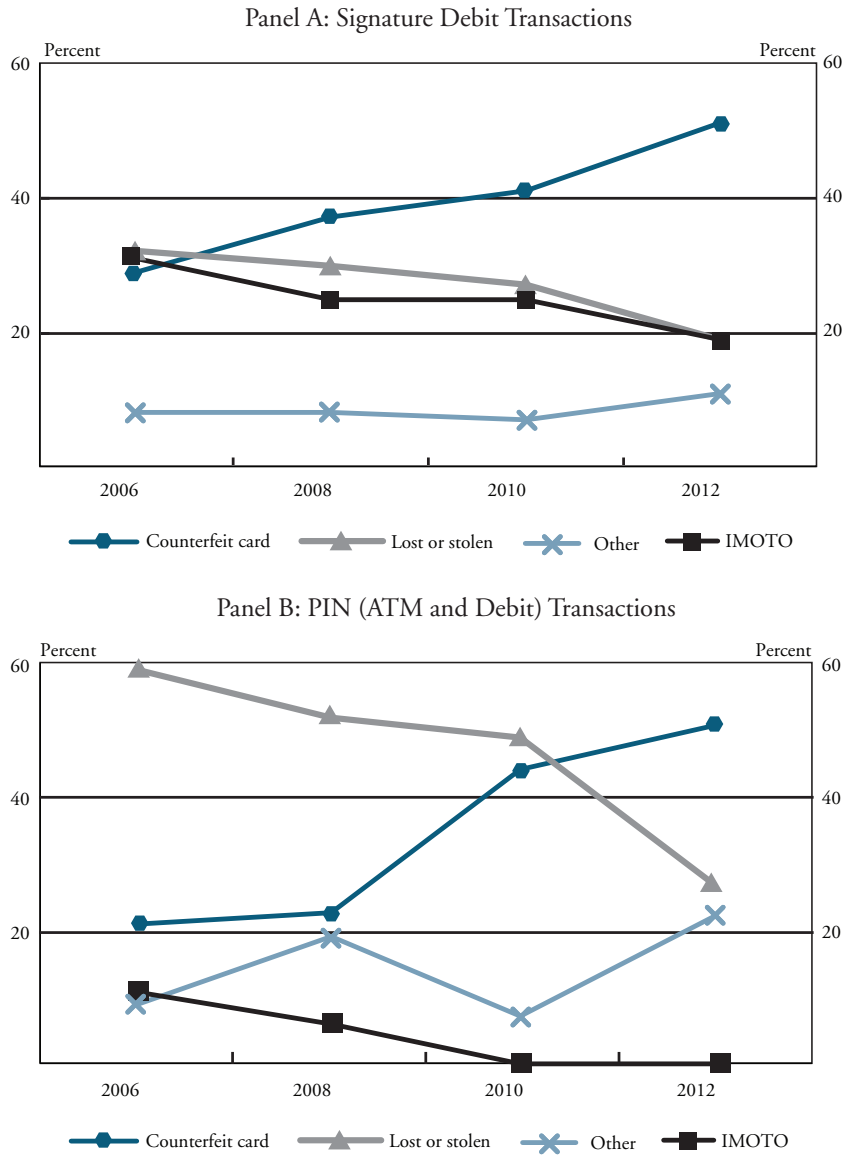
share of fraud due to lost or stolen cards has declined significantly, as has the share of fraudulent Internet, mail order, or telephone order (IMOTO) transactions.

Access to sensitive data has become a key factor enabling many methods of payment fraud. Stolen data allow fraudsters to misrepresent authority, counterfeit cards and checks, and take over or create new payment accounts. Data is more valuable to fraudsters because today payers use fewer paper checks and more electronic payments (cards, ACH), thus initiating more noncash retail (smaller-value) payments with data alone. In 2012, payers initiated 85 percent of all noncash retail payments electronically, up from 42 percent in 2000.[4]

The type of information exposed in breaches increasingly provides data useful for payment fraud. Breaches exposing payment data (payment card numbers and bank account numbers) have an upward trend, rising from 127 in 2009 to 217 in 2013 (Chart 3).[5] Breaches exposing personally identifiable information (Social Security numbers, medical information, passwords, or financial information such as tax returns), the type of data that helps in account takeovers and identity theft, rose

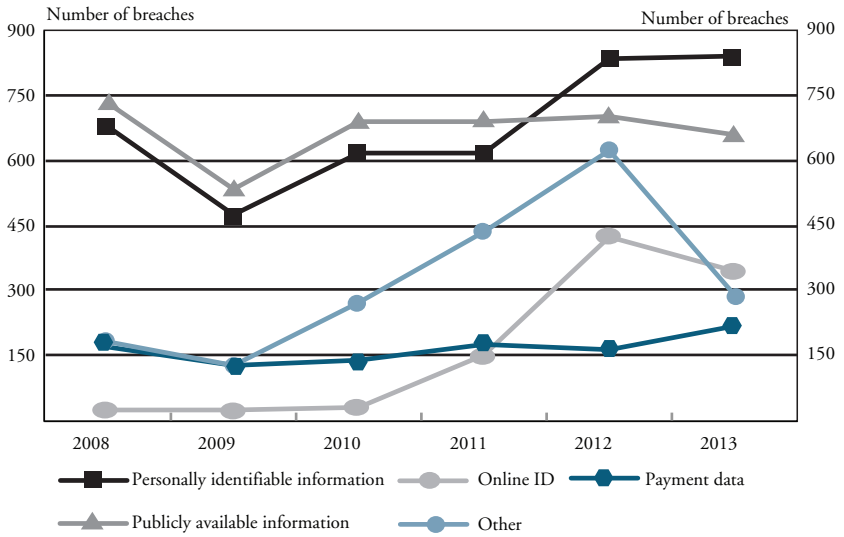
Chart 2

SHARES OF U.S. PAYMENT CARD FRAUD BY METHOD OF COMPROMISE



Note: IMOTO includes Internet, mail order, and telephone order transactions.
Source: American Bankers Association.

Chart 3
TYPE OF DATA EXPOSED IN U.S. DATA BREACHES



Notes: Breaches exposing more than one type of data are counted in multiple categories. The total number of incidents in a given year will be higher in Chart 3 than in Chart 6 due to this double-counting.
Source: Risk Based Security.

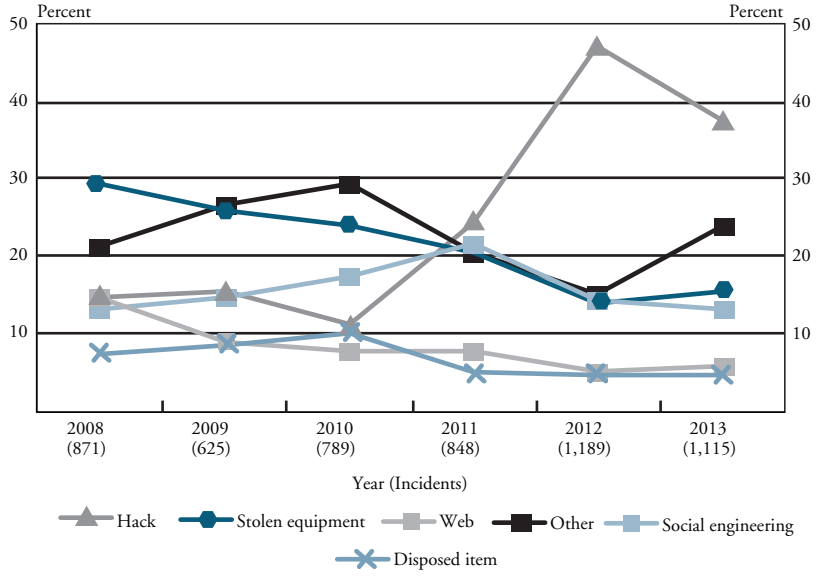
to 841 in 2013, up from 475 in 2009. The number of breaches exposing online IDs has risen rapidly, from 22 in 2009 to 342 in 2013.[6]

Methods used to gain unauthorized access to data also changed from 2008 to 2013. The share of attacks involving hacking into computer systems rose after 2010 while the share involving stolen equipment declined (Chart 4). The share of attacks attributable to accidents by individuals inside the organization declined after 2010 while the share attributable to outsiders increased (Chart 5).

The number of publicly disclosed data breaches in the United States has risen recently, but the number of records exposed fluctuates significantly from year to year and shows no trend. From 2008 to 2013, publicly disclosed data breaches peaked at 1,189 incidents in 2012 and fell slightly to 1,115 in 2013 (Chart 6). The year 2013 stands out as particularly bad: breaches exposed 547 million records, nearly matching the cumulative 603 million records exposed from 2008 to 2012. Megabreaches—those exposing 10 million or more records—occur infrequently, yet contribute to the lion's share of total records exposed.

Chart 4

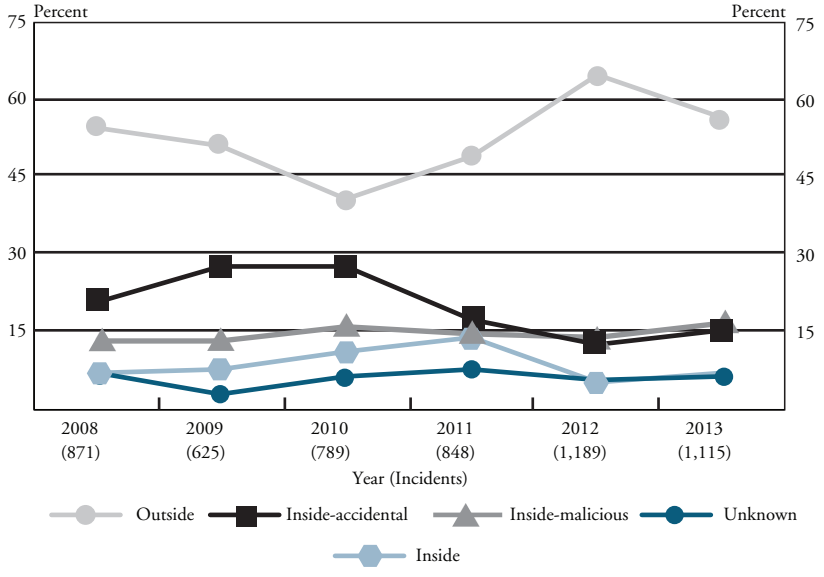
DISTRIBUTION OF ATTACK METHODS IN U.S. DATA BREACHES



Source: Risk Based Security.

Chart 5

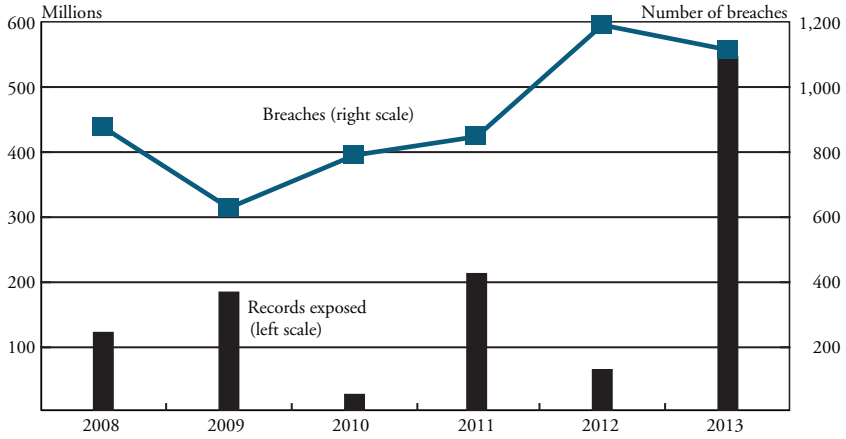
INTENT AND INSIDER STATUS OF INDIVIDUALS ASSOCIATED WITH U.S. DATA BREACHES



Source: Risk Based Security.

Chart 6

PUBLICLY DISCLOSED U.S. DATA BREACHES AND RECORDS EXPOSED



Note: The number of records exposed is a lower bound because the number is not available in 35 percent of breaches.
Source: Risk Based Security.

From 2008 to 2013, mega breaches accounted for only 17 of the 5,437 publicly disclosed data breaches, but together exposed 979 million records, 85 percent of all records exposed (Chart 7).[7]

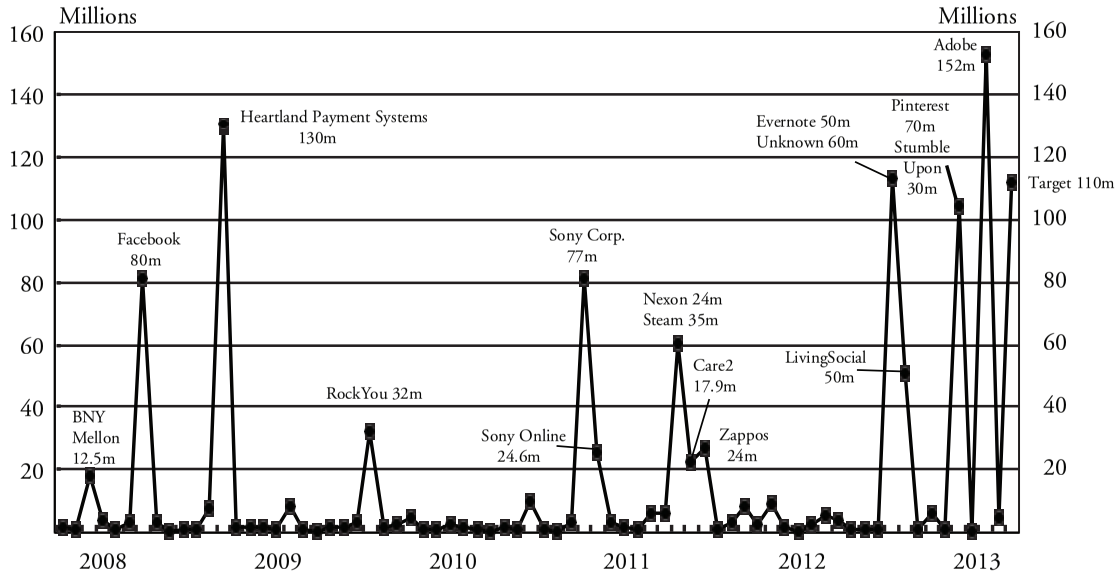
Fraud losses and incidents

From 2006 to 2012, the loss per value of check payments DFIs suffer due to fraud has not risen or fallen substantially.[8] DFIs lost 0.0023 percent of the value of checks in 2006, 0.0030 percent in 2009, and 0.0025 percent in 2012 (Chart 8).[9] The value of attempted fraud relative to total check value is 10 to 12 times that of actual losses because DFIs and corporations implement effective deterrence and intervention. Attempted check fraud, as measured by avoided loss, also does not show substantial increases or decreases since 2006. The fraud loss rate on card payments in the United States has not increased since 2009, but it is higher than in some other countries.

The fraud loss rate on card payments was an estimated 0.0921 percent of purchase value for the United States in 2012 (Table 2), lower than an estimated 0.1100 percent for 2009 (Sullivan). The loss rate on cards payments in 2012 for the United States is slightly lower than that for Canada but somewhat higher than that for the United

Chart 7

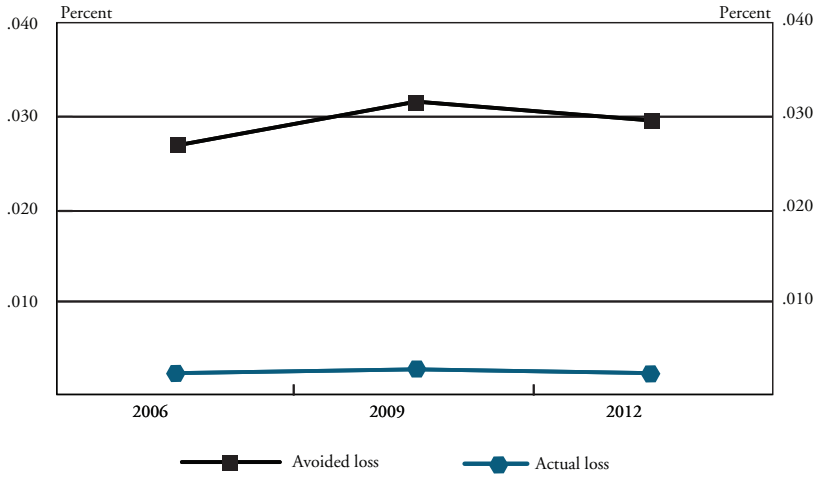
RECORDS EXPOSED IN U.S. DATA BREACHES, 2008-2013, MONTHLY



Source: Risk Based Security.

Chart 8

LOSS RATE AND AVOIDED LOSS RATE BY VALUE ON FRAUDULENT CHECKS



Sources: Federal Reserve Payments Study, (2014, 2011, 2007); ABA Deposit Account Fraud Survey Report, (2013, 2011, 2009, 2007) author's calculations.

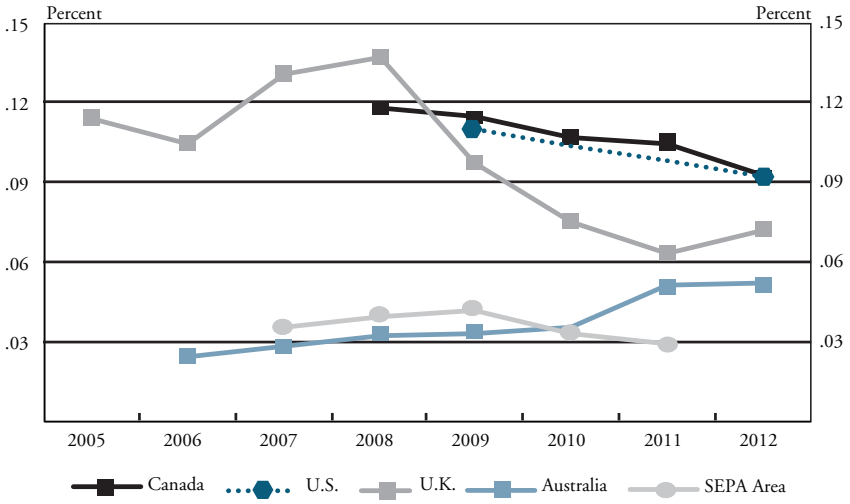
Table 2

VALUE OF UNAUTHORIZED THIRD-PARTY FRAUD TRANSACTIONS PER VALUE OF DEBIT AND CREDIT CARD PURCHASE TRANSACTIONS, 2012

Country	Loss rate* (percent)
United States	.0921
United Kingdom	.0716
Canada	.0927
Australia	.0523

*Fraud value per value of payment before recoveries and chargebacks, or the gross loss (or simply "loss").
Sources: Federal Reserve System (2014), Financial Fraud Action U.K., U.K. Cards Association, Interac, Canadian Bankers Association, Australian Payments Clearing Association, and author's calculations.

Chart 9
FRAUD LOSSES PER VALUE OF PURCHASE TRANSACTIONS



Note: Losses calculated are for domestically issued debit and credit cards (2013, 2011).
Sources: Federal Reserve System, (2014, 2011); Board of Governors, (2013, 2011); Interac; Canadian Bankers Association, (2014a, 2014b); Australian Payments Clearing Association, (2014); European Central Bank, (2014, 2013, 2012); U.K. Cards Association, (2013); Financial Fraud Action U.K., (2014); author's calculations.

Kingdom, the Single European Payment Area (SEPA) countries, and Australia (Chart 9).

Available information for ACH shows fraud is decreasing. Unauthorized ACH debit transactions were 0.0288 percent of transaction volume in 2013 (NACHA).[10] The rate has declined for 11 years in a row.

Data security and payment fraud

Evidence does not show significant adverse trends in loss rates due to retail payment fraud in the United States. This record, however, does not imply a rising concern over payment security is misplaced. First, the extraordinary experience with data breaches in 2013 is alarming on its own. Second, what is known about recent breaches suggests a fair amount of exposed data is feeding payment fraud. News stories after the data breach at the Target retail chain revealed a worldwide network for selling card data (Krebs 2014a), attention to the quality of card data in the batches offered for sale (Krebs 2014b), the geographic tailoring of batches to thwart location as an indicator of potential fraud (Krebs

2013b), and the mass production of counterfeit cards (The Associated Press). Together, these stories suggest a decentralized "virtual fraud factory" organized through the Internet, using specialized agents and with a worldwide scope.[11]

Moreover, most of the available statistics on fraud losses are for 2012 and earlier, prior to the large data breaches in 2013. Early evidence suggests exposed payment card numbers in 2013 may be responsible for a recent increase in the fraud loss rate on debit card transactions.[12] Because it can take some time for lost data to translate into fraud, damage in terms of losses resulting from the four megabreaches in the second half of 2013 (Chart 8) may not occur until 2014 or later.

II. DEFENDING THE PAYMENT SYSTEM TO PREVENT FRAUD

Incentives for payment participants to secure the payment system are often misaligned and lead to inadequate security. Payment networks establish specific controls to ensure security and limit fraud. Public authorities pass laws, write regulations, and monitor payment system participants for compliance. These activities form a "control structure" that determines how a payments system manages risks. Recent research provides insights into how the payment system protects privacy and integrity and how dissimilar conditions might lead to different defensive strategies.

The role of incentives and the control structure over payment security

Under ideal conditions—in which payment participants are responsible for the full costs of their failure to take appropriate security precautions—private incentives will lead to a socially beneficial level of care. Several market imperfections, however, prevent this outcome. Consequences of security failures spill over to innocent payment participants, and identifying victims and valuing the resulting damage can be difficult. Who bears the consequence of a security failure does not always match who has the ability to correct a security gap. Some payment participants do not value strong security and may avoid its costs. Information about the quality of commercial security products is imperfect and can cause incorrect investment decisions.[13] Some security protocols require many parties to adopt them jointly (for example, computer-chip cards need to be adopted by DFIs, payment processors, merchants,

and consumers), creating the potential for coordination failure such as chicken-and-egg problems.[14]

The control structure over security risk in payment systems emerged in part to counteract the imperfections inherent in network markets by influencing the incentives of network managers, DFIs, and end-users to protect against payment fraud. Incentives to invest in fraud deterrence systems, to devote ongoing resources to monitor payments for possible fraud, and to respond effectively to security failures are strong for those who bear direct losses from payments fraud. The control structure supplements these incentives with rules, regulations, and legal requirements embedded in commercial agreements, best practices, standards, and guidance on payment security. Legal recourse is also available to seek compensation for damages resulting from inadequate security. More detail on the four major elements of the control structure is provided in the Appendix.

Defense of payment systems

Strategies of attack and defense in computer network security evolve over time and lead to changes in targeted data, methods of attack, and types of data stolen. Research on network security provides insights into these changes. For example, two lines of research imply shifts in the weak links of a payment system and thus shifting trends in attacks and targeted data.

Early models of network security focused on points of significant vulnerabilities on a network. Preferences—and thus efforts—toward safety and security among payment participants differ. When overall security depends on the security of each element of a network, differences in participant security efforts may create weak links (Hirshleifer, Varian). Furthermore, these weak links can change as the security preferences or makeup of payment participants change over time.

More recent models recognize the Internet consists of many components—computers, communication channels, software, and users—each subject to attack and requiring defense. The weakness of each component will vary, and attackers will strike vulnerabilities with the highest expected payoff. Engineers who protect these components make judgments about their vulnerability and prioritize each component to determine which weakness to correct. These assessments are

difficult, costly, and uncertain, and some weaknesses will likely remain due to undetected vulnerabilities or imprecise assessments (such as underestimates of potential damages).

Böhme and Moore simulate a model with these characteristics and although the models are stylized, they generate realistic insights into protecting information in computer networks. The defense will protect a handful of weak links but not all of them. Over time, the set of weak links will change. A mild amount of uncertainty can lead to additional protection of weaker links where expected losses are high and countermeasures are justified. On the other hand, high uncertainty can lead to no protection: the defender may not know which link is weakest and thus leave all links unprotected.[15]

By studying successive rounds of attack and defense, this research provides implications for learning and network security. Attackers search for vulnerabilities and move on to other nodes in the network with the same vulnerability when successful. Defenders respond to a successful attack by fixing that particular vulnerability. In this scenario, information sharing would be useful to allow organizations to learn from one another so that they can deter attacks.

The research also provides perspective on longer-term strategies. First, a wait-and-see approach to defense could improve returns to security investment for an organization even if it accepts some successful attacks. Second, organizations can engage in proactive defensive strategies or pursue reactive containment strategies. Given costly and uncertain investments in data security, organizations may lean toward reactive strategies, which can lead to periods of security failures such as the recent rise in data breaches in the United States. Third, organizations may employ more proactive security strategies at other times to preserve the value of prior security investments.

The recent record on data breaches indicates security over sensitive information fueling payment fraud is inadequate. The defense put in place by those processing and storing sensitive payment information appears insufficient relative to the attacks mounted by the criminal enterprise generating payment fraud. Sensitive nonpayment data, such as Social Security numbers, user names, and passwords, are also at risk. Computer networks need better strategies and tactics to ward off further unauthorized access to sensitive data. Research on network security

provides some insight into network protection, but more broadly, the control structure over payment security also needs to improve its ability to adapt as threats arrive.

III. IMPROVING PAYMENT SECURITY AND REDUCING FRAUD

The payment system is complex, both within and across all payment types, with a variety of vulnerabilities and inadequate approaches to security. A complete review of options that would improve payment security is beyond this article's scope.[16] Instead, the goal of this section is to illustrate a number of options for improving payment security and to suggest priorities in the short, medium, and long term.

Reducing fraud will take efforts on both public and private fronts. While options are available, many of which are under way, prioritizing where to direct efforts and resources into security improvements is a challenge. Given the poor recent record on data breaches, protecting sensitive data is a high priority in the short term, made even more urgent by evidence that consumers lose confidence in some payment types after a data breach (Petru). Medium-term priorities focus on spurring progress on existing efforts in the industry to bolster network and payment security. In the long term, more fundamental changes can help ensure the payment system is resilient and can adapt to the changing security environment.

Short-term priority: protect payment and other sensitive data

The United States suffered an upward trend in publicly disclosed data breaches since 2009. In 2013, there were 1,115 breaches, including seven megabreaches.[17] The breaches expose all forms of sensitive payment account numbers—debit, ATM, credit card numbers, and deposit account numbers—and thus could be used to commit fraud in any payment channel. In the near term, hackers will continue attacks aimed at acquiring data useful to payment fraud.

The record suggests serious data security weakness at merchants, DFIs, and payment processors. From 2008 to 2013, merchants suffered 1,489 publicly disclosed breaches, 13 of which were megabreaches, exposing at least 862 million records. In the same period, DFIs suffered 207 publicly disclosed breaches exposing at least 6 million records.

While more records exposed come from merchants, DFIs have a worse record based on the incidence of data breaches from 2008 to 2013. The incidence rate (the number of breaches divided by the number of DFIs or merchants) was 0.23 percent for DFIs but only 0.02 percent for merchants.[18] Finally, the breaches in 2005 at CardSystems and in 2009 at Heartland Payment Systems, which exposed 40 million and 130 million records, respectively, tarnished payment processors' reputations for data security.

Industry efforts and public policy should consider a short-term goal of strengthening security over sensitive data, especially at larger organizations that can expose large amounts of sensitive data. The quickest avenue is to strengthen existing private and public enforcement of data security standards.

Credit card networks created the Payment Card Industry (PCI) Council in 2006 to improve card payment security.[19] The PCI Council establishes data security standards for the credit card networks' debit and credit cards and provides guidance on their implementation. Larger merchants and processors must validate their compliance with the standards by engaging an independent assessor to review their card data security. Since 2009, nearly 100 percent of large merchants validate annually that they comply with the standards.

Despite emphasizing larger merchants and recently imposing a system of fines for failing to comply with PCI standards, the PCI process has not prevented security weaknesses that allow large data breaches. The PCI Council should consider steps to improve enforcement mechanisms. Megabreaches should not occur at merchants and payment processors that have validated compliance with the data security standards (Heartland, Target, TJX). The Council may need to increase the responsibility of DFIs in monitoring their merchant clients for PCI compliance and consider imposing fines on DFIs in cases where their clients suffer data breaches. Other changes could also help. Organizations providing both validation and security services should establish mechanisms to reduce conflicts of interest that can compromise assessments (Zetter). Assessments could be more than an annual event for computer systems with equipment, programs, and architecture that change frequently (Robertson). Merchants and processors need to

have sufficient technical expertise to work with assessors and to provide complete information on internal payment processing systems.

Strengthening public oversight of data security in nonbank organizations could supplement improvements to the PCI system. Currently, the Federal Trade Commission and the Consumer Finance Protection Bureau have jurisdiction to enforce data security measures that deter payment fraud at merchants and processors (Mallow and Thurman). The FTC has recently sought to prohibit telemarketers from creating certain types of fraud-prone payments such as remotely created checks, remotely created payment orders, remittances, and prepaid cards (Digital Transactions News 2013b). In light of recent data breaches, legislators have proposed giving the FTC authority not only to enforce data security standards but to set them as well (Bjorhus and Spencer).

On a proportional basis, data breaches afflict DFIs more than they afflict merchants. While breaches at DFIs have not exposed large quantities of sensitive data, what is exposed is particularly useful for identity theft.[20] The most common types of information exposed in data breaches at DFIs are names, Social Security numbers, DFI account numbers, financial information, and addresses, all of which fraudsters can use for identity theft. Most identity theft involves the takeover or creation of payment accounts, and, according to the Department of Justice, victims of identity theft lost $24.7 billion in 2012 (Harrell and Langton).[21]

Federal financial institution regulators may need to speed implementation of their new cybersecurity assessments of financial institutions and strongly emphasize data security (Kitten). Regulators expect DFI management to have access to accurate and timely information to direct resources that control security risks, use external intelligence sources to identify threats, take care with third-party relationships, and respond appropriately to security breaches (Federal Financial Institutions Examination Council 2014). While these guidelines include strategies to manage the risk of data breaches, regulators may need to particularly reinforce DFIs' responsibility to prevent data breaches altogether.[22]

Medium-term priority: protect electronic cash letters and improve authorization in card payments

Check processing uses check images and data collected in data files called electronic cash letters. Many of these cash letters are transmitted in clear text. Unscrupulous operators can add or delete check data and alter the payee, dollar value, or routing information. Hackers who access electronic cash letters obtain DFI routing and account numbers along with images that often include names and addresses of account holders.

To ensure the integrity of an electronic check file, some financial institutions and processors encrypt the file when transmitted. However, there is no legal or regulatory requirement to encrypt transmitted electronic check files, nor are there common standards of encryption to follow. Some financial institutions and processors agree bilaterally to transmit encrypted files. The practice could become more widespread, however, if standards for check file encryption were established. A common standard would make it easier for financial institutions and check processors to find partners to exchange encrypted check files.

New forms of payment processing will require protection as well. Card issuers and card-accepting merchants in the United States will soon upgrade their payment processing systems to accommodate computer-chip payment cards. The computer chip allows enhanced security capabilities unavailable with magnetic stripe cards and is nearly impossible to counterfeit (Sullivan).[23] The experiences of other countries that have adopted computer-chip cards show that they significantly reduce fraud from counterfeit cards.

However, these countries found that fraudsters shifted their efforts to IMOTO transactions, causing a dramatic rise in associated fraud losses.[24] Card issuers may be anticipating a similar outcome for the United States by developing an alternative method to initiate card payments in e-commerce transactions. In this method, shoppers register a payment card at a merchant who then obtains a token number tied to the card from the card issuer. The merchant obtains authorization for payment with the token. The payment card number alone cannot be used to initiate an e-commerce transaction.

While card issuers deserve credit for anticipating the unintended consequences of adopting computer-chip cards, fraudsters can use other methods to create fraudulent payments. In the United Kingdom, for example, fraudsters have turned to social engineering tactics, tricking cardholders into handing over their computer-chip card and revealing security details such as the card's PIN. These scams have caused fraud losses from lost or stolen cards to rise in 2013 after many years of decline.

A rise in losses due to lost or stolen cards is even more likely in the United States because many issuers will allow cardholders to authorize a computer-chip card payment with signatures. Thieves may then increasingly target wallets and purses to steal payment cards and make fraudulent purchases with forged signatures.[25]

Card issuers need to prepare for added fraud due to lost or stolen cards. They should remind cardholders to protect their cards, to be vigilant against social engineering, and that DFI representatives or police would not ask for card security details or for online banking passwords. In addition, cardholders should give their payment cards only to trustworthy individuals.

The incentive to steal payment cards in the United States would fall if cardholders were authenticated with a PIN instead of an easy-to-forge signature. Some card networks and issuers are concerned about the inconvenience of entering a PIN. However, most cardholders use PINs without difficulty. More important, card issuers have the option of allowing "PIN-less" card payments, where authorization with only the card is sufficient. In fact, PIN-less and signature-less card payments are used extensively today, such as in quick service restaurants. Card issuers can manage the risk of fraud in PIN-less card payments by setting upper limits on the value of PIN-less card payments, as well as requiring PINs at higher risk merchants and if their transaction analysis suggests excessive risk.

Long-term priorities: effective security standards and improved incentives

Security standards are crucial for protecting payments. One key long-run principle to ensure efficient processing and strong security would be to standardize security protocols embedded in electronic payment messages.

Standardization improves efficiency because processors adapt their systems to a limited set of protocols. At times, however, private providers can rapidly introduce security solutions before standardized solutions are developed and adopted. For example, there are a number of efforts to develop tokens for e-commerce transactions to replace card numbers in processing. The tokenization schemes work similarly, and if they all go to market, much of the processing chain will need costly upgrades to integrate with token systems that address the same security weakness.

A second long-run principle places emphasis on compliance with security standards over the speed of their development. While proprietary standards may be quick to develop, research suggests that an inclusive and cooperative development process, such as that provided by the American National Standards Institute, improves motivation to comply with standards (Greenstein and Stango). In any large and diverse payment system, even well-designed security standards will be adopted unevenly across participants, so it is critical to motivate participants to comply. Some delay in developing security standards may be valuable overall if more payment participants adhere to the standards.

Incentives are crucial to encourage good security practices among all payment participants. For check payments, statutory law sets the basic rules to allocate liability for fraud losses. The rules use a basic principle that the entity in the best position to deter check fraud will bear the losses for a check it processes.[26] This principle of assigning liability to the control point best suited to prevent fraud provides strong incentive to detect and deter fraud in a cost-effective manner.[27] The check system has attained low fraud loss rates without a central authority implementing significant rules or oversight.

Applying the same principle to data could help protect sensitive data on home computers. Malware, such as key loggers installed on desktop computers, gives fraudsters login credentials of consumer or business payment accounts. Stolen credentials allow unauthorized access to online banking systems and thus the ability to initiate fraudulent payments. Devising systems to prevent malware is a challenge because many users are unable to protect their computers. Financial institutions often refuse to provide security advice or anti-virus software because they may bear liability if their customers' computers become infected.

A better control point is the Internet service provider (ISP) (Moore). ISPs have the ability to monitor their users' Internet traffic to detect malware infections.[28] Because responsibility for malware is unclear, ISPs resist regulatory requirements to detect and clean up infected computers. An alternative is to make ISPs legally responsible for the damage caused by infected computers on their network but at the same time provide incentives and compensation if the ISPs assist customers in securing their computers.[29]

Improving the security of home computers could reduce fraud on all forms of payments. The key is to provide the correct incentives to effectively control security risks. Implementation requires changing laws concerning liability over damage due to malware and creating institutions to coordinate efforts to prevent and remediate malware.

Along these same lines, some have proposed strengthening breach disclosure laws (Schuman; Bjorhus and Spencer). Research has found that requiring payment participants to disclose data breaches provides incentives to better protect data (Romanosky and others). Another proposal would give additional incentive to merchants to comply with PCI standards by providing some relief from liability for data breaches if the merchant is validated as compliant at the time of the breach (Schuman).

IV. CONCLUSION

The payment industry is working hard to protect payment data, improve security, and prevent fraud. The options to improve security discussed in this article, while representing only a subset of possible approaches to strengthen security, involve all elements of the control structure—governance, rules, security technology, and enforcement. Correcting misaligned incentives to secure payments may require multiple changes to the control structure. These changes may require significant coordination and cooperation across the payment system.

Fraudsters are attacking payment systems to obtain sensitive data useful for payment fraud with a vigor unseen in the past. Data security would be enhanced by immediate acceleration of private and public efforts encouraging payment participants to adopt effective security protocols. The payment industry should consider improving elements of the control structure to better protect payments and respond to attacks with initiatives that promote information sharing on security threats. Shared

security techniques, protocols, and standards would also help. Furthermore, the payment industry should provide data measuring progress in payment security as well as weaknesses that require attention.

Because of the modern payment system's complexity, policymakers and industry leaders need a broad perspective to judge weaknesses in the control structure over payment security and the control structure's ability to adapt as new fraud methods arrive. A long-term perspective is especially important because fraudsters' incentives to exploit security weaknesses will not disappear. Critical contributions to the control of payment fraud will continue to come from private security services. Improvement could also come from contributions that take a payment system-wide approach, such as a group coordinating diverse payment participants, promoting cooperation, and finding effective solutions to weak payment security.

APPENDIX

ELEMENTS OF THE CONTROL STRUCTURE OVER SECURITY RISK IN PAYMENT SYSTEMS

The control structure typically has four elements: network organization and governance, payment network rules, security techniques and protocols, and supervision and enforcement. The elements control access to the network, coordinate payment security, set operational rules that embed security features, determine responsibility for security (including liability for fraud losses), determine and design appropriate security techniques and protocols, define and oversee adherence to security standards, and apply sanctions for noncompliance.

Network organization and governance. Much of a payment network's ability to limit fraud derives from controlling access to the network (Braun and others). The network organization chooses members, typically DFIs, to control network access by screening end-users prior to providing payment services.[30] Controlling network access prevents known malefactors from using the payments network. More critically, because access to the network has value, trustworthy participants have incentive to follow the network's rules and procedures to ensure integrity and confidentiality. Networks provide a coordinating function over payment security, which is especially important in electronic payment processing, where all links of the processing chain must use common security-related processes.[31]

Payment network rules. In practice, payment security involves rules set by the payment networks. Rules must accord with laws and regulations and be tailored to specific payment types. Operational rules under which payments are processed embed security-related steps. Some network rules are devoted to protocols requiring a set of specific security techniques while others define best practices to ensure security. Networks enforce their own rules. DFIs in the network are contractually obligated to follow security rules and implement procedures to follow when an end-user suspects a fraudulent payment. Network rules may also assign liability for direct losses or indirect costs of fraud and security failures.

Security techniques and protocols. Modern payment processing systems employ electronic communication networks to carry messages

initiating, authenticating, authorizing, clearing and settling payments. Security techniques and protocols protect these communication channels.[32] Policies allow only authorized individuals access to the network. Encryption protects payment message privacy. The payment message itself can include security codes to help authenticate payers and payment instruments. If multiple networks use the same security techniques and protocols, they are typically formalized into common standards. Standards development can be closed and proprietary or open and freely available.

Supervision and enforcement. Payment networks, as well as public entities, monitor payment participants for responsible behavior, such as complying with security policies and disclosing security breaches. Sanctions may apply for noncompliance. Some payment networks enforce rules using a "delegated monitoring" system, where contracts with end-users and payment processors specify responsibilities required to protect payment security and the DFI monitors compliance with these responsibilities. Public entities, such as regulatory agencies over DFIs or the FTC over nonbanks, have legal authority to prescribe expectations for payment participants to protect confidentiality and integrity, monitor for appropriate internal controls of payment security, and sanction inappropriate behaviors. Privacy laws and regulations require strong security measures over personally identifiable information (Romanosky and others).

ENDNOTES

[1]Corporations report the most common type of payment fraud they suffer is with checks (Association for Financial Professionals).

[2]Data breaches also expose usernames and passwords. Alternatives using deception to reveal sensitive information include social engineering (fraudsters posing as legitimate individuals persuade others into revealing sensitive information) or phishing (legitimate looking but malevolent email). In an extreme form of account takeover, identity theft, fraudsters use a person's credentials to create a new account under their control. Identity theft often results in large fraud losses because the victim is unaware of transactions on the new account (Javelin). The U.S. Department of Justice estimated that 1.125 million persons in the United States suffered new account fraud in 2012, causing an average of $1,598 out-of-pocket losses to victims (Harrell and Langton).

[3]The loss is before any chargebacks or recoveries. For simplicity, this paper uses "fraud loss" to refer to the volume or value before any chargebacks or recoveries of unauthorized third-party fraud transactions. Chargebacks refer to merchants returning funds to a card-issuing bank. Chargebacks for fraud can occur in cases of e-commerce transactions if the cardholder reports that the payment was unauthorized. In this case, the merchant absorbs the loss.

[4]This is mainly a result of a decline in paper checks, which fell from 41.9 billion in 2000 to 18.3 billion in 2012 (Gerdes; Federal Reserve System 2014).

[5]Phishing emails have also increasingly targeted payment data. In the first quarter of 2014, the Anti-Phishing Working Group detected 125,000 unique phishing emails, of which 47 percent targeted payment data. The percentage has had an upward trend since mid-2011 (Anti-Phishing Working Group).

[6]A user ID and password that would allow unauthorized access to an online bank account have been increasingly targeted. In fact, user IDs may have become a target by themselves in recent years because many consumers and businesses use passwords that are easy to guess (Hachman, Javelin).

[7]The actual number of records exposed is understated because the source of the data does not report the number of records exposed in roughly 35 percent of breaches.

[8]The total loss resulting from payment fraud is important to those who bear the loss because it strongly reflects the incentive to prevent fraud. This article looks closely at the loss relative to the total value of payments because it is the most important measure of performance over time for payment security. The incidence rate (number of fraudulent transactions relative to the total number of transactions) is also useful.

[9]The loss rates on checks for 2012 differ from those shown in Table 2. The difference may be due to sampling methods or to alternative fraud definitions.

[10]ACH debit transactions are relatively risky because a third party requests funds to be withdrawn from the payer's bank account. DFIs control this risk by screening and monitoring organizations that initiate ACH debits.

[11]Research is addressing methods to disrupt fraud from stolen data (Peacock and Friedman).

[12]Respondents to a survey reported a loss rate of 0.057 percent of purchase value for signature debit transactions in 2013, up from 0.054 percent in 2012 (Pulse Network). For PIN debit, respondents reported a loss rate of 0.0073 percent of purchase value in 2013, up from 0.0065 percent in 2012.

[13]For example, claims of high-quality security software are hard to verify (Moore).

[14]Computer-chip card adoption is a good example of a chicken-and-egg problem. Card-issuing banks have little incentive to replace magnetic stripe cards with more expensive chip cards until a large number of merchants have installed terminals that can read them. But merchants have little incentive to invest in new terminals unless they expect many banks provide those cards to their customers.

[15]In another study, Grossklags and others modeled security defenses that were either protection (firewalls, antivirus, patching) or loss management (backup facilities, insurance). Under some assumptions, strategic uncertainty may lead to more effort to protect than is socially optimal.

[16]For a more complete discussion of weaknesses and improvement opportunities in U.S. payment security, see Federal Reserve Financial Services, "Ensuring Payment Security in the United States," available at *http://fedpaymentsimprovement.org/wp-content/uploads/payments_security_roundtable.pdf.*

[17]In January 2014, Foursquare disclosed a breach exposing 45 million email addresses, and in September 2014, Home Depot disclosed a breach exposing data on 56 million payment cards.

[18]From 2008 to 2013, an average of 14,732 commercial banks, savings institutions, and credit unions operated. These organizations publicly disclosed 207 data breaches for an incidence rate of 0.23 percent. In the same period, an average of 1.95 million merchants operated and disclosed 1,486 data breaches for an incidence rate of 0.02 percent. The gap widens if only larger organizations (greater than nine employees) are included. The incidence rates for other sectors are Education, 0.05 percent; Insurance and Finance, 0.01 percent; Medicine, 0.01 percent.

[19]The card brands are American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. The council has standards for securing card data, computer applications used to process card payments, and payment terminals used for card transactions requiring a PIN. The card networks monitor and enforce standards for the issuers, processors, and card-accepting merchants in their networks.

[20]From 2008 to 2013, breaches at retailers exposed 862 million records but those at DFIs exposed 6 million records.

[21]By contrast, victims of property crime lost $14 million.

[22]In 2011, regulators issued guidance that recommended additional steps to authenticate users in online banking systems, rendering stolen data less useful for account takeover (Federal Financial Institutions Examination Council 2011). Enhanced authentication, however, does not directly help prevent data breaches at financial institutions.

[23]These cards will use the Europay, MasterCard, and Visa (EMV) payment card specification, a suite of protocols for cards with an embedded computer chip. Card issuers have adopted EMV cards worldwide.

[24]An enhanced authentication process called 3D secure has proven effective at reducing payment fraud in e-commerce (Financial Fraud Action U.K.). In 3D secure systems, an e-commerce transaction requires an additional step where the cardholder enters a password or a special code transmitted to a mobile device.

[25]Card issuers have sophisticated transaction analysis systems that can rapidly identify fraudulent card payments. However, thieves are aware of this and will likely be able to complete a few fraudulent purchases before the card is deactivated.

[26]In economic terms, the optimal control point should use a least-cost method to enhance security (Levitin). The payer's bank, for example, can best determine whether the payer's signature on a check is genuine, and the payee's bank can best determine whether the payee's endorsement on the check is genuine. The payee must also exercise care in accepting a check, such as confirming the identity and signature of the individual who writes the check. If not, the payee may bear some responsibility for a fraudulent check.

[27]This principle applies to check payments in both statutes and in regulations. The Federal Reserve updated Regulation CC in 2005 so that the depository bank warrants that the account holder authorized by telephone a check created remotely by the merchant. The merchant is a customer of the depository bank, and the bank is in the best position to monitor the merchant for excessive rates of unauthorized, remotely created checks. This could mean the depository bank bears the loss of the unauthorized payment. The legal status of remotely created payment orders is uncertain (Douglass). The Federal Reserve has recently proposed new changes to Regulation CC to make any electronically created items subject to similar warrantees (see *www.gpo.gov/fdsys/pkg/FR-2014-02-04/pdf/2013-30024.pdf*).

[28]Malware is often distributed via botnets, a network of computers with software clandestinely installed to give control to the attacker. The attacker can then install key loggers to capture credentials or use services such as email to send out large numbers of fake messages that can fool recipients into revealing login credentials.

[29]The ISP could avoid liability if it has services to clean up and protect its customers' computers (Moore). ISPs, governments, software companies (whose software may not be protected against infection), and consumers could share the costs of cleanup.

[30]Membership of a DFI in a payment network can sometimes occur through a relationship to a larger DFI. For example, smaller DFI access to Federal Reserve

Bank reserve accounts and to wire services may be through correspondents, corporate credit unions or bankers' banks. Similarly, a smaller DFI may gain access to card networks through a larger DFI's sponsorship. Many networks and DFIs outsource payment processing to third-party service providers. Networks and DFIs grant access to service providers under contracts obligating the providers to operate securely and follow network security requirements.

[31]In some cases, networks have support organizations that coordinate security-related functions, such as NACHA for ACH and the PCI Council for credit card networks.

[32]Some payment networks provide real-time information to confirm payment accounts. Computerized analysis predicts the probability of a fraudulent payment and helps the paying bank approve a payment correctly.

REFERENCES

American Bankers Association. 2013. "2012 Deposit Account Fraud Survey Report."

_____. 2011. "2010 Deposit Account Fraud Survey Report."

_____. 2009. "2008 Deposit Account Fraud Survey Report."

_____. 2007. "2006 Deposit Account Fraud Survey Report."

Anti-Phishing Working Group. 2014. "Phishing Activities Trends Report," available at *http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf*.

Association for Financial Professionals. 2014. "Payments Fraud and Control Survey." April.

Associated Press, The. 2014. "Cards From Target Breach Being Sold in Custom Sets, Police Say," *New York Times*, January 20.

Australian Payments Clearing Association. 2014 and earlier issues. "Payment Statistics."

Bjorhus, Jennifer, and Jim Spencer. 2014. "Financial, retail industries keep cybersecurity mistakes secret," *Star Tribune*, February 23.

Blank, Christine. 2013. "Counterfeit Card Scheme Costs Retailers $2 Million." *FierceRetailIT*, available at *http://www.fierceretail.com/retailit/story/counterfeit-card-scheme-costs-retailers-2-million*. December 18.

Board of Governors. 2013. "2011 Interchange Fee Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions."

_____. 2011. "2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions."

Böhme, Rainer, and Tyler Moore. 2010. "The Iterated Weakest Link," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 53-55.

Braun, Michele, Jamie McAndrews, William Roberds, and Richard Sullivan. 2008. "Understanding Risk Management in Emerging Retail Payments," Federal Reserve Bank of New York, *Economic Policy Review,* vol. 14, no. 2, pp. 137-159., September.

Canadian Bankers Association. 2014a and earlier issues. "Credit Card Fraud and Interac Debit Card Fraud Statistics."

_____. 2014b and earlier issues. "Credit Card Statistics—Visa and Mastercard."

Digital Transactions News. 2013a. "Why ATM Skimming Fraud Jumped Ahead of Point-of-Sale Skimming in 2012," available at *http://www.digitaltransactions.net/ news/story/3929*. March 25.

_____. 2013b. "Citing Fraud Risk, the FTC Seeks to Bar Telemarketers from Using Four Payment Methods," available at *http://www.digitaltransactions.net/news/story/4001*. May 23.

Douglass, Duncan. 2012. "What Are EPSs, Do We Need Them and If They're So Great, Why Aren't They More Common?" Presentation to the Payments Symposium, Federal Reserve Bank of Chicago, available at *http://chicagopaymentssymposium.org/wp-content/uploads/2013/10/Electronification-Duncan-Douglas-ChicagoFedConferencePresentationFall2013.pdf*.

European Central Bank. 2014. "Third Report on Card Fraud." February.

_____. 2013. "Second Report on Card Fraud." July.

_____. 2012. "Report on Card Fraud." July.

Federal Financial Institutions Examination Council. 2014. "Executive Leadership of Cybersecurity," available at *http://docs.ismgcorp.com/files/external/FFIEC_CCIWG_Cybersecurity_Draft_Webinar.pdf*. May 7.

_____. 2011. "Supplement to Authentication in an Internet Banking Environment," available at *http://www.ffiec.gov/pdf/auth-its-final%206-22-11%20%28ffiec%20formated%29.pdf*.

Federal Reserve System. 2014. "The 2013 Federal Reserve Payments Study."

_____. 2011. "The 2009 Federal Reserve Payments Study."

_____. 2007. "The 2006 Federal Reserve Payments Study."

_____. 2008. "The Check Sample Study."

Financial Fraud Action U.K. 2014. "Fraud the Facts," available at *http://www.financialfraudaction.org.uk/download.asp?file=2796*.

Gerdes, Geoff. 2008. "Recent Payment Trends in the United States," *Federal Reserve Bulletin*. October.

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

Grossklags, Jens, Nicolas Christin, and John Chuang. 2008. "Secure or Insecure?: a Game-theoretic Analysis of Information Security Games," *Proceedings of the 17th International Conference on World Wide Web*, April, pp. 209-218.

Hachman, Mark. 2010. "RockYou Hack Reveals the Worst 20 Passwords," *PC Magazine*, January 21.

Harrell, Erika, and Lynn Langton. 2013. "Victims of Identity Theft," *Bulletin.* Bureau of Justice Statistics, December.

Hirshleifer, Jack. 1983. "From Weakest Link to Best Shot: The Voluntary Provision of Public Goods," *Public Choice,* vol. 41, no. 3, pp. 371–386 .

Interac. 2014. "Research and Statistics," available at *http://www.interac.ca/media/stats.php*.

Javelin. 2014. "Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends," February.

Kitten, Tracy. 2014. "FFIEC Cyber Assessments: What to Expect," Bank Info Security, available at *http://bankinfosecurity.com/ffiec-a-6831/op-1*. May 12.

Krebs, Brian. 2014a. "Target Hackers Broke in Via HVAC Company," *Krebs on Security,* available at *http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company.* February 5.

_____. 2014b. "Fire Sale on Cards Stolen in Target Breach," *Krebs on Security,* available at *http://krebsonsecurity.com/2014/02/fire-sale-on-cards-stolen-in-target-breach/#more-25029*. February 19.

_____. 2013b. "Non-US Cards Used At Target Fetch Premium," *Krebs on Security,* available at *http://krebsonsecurity.com/2013/12/non-us-cards-used-at-target-fetch-premium/*. December 22.

Levitin, Adam J. 2010. "Private Disordering? Payment Card Fraud Liability Rules," *Brooklyn Journal of Corporate Financial and Commercial Law,* vol. 5, no. 1, pp. 1-48.

Mallow, Michael L., and Michael A. Thurman. 2013. "FTC cracks down on payment processors," Loeb & Loeb LLP USA, available at *http://www.lexology.com/library/detail.aspx ?g=674216fb-6af4-439b-a9fa-f8339f044ea3.* December 16.

Moore, Tyler. 2010. "The Economics of Cybersecurity: Principles and Policy Options," *International Journal of Critical Infrastructure Protection,* vol. 3, no. 3-4, pp. 103-117.

NACHA. 2014. "ACH Volume Grows to Nearly 22 Billion Payments in 2013," available at *http://www.nacha.org/news/ach-volume-grows-nearly-22-billion-payments-2013.* April 7.

Peacock, Timothy, and Allan Friedman. 2014. "Automation and Disruption in Stolen Payment Card Markets," *The 13th Annual Workshop on the Economics of Information Security*, available at *http://weis2014.econinfosec.org/papers/PeacockFriedman-WEIS2014.pdf.*

Petru, Alexis. 2014. "Can Companies Restore Consumer Confidence After a Data Breach?" *TriplePundit,* available at *http://www.triplepundit.com/2014/07/can-companies-restore-consumer-confidence-data-breach/.* July 8.

Pulse Network. 2014. "Debit Issuer Study: Executive Summary."

Risk Based Security. 2014. Data Loss Database.

Robertson, Jordon. 2014. "Why So Many Retail Stores Get Hacked for Credit Card Data," *Business Week,* March 20.

Romanosky, Sasha, and others. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management*, vol. 30, no. 2, pp. 256-286.

Schuman, Evan. 2014 "One Law to Rule All Data Breaches—but Let's Make It a Real Law," *Computerworld,* May 13.

Sullivan, Richard. 2013. "The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud." Federal Reserve Bank of Kansas City, *Economic Review,* vol. 98, no. 1, pp. 59-87.

U.K. Cards Association. 2013. "Card Expenditure Statistics," available at *http://www.theukcardsassociation.org.uk.* December.

Varian, Hal R. 2004. "System Reliability and Free Riding," in *Economics of Information Security*, Jean Camp and Stephen Lewis, eds. Springer Science+Business Media.

Zetter, Kim. 2014. "Will Target's Lawsuit Finally Expose the Failings of Security Audits?" *Wired Magazine*, March 28.