Clarifying liability for twenty-first-century payment fraud

Sandeep Dhameja, Katy Jacob, and Richard D. Porter

Introduction and summary

At present, it is difficult to identify clear-cut guidance for preventing and mitigating fraud in retail payments in the United States.[1] Part of the difficulty stems from the fact that the U.S. retail payment system has a decentralized governance structure. The Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau (CFPB) play an important role in developing and implementing guidance to curb retail payment fraud in the nation. However, in very large part, fraud prevention and mitigation are the primary responsibilities of the numerous entities running the various electronic and paper-based payment schemes across the country. These schemes include those for payments made via the automated clearinghouse (ACH) system, payment cards (credit, debit, and prepaid cards), and imaged and paper checks. Federal, state, and local law enforcement agencies investigate instances of fraud, identity theft, and data breaches related to retail payments, but not pursuant to any established overarching policies or goals set by a central authority for all retail payments. Payment transactions, whether conducted domestically or abroad, are at risk for fraud orchestrated from anywhere in the world and, therefore, might rightfully fall under the jurisdiction of foreign authorities. Hence, international, federal, and state or local agencies may be responsible for the regulation, supervision, and investigation of retail payments, as well as the enforcement of the laws and rules pertaining to retail payment fraud.

Establishing specific, overarching governance objectives for retail payments is becoming increasingly important in light of the growing complexity of the U.S. retail payment system. Setting up such objectives is becoming particularly vital as far as transaction security is concerned. Over the years, more and more nonbank firms (such as retailers and technology firms) have entered the payments market, competing with banks, which are regulated and supervised differently. Additionally, many seemingly simple payment transactions nowadays actually represent the interests of as many

Sandeep Dhameja is a risk-management team leader in the Supervision and Regulation Department at the Federal Reserve Bank of Chicago. Katy Jacob is a payments information consultant in the Payments Information and Outreach Office at the Federal Reserve Bank of Minneapolis and was a business economist in the Economic Research Department at the Federal Reserve Bank of Chicago while writing this article. Richard D. Porter is a vice president and senior policy advisor in the Economic Research Department at the Federal Reserve Bank of Chicago.

The authors thank the following individuals for their comments on earlier drafts of this article: Duncan Douglass, Alston & Bird; Jane Larimer, NACHA; and David Walker, ECCHO. The authors also thank the following individuals for their participation in a meeting to develop the ideas for this article: Carol Coye Benson, Glenbrook Partners; Peter Burns, Heartland Payment Systems; BC Krishna, MineralTree; John Morton, Green Dot Corporation; and Paul Tomasofsky, Secure Remote Payment Council.

Economic Perspectives is published by the Economic Research Department of the Federal Reserve Bank of Chicago. The views expressed are the authors' and do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Federal Reserve System.

ISSN 0164-0682

as a dozen parties.[2] Given these two factors, the determination of who has responsibility or liability for which specific payment-related activity can easily become obscured.

Further, the United States lacks a uniform set of consumer disclosures, error resolution techniques, and liability allocation structures for retail payments. Hence, determining who's responsible or liable can be quite difficult in instances of payment fraud. When payment fraud occurs, liability must be clearly assigned so that end-users of the payment system (such as consumers and merchants) are made whole and so that their trust in the overall architecture and integrity of the system is maintained. Processing retail payment transactions is quite complex, often involving multiple points of access to the payment system, many of which criminals can manipulate to commit fraud. It is important to determine which party in the transaction processing chain is responsible for handling fraud events, and it is vital for the rights and responsibilities of all the parties along the chain to be clearly defined. Ideally, fraud events should be managed by the parties (both banks and nonbanks) that are in the best position to stop them from occurring or can best mitigate them when they do occur. And, of course, the criminals directly responsible for the fraud should be held liable whenever possible. Unfortunately, in most cases, perpetrators are not found quickly, if at all, and it can be difficult to bring charges against them. As a consequence, attention shifts to various legitimate participants involved in carrying out the payment transaction in order to determine fraud liability.

In this article, we explain the governance structure of retail payments in the United States. We then provide an overview of payment fraud. Following that, we discuss in depth the liability frameworks for fraud involving specific payment methods (check, ACH, and payment cards). Some of our analysis is derived from extensive interviews with experts in the payments industry.[3] Finally, we suggest a series of recommendations that describe how the public sector might work together with private organizations in the payments industry to clarify fraud liability.

Governance structure of U.S. retail payments

The United States currently has no overarching regulatory body or industry association that oversees all retail payments. When checks and paper currency were the dominant methods of payment, the Federal Reserve System played a central role in governing retail payments. But today, following the rise of various electronic forms of payment, specific governance objectives for the payment system as a whole are largely undefined. While several federal agencies are involved with retail payments in some way, across-the-board objectives governing these payments often do not reach a high level of specificity. For example, at this point, there is no government mandate to determine who would have primary responsibility for defining and enforcing security measures for all U.S. retail payments.

A variety of federal agencies—including the Federal Reserve System,[4] the CFPB, the U.S. Department of Justice, the Federal Bureau of Investigation (FBI), and the U.S. Secret Service—as well as state agencies have some purview over payment policy and payment fraud issues. Both banks and nonbank institutions act as payment providers in the United States, and a variety of U.S. laws and regulations apply to their activities. For example, certain nonbanks in markets for consumer financial products and services may be determined by the CFPB to be "larger participants" and, therefore, be subject to its direct supervision.[5] Other nonbanks operating under state money transmitter licenses are subject to state agency supervision. There are also a variety of state laws that address consumer rights in instances of identity theft or data breaches.[6]

Still, by and large, the retail payments industry in the United States is self-governing and balkanized. Each payment scheme operates on a competitive platform with its own set of practices and procedures.[7] Because there is no overarching regulatory body or industry association responsible for all retail payments in the United States, when payment system security questions arise, industry players will consult payment scheme owners, such as NACHA[8] (which administrates the ACH network), or other industry-sponsored groups, such as the Accredited Standards Committee X9 Incorporated (ASC X9 Inc.), ECCHO (Electronic Check Clearing House Organization), and the PCI (Payment Card Industry) Security Standards Council (see appendix 1 for details). All of these groups operate independently (although the public sector, including the Federal Reserve System, is significantly involved in many of them). So, when it comes to fraud and security standards, the industry itself makes most of the rules, but without the broad consensus that an overarching organization from either the public sector or private sector might achieve.

An overview of payment fraud

Payment fraud, which is manifested in a variety of ways, can be broadly defined as any activity that uses confidential personal (or financial) information for unlawful gain, including criminals initiating transactions without the consent or authorization of the payer. Specifically, such activities include counterfeiting, deception, altering payment instruments, hacking, and data interception. Payment fraud can happen at any point along the transaction processing chain.

Over the years, the transaction processing chain has become increasingly complex as new players (mostly nonbank firms) have entered the payments market and as new payment products and services have quickly gained popularity; most transactions nowadays often involve multiple parties, including third-party vendors and processors. More specifically, new physical forms to complete electronic payments have emerged and gained traction in recent years—for instance, some consumers can now use contactless cards (payment cards that use chip technology to allow for tap-and-go payments) and mobile devices to complete their transactions. Also, electronic payments can now be made at many more venues—for example, nonbank financial centers (including check cashers and retail stores), vending machines, and taxis. Indeed, a rapidly increasing number of payees are accepting electronic forms of payment, and these payments are often facilitated by nonbank firms, many of which have no prior experience in providing or securing payment services.

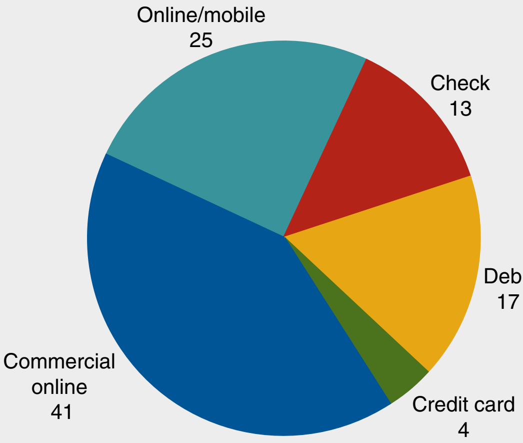
As emerging payment channels (such as online and mobile payments) substitute more and more for legacy payment methods (such as paper checks), financial institutions are naturally shifting the emphasis of their fraud prevention and mitigation strategies to the new channels. For example, in 2011, Aite Group researchers conducted interviews with financial institution officials and found that technology investments for fraud prevention and mitigation were being shifted toward business units for online and mobile payment channels (see figure 1).

Moreover, as the new payment channels have become more popular, the number of access points along the payment chain have grown markedly, giving fraudsters more opportunities to commit crimes and increasing the security challenges for all legitimate participants. Payment fraud is constantly evolving as criminals discover new ways to thwart the efforts of financial institutions and other interested parties to protect transaction data. Indeed, the techniques employed by fraudsters are numerous and are adapted to overcome new protection measures; we discuss some of the techniques that pose threats to electronic payments in box 1.

Many of the access points exploited to commit fraud are *not* controlled by the institutions (mostly banks) that hold the underlying funds, even though these institutions may be ultimately liable for the fraud losses that occur. The majority of the current laws and regulations covering payment fraud refer to the institutions that guarantee or issue the funds—namely, banks. Thus, the incentives to properly secure transactional information for individual customers and nonbank firms facilitating retail payments may be obscured. In other words, given the liability frameworks at present, individual customers and nonbanks are not always liable for fraud occurring on their watch, so they may not be taking adequate measures to reduce payment fraud.

FIGURE 1

Payment channel with highest priority for fraud prevention technology investment



Notes: This figure is based on the Aite Group researchers' interviews with officials from 32 North American financial institutions over the period August through October 2011. The pie chart slices represent the percentages of financial institutions surveyed that cited the particular channel as their highest priority for fraud prevention technology investment.
Source: Aite Group.

Because payment practices are changing faster than the laws and regulations that govern them, the assignation of liability when fraud occurs is quite complicated in the current payments landscape. Collaboration within and among both banks and nonbank firms is necessary for successful payment fraud management, since security is so expensive to achieve and maintain. In order to be effective, efforts to prevent and mitigate payment fraud need to involve all parties “touching” the payment transactions. Additionally, the incentives of the parties to act optimally to ensure the security of the transaction (data) must be properly aligned with those of one other. As we will explain, the laws and regulations for retail payments differ greatly depending on the type of payment used, the method of processing the payment, and other factors; therefore, it is yet unclear if incentives for fraud prevention and mitigation are adequate for all parties involved in each transaction.

BOX 1

Threats to electronic payments

Here we discuss some of the threats to electronic payments. More specifically, we explain some of the techniques used to commit payment-related cybercrime, as well as cybercrime that indirectly affects financial services.

Hacking

Hacking is accessing information assets without proper authorization by thwarting security mechanisms. Hacking is usually conducted remotely and anonymously. The most well-known hacking incidents of late have involved the exploitation of default or easily guessable credentials; the use of stolen login credentials; brute force (for example, attacks that systematically try every possible combination of letters, numbers, and symbols until the correct combination grants access); "dictionary attacks," or strategies involving systematically entering every word in a dictionary as a password to access password-protected servers or encrypted information; and the exploitation of insufficient authentication protocols. Over the past few years, two of the most prominent payment-related hacking events occurred at Global Payments—an electronic transaction processor used by Visa and MasterCard—and at Citigroup.[1] Additionally, two breaches occurred in late 2012 and early 2013 (one at India-based card processor ElectraCard Services), leading to $45 million in stolen funds from automated teller machines (ATMs) around the world; the breaches were made to raise the balances and withdrawal limits on prepaid cards used in the theft (Nair and Dye, 2013). Prior to all of those events, the RBS WorldPay breach resulted in a number of prepaid payroll cards being compromised in 2008. These cards were used to obtain $9 million in cash in one day from ATMs located in several dozen cities around the world (Krebs, 2009a).

Malware

Of the 44 million records compromised through the 621 confirmed data breaches in 2012, 40 percent were due at least in part to malware, or malicious software (Verizon RISK Team, 2013, pp. 11, 29). Malware is designed and used for the purpose of compromising or harming information assets without the owner's informed consent. Malware attacks are designed to run covertly. Examples of malware are computer viruses, Trojan horses, and spyware. Malware is no longer simply used to gain a point of entry for hacking; rather, it also often serves as a means to remain in control after gaining access to a computer system, especially for financially motivated crimes. Pathways for malware infection include the following: installation or injection by remote attacker; targeted email with an infected attachment; web-based automatically executed "drive-by" download; and user-executed download (for example, from an advertisement on a legitimate website).

Once in the system, malware performs a variety of harmful activities, each serving one or more of three basic purposes: to enable or prolong access while disguising its presence; to harvest data of interest; and to further the attack in another manner. Increasing uses of malware include the following: logging keystrokes (and other user inputs); sending victims' data to external locations either in real time or in batches using encrypted channels of communications; and bypassing normal authentication/security mechanisms to control systems remotely.

One quite complex form of malware-related cybercrime committed against financial firms has been dubbed by some experts as "Operation High Roller." In this type of attack, large amounts of money are siphoned from high-balance accounts with no human action required. Servers are programmed to automate the thefts through wire transactions from special-purpose commercial and investment accounts. Specific strategies using this form of attack have emerged in the European Union (EU), Latin America, and the United States; the attacks have been altered from focusing on the accounts of individual retail customers to business accounts. Financial institutions of all sizes—from the largest banks to the smallest credit unions—have been targeted. Most malware attacks rely on social engineering (that is, human manipulation of people for them to break normal security procedures or divulge confidential information), as well as on remote technical manipulation, to succeed. However, the Operation High Roller attacks are completely automated from start to finish and are able to bypass even multifactor authentication systems.[2] Such attacks were developed specifically to thwart bank-fraud-detection standards (for example, by making only one transaction per account and never exceeding the dollar transfer limits that trigger suspicion) at even the most sophisticated and well-resourced institutions (Marcus and Sherstobitoff, 2012).

Indirect effects of cybercrime

There are many examples of electronic malfeasance that are not related to payments per se. They include advanced malware such as Flame (a cyberespionage program)[3] or Stuxnet (a cyberweapon designed to destroy other software and computer systems). Although these two pieces of software may not be necessarily linked directly to financial fraud, variants based on

BOX 1 (CONTINUED)

Threats to electronic payments

them and other advanced malware can unquestionably affect the integrity of retail payment systems. Using these variants and other cyberweapons, organized groups all over the globe can conduct cyberattacks that affect payments, even if they are not necessarily motivated solely by monetary gain.

For example, in September 2012, cyberattacks on some of the largest banks challenged their computer defenses in the first documented large-scale "distributed denial-of-service" (DDoS) attacks (Strohm and Engleman, 2012). These attacks flooded bank websites with Internet traffic, rendering them unreachable by their customers for various lengths of time. Such attacks can have adverse effects on payments, even if no payment-specific data are compromised or bank account funds are stolen, since consumers and businesses are unable to access their accounts online to pay bills or make purchases.

[1] For more information on payment card data breaches, see appendix 2. Also see Cheney et al. (2012).

[2] Multifactor authentication is an approach to validating the user by requiring the presentation of two or more authentication factors: a knowledge factor (something the user knows, for example, a password or personal identification number), a possession factor (something the user has, for example, a payment card or mobile phone), and an inherence factor (something the user is, for example, a user's biometric characteristic, such as a fingerprint or voiceprint).

[3] Flame provides the attacker remote access to an infected computer with control of many of its functions, such as its microphone and webcam. For further details, see Zetter (2012).

Who is liable for losses from payment fraud?

Fraud reduces the efficiency of the payment system because it degrades operational performance and increases costs—not only for the parties whose payments are compromised but also for everyone participating in the system.[9] When executed successfully, payment fraud can lead to adverse consequences for participants at different points along the transaction processing chain. For instance, when a criminal steals a payment card and uses it (or its information) to purchase an item, the legitimate cardholder's liability for the fraudulent transaction is limited by statute or regulation. However, participants further down the payment chain—such as the card-issuing bank or a merchant—are often likely to incur losses for such fraudulent transactions.[10]

Table 1 outlines several different types of fraud, as well as some potential strategies for preventing and mitigating them. These strategies include know-your-customer (KYC) protocols, fraud reviews, anti-money-laundering (AML) rules, the Bank Secrecy Act (BSA)[11] and Office of Foreign Assets Control (OFAC)[12] requirements, and suspicious activity reports (SARs), which are made to the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). These strategies can be used to attempt to prevent fraud before it happens or to lessen the impacts of fraud when it does occur, and they are primarily focused on or applicable to regulated financial institutions (banks) as opposed to nonbank participants in the payment chain. This emphasis makes sense because, as we have mentioned before, the majority of the laws and regulations covering payment fraud refer to the institutions that guarantee or issue the funds—that is, banks. Moreover, as we will see later, ultimate liability for making customers (individuals and businesses) whole when payment fraud occurs often lies with these institutions as well.

The safeguards outlined in table 1 help financial institutions, merchants, and others along the payment chain manage their payment fraud risk. However, when fraud does occur, liability must be assessed and losses allocated. Ideally, the party with the most control over fraud prevention and mitigation would also be the one that bears the most liability and absorbs the highest loss. However, we find that in reality, payment fraud liability is much more complicated. A discussion of liability issues for different types of payment fraud follows.

Check fraud liability

Most consumers and businesses are aware of how check fraud has taken place historically. Forgery of checks and "passing bad checks" are well-known concepts. The *2013 AFP Payments Fraud and Control Survey* (which mostly reports on payment fraud for corporations such as large merchants, as opposed to financial institutions) finds that checks are the payment type most often targeted by fraudsters. Among the surveyed firms, 87 percent of them experienced attempted or actual check fraud in 2012 (compared with 27 percent that experienced ACH debit fraud and 29 percent that experienced corporate and commercial payment card fraud). Moreover, 69 percent of the surveyed firms that suffered losses as result of payment fraud stated that they did so primarily on account of check fraud (Association for Financial Professionals, 2013, pp. 5, 9).

TABLE 1

Types of fraud and related prevention and mitigation strategies

Type of fraud	Prevention and mitigation strategies
Automated clearinghouse (ACH) debit fraud: Unauthorized ACH entries resulting in losses to the receiving bank (that is, the receiving depository financial institution, or RDFI) and/or its corporate customers	• Protect privacy of customer demand deposit account (DDA) data • Offer positive pay[a] and debit blocks[b] • Respond to unauthorized transactions in a timely matter
ACH debit fraud: Unauthorized ACH entries resulting in losses to the originating bank (that is, originating depository financial institution, or ODFI)	• Perform due diligence on prospective ACH originator before allowing ACH initiation • Perform risk-based review of originator's authorization forms and processes • Monitor ACH return[c] rates of originator and third party
Check fraud: Check kiting from accounts with insufficient funds	• Monitor accounts for suspicious activity • Clear items quickly or immediately
Check fraud: Counterfeit or unauthorized remotely created checks (RCCs)[d] deposited	• Perform due diligence on all customers depositing RCCs
Check fraud: Dual presentment/deposit of a remotely deposited check results in loss from insufficient funds	• Audit customers before opening DDAs • Train frontline staff to recognize suspicious activity • Monitor customer behavior and flag suspicious items • Perform manual review and delay posting on all suspected items above a certain dollar threshold
Payment card fraud: Legitimate cards stolen and used to make illegitimate transactions	• Monitor accounts for unusual activity and immediately contact cardholders to verify transactions • Educate customers on their rights and responsibilities and emphasize the importance of monitoring statements
Payment card fraud: Identity or card information stolen and used to create counterfeit cards	• Monitor accounts for suspicious activity • Monitor automated teller machines and encourage merchants to monitor point-of-sale terminals for skimming[e] devices • Educate consumers on their rights and responsibilities
Wire transfer fraud: Information stolen and used to initiate unauthorized wire transfers	• Educate customers about phishing[f] and methods of data protection • Monitor online banking portals for unauthorized access • Establish and maintain processes, such as callbacks, to identify and stop fraudulent transactions

[a] ACH positive pay is a fraud detection service; it lets customers safeguard against fraudulent activity by filtering or blocking unauthorized ACH transactions according to criteria set by the customers (usually firms).

[b] Debit blocks refer to the practice of disallowing regular ACH debits without specific advance permission from the payer.

[c] ACH returns are ACH debits returned to the ODFI (either unpaid or for a refund) by the RDFI for any reason (including insufficient funds, an incorrect bank account number, and lack of authorization per the payer).

[d] Remotely created checks are checks that do not bear the signature of a person on whose account the checks are drawn; instead of the signature, RCCs bear the account holder's printed or typed name or a statement of the account holder's authorization of the checks; for more details, see http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/payment-instruments,-clearing,-and-settlement/check-based-payments/remotely-created-checks.aspx.

[e] A skimming device is one that is mounted to an automated teller machine or point-of-sale machine to copy encoded data from the magnetic stripe on the back of a payment card; for more information on skimming, see www.spamlaws.com/online-credit-card-fraud.html.

[f] A phishing attack uses randomly distributed emails to attempt to trick recipients into disclosing personal information, such as account numbers, passwords, or Social Security numbers; for more information on phishing, see www.spamlaws.com/online-credit-card-fraud.html.

Notes: This table should not be interpreted as being a comprehensive list of the appropriate processes to prevent and mitigate various forms of fraud but rather as a brief introduction to some of the important means that are currently in use. Some of the content in this table was adapted from information from The Clearing House.

Undoubtedly, vigilance to prevent or mitigate check fraud remains a high priority for overall fraud prevention because the stolen amounts are sizable. According to the American Bankers Association's *2011 Deposit Account Fraud Survey*, 73 percent of banks reported that they suffered check fraud losses totaling approximately $893 million in 2010. However, *attempted* check fraud against bank deposit accounts resulted in around $11 billion in actual losses and expenses incurred to avoid losses in 2010. That figure was just below the $11.4 billion figure recorded for 2008.[13] In the Minneapolis Fed's *2012 Payments Fraud Survey*, 43 percent of its financial institution respondents that faced attempted payment fraud in 2011 reported checks among the top three payment types with the highest number of fraud attempts; the financial institutions surveyed were mostly small banks, with 2011 revenues under $50 million (Federal Reserve Bank of Minneapolis, Payments Information and Outreach Office, 2012, pp. 5, 9).

Thus, from these surveys, it is clear that checks today remain vulnerable to fraud. However, the acceleration of clearing time as a result of Check 21 legislation,[14] which facilitates check truncation (digital conversion) and the processing of check information electronically, has greatly reduced check exceptions (that is, checks requiring special handling to be processed) and enabled institutions to remediate fraudulent transactions in an expedited fashion. According to a recent Federal Reserve study, only 6 million imaged checks in 2009—about 0.04 percent of all imaged checks that year—were exceptions; poor image quality and data mismatching were the main reasons reported for the exceptions (Federal Reserve System, 2011, pp. 12–13). Also, only 2 percent of organizations that converted checks electronically reported that the check conversion service was used for fraud, according to the Association for Financial Professionals (2012, p. 3).

While the check market has experienced a rapid transformation from paper processing to electronic processing, the underlying structure of the parties in each transaction remains much the same: Each check transaction includes a drawer (the person who writes the check), the payee (the person to whom the check is payable), the drawee (the bank that maintains the funds on which the check is drawn), and the depository bank (the first bank to receive a check for collection). Check fraud is different from other payment fraud because primary liability for check fraud is assigned to the party that pays, as opposed to the party expecting or initiating the payment, unlike, for example, with payment card fraud. Generally speaking, in the case of check fraud, consumers are *not* exempt from liability; their accountability for check fraud is in sharp contrast with their lack of liability for most types of payment card fraud (on account of the "zero liability" policies offered to them by card issuers).

The Uniform Commercial Code (UCC)[15] assigns liability for check fraud and defines responsibilities for check issuers and paying banks under the term "ordinary care" (that is, following reasonable prevailing commercial standards). UCC articles 3 and 4 were written to assign liability to the bank that should have been able to prevent the check fraud at the lowest cost. In general, the UCC states that a drawee bank is liable for fraud claims involving the drawer's signature on the face of a check and that a depository bank is liable for fraud claims involving the payee's endorsement on the back of the check. Under sections 3-403(a) and 4-401(a) of UCC articles 3 and 4, respectively, a bank can charge items against a customer's account only if they are "properly payable" and the check is signed by an authorized individual. However, if a signature is forged, the customer may be liable for fraud losses under a variety of exceptions, including the following: if the account holder fails to exercise ordinary care; if the customer fails to reconcile statements within a reasonable time; if "comparative fault" is found;[16] or if the counterfeit is virtually identical to the original. Under the law as it has been revised over time, the burden of proof shifts back and forth between parties that are claiming that fraud has occurred. Further, the UCC *does not* impose specific time frames for restoring disputed funds into a customer's account.

Because checks are processed in many different ways, the assignation of liability has become more complicated in recent years. The electronification of check processing has altered the ways in which the liability issues are considered, at least to some extent. Check laws were written to cover paper instruments and have not necessarily been updated to reflect the digital reality of check processing today. Check 21 legislation freed financial institutions from some of the provisions of the UCC governing check transactions. The diminished importance of the UCC contrasts with the increased significance of private rules from industry bodies—such as check-image-exchange rules from ECCHO. Together, the UCC, the Expedited Funds Availability Act (EFAA), and the Federal Reserve's Regulation CC[17] (which implements the EFAA) provide legal authority for banks to exchange images of paper checks and assign liability in cases of check fraud, but the details for check image exchange are left to private agreements or clearinghouse rules. For example, banks that clear checks through the Federal Reserve System are held liable for check fraud under contracts with the Federal Reserve. In recent years, private agreements among financial institutions have taken on increased importance in ensuring that liability for check fraud is clearly assigned in transactions involving check image exchanges.

It is important to point out that a substitute check (a paper check converted into an electronic image and reconverted into a paper check[18]) is governed by Check 21 regulations. A check converted into an ACH debit is governed by the Federal Reserve's Regulation E and NACHA's operating rules.[19] Court cases involving fraudulent imaged checks are few, but have resulted in rulings that make liability issues more difficult to ascertain and settle than in the prior paper check regime.[20] Moreover, checks that are cleared via the ACH network highlight the opportunity for cross-channel fraud—where fraud takes place in one part of the payment system but impacts multiple channels (for more on cross-channel fraud, see box 2). An imaged check transaction that occurs in the absence of a contract outlining liability is not presently covered by existing check law, leading to potential disputes if fraud occurs. Private rules have attempted to correct some of the problems associated with the absence of laws covering such checks. For example, ECCHO has developed rules that assign liability for altered electronic images of checks.[21]

Remote deposit capture (RDC) further complicates the issue of check fraud because the banks processing the checks deposited via RDC can pass back the liability to customers who deposit check images. RDC refers to the ability to deposit a check without having to physically send the paper check to a bank. This process is usually done by scanning a digital image of a check (or taking a photo of the check on a smartphone using a bank-supplied application) and electronically transmitting it to the bank. Banks are more likely to offer this service to business customers, but recently RDC has begun to be used by individual customers as well. The incidence of check fraud committed via RDC may rise as this method of check depositing becomes more popular.

It should be noted that remotely created checks (RCCs) also provide a fairly new opportunity for criminals to commit fraud. An RCC, also called a demand draft, is defined as “a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn.”[22] In the absence of a signature, the RCC includes a statement indicating that the payer authorized the payment. Because RCCs do not require a signature or any other documentation to indicate authorization, fraudsters can attempt to steal funds with unauthorized RCCs. Indeed, some instances of abuse have already been found in the RCC market; recently, the Federal Trade Commission (2013) issued a rule to ban the acceptance of RCCs from telemarketers as a way to combat fraud against consumers.

Additionally, the advent of RCCs has led some criminals who might have focused on other areas of the payment system (such as the ACH system) to turn their focus back on the check realm. This has happened in part because of the lack of clear-cut rules governing RCCs, as they are not typical paper checks and liability can be unclear under UCC rules as well as state laws.

BOX 2

Cross-channel fraud liability

Payment fraud does not always occur solely within a given payment silo. In other words, criminals might use one payment channel to commit fraud in a separate payment channel. When corporations are the targets, cross-channel fraud often involves corporate account takeover; for example, credentials are stolen from a merchant’s corporate bank account after it has been hacked—that is, actual demand deposit account information is breached—and that information is used to initiate fraudulent ACH or wire transactions. In cases of cross-channel fraud against corporations, the assignation of liability can be quite convoluted. Corporate customers often do not understand that Regulation E rules do not apply to them, and the courts often determine which party has ultimate responsibility.

Cases of fraud against consumers can involve multiple payment channels as well. For example, criminals might trick consumers into revealing private account information and then use it with remotely created checks, ACH debits, and payment cards to siphon funds from their deposit accounts. As another example, criminals could steal consumer credentials from the information available on a check in order to establish a credit card in someone else’s name. Although the check might have been used to commit this fraud, this case would not be considered check fraud, potentially complicating liability assignation if the criminals are not caught.

Finally, all parties that “touch” payment transactions must contend with the potential for *internal fraud*—that is, fraud perpetrated by corporate and financial institution employees who have access to sensitive customer information. This form of fraud can affect a variety of payment channels, including check, ACH, and payment cards. The assignation of fraud liability can be quite challenging in such fraud cases—as the firms might be liable for fraud committed by their employees in some cases, while the employees themselves might face criminal charges in others.

Further, the Federal Reserve’s Regulation CC stipulates that interbank warranties “shift liability for the loss created by an unauthorized remotely created check to the depository bank” (Board of Governors of the Federal Reserve System, 2005, p. 71220). As we explained earlier, for traditional checks, a drawee bank is liable for fraud claims that involve the drawer’s signature on the face of a check and a depository bank is liable for fraud claims that involve the payee’s endorsement on the back of the check. In contrast, for RCCs, the depository bank is liable for the vast majority of fraud claims (because the drawer’s signature is not part of the check clearing process). Thus, the drawer's and drawee's incentives to reduce RCC fraud may not be correctly aligned.

ACH fraud liability

Automated clearinghouse transactions are electronic payments routed from the demand deposit account of a consumer, business, or government payer to that of a payee. In the case of an ACH *debit,* a payee initiates a debit transaction from the payer's bank account, with the funds being moved into the payee's account; this activity is usually done with the express permission of the payer. Examples of ACH debits include consumer payments on insurance premiums and mortgage loans, as well as other types of bill payments. In the case of an ACH *credit,* the payer initiates a credit transaction that shifts funds to the payee's account. Examples include direct deposits of payrolls and payments to contractors and vendors. ACH fraud events can occur in either credit or debit transactions.

The *2013 AFP Payments Fraud and Control Survey* finds that 27 percent of its respondents experienced attempted or actual fraud via ACH debits in 2012 and 8 percent experienced fraud activity in ACH credits (Association for Financial Professionals, 2013, p. 5); only 16 percent of the respondents with payment fraud losses reported that ACH fraud accounted for their greatest financial loss due to fraud.[23] Additionally, in the Minneapolis Fed's *2012 Payments Fraud Survey*, 16 percent of the financial institution respondents that faced attempted payment fraud in 2011 reported ACH debits among the top three payment types with the highest number of fraud attempts, while only 2 percent reported ACH credits among them (Federal Reserve Bank of Minneapolis, Payments Information and Outreach Office, 2012, p. 9).

New payment schemes, such as PayPal, rely on either the ACH system or payment card infrastructure; so, fraud events that occur through these alternative payment schemes might be captured in ACH fraud statistics as well. There is also the growing issue of corporate account takeover of businesses and nonprofits—which is a form of identity theft wherein criminals use malware to gain access to a party's online credentials and initiate fraudulent activity.[24] Criminals may create transactions that resemble a corporate customer's regular ACH (or wire) transactions—for example, for payroll disbursements—as a way to siphon funds. Losses from corporate account takeover grew to $4.9 billion in 2012, according to one estimate; that number represents a 69 percent increase over the previous year.[25]

According to NACHA's operating rules (and some of our interviewees), the originating depository financial institution (ODFI) involved in an ACH transaction is responsible for that transaction and must perform due diligence on the third parties involved in that transaction.[26] So, according to the ACH network rules, the bank that sent out the payment (the originating bank) has liability for any fraud that may occur in that ACH transaction. Under the NACHA rules, the ACH network has grown while reducing fraud. NACHA reports that the volume processed by ACH operators rose from just below 15 billion transactions in 2008 to a little over 16 billion transactions in 2011—a gain of 7.5 percent; the total volume of unauthorized ACH returns[27] dropped 22 percent during that same time period.[28] ACH fraud occurs typically because of slow account reconciliation or ACH return, lack of ACH debit blocks (or filters), or misuse or nonuse of ACH positive pay by a firm.[29] As we mentioned earlier, according to the Association for Financial Professionals (2013, p. 5), fraud is more common for ACH debits than ACH credits.

One complicating factor with ACH fraud is that the Federal Reserve's Regulation E does not apply to business customers for ACH transactions; it only covers individual consumers for such transactions. Therefore, UCC article 4A and contract law ultimately determine fraud liability in many corporate fraud cases involving the ACH network. UCC article 4A relies on a "commercially reasonable" security procedures standard when it comes to fraud liability issues related to ACH transactions. The Federal Financial Institutions Examination Council (FFIEC)[30] has issued guidance to banks on how to determine what is commercially reasonable, and case law often determines fraud liability based on contracts between banks and customers related to these types of transactions.

For ACH debit fraud, the financial institution that promises that the payment is authorized (that is, the originating depository financial institution with respect to the debit entry) assumes liability for the payment, under ACH rules. The monetary loss is usually shifted contractually from the financial institution to the merchant or biller that actually was responsible for obtaining the payment authorization from the payer.

ACH credit fraud—while less common than ACH debit fraud—remains a concern. ACH credit fraud became an issue in 2009, with the advent of corporate account takeover. UCC article 4A covers fraudulent ACH credit transactions, and contractual agreements and case law determine liability for this type of ACH fraud. While banks have relied on private agreements (assuming they would suffice), divergent court rulings regarding liability for losses due to ACH credit fraud have caused banks to reconsider their strategies to prevent this form of fraud and mitigate losses from it.

Thus far, banks have been found liable for losses due to corporate account takeover more often than their corporate customers. For example, in 2009, a construction company called PATCO Construction Inc. lost more than $270,000 through corporate account takeover, and in 2011 a Maine district court ruled that PATCO was liable for the loss. However, that decision was reversed by the U.S. Court of Appeals for the First Circuit in 2012, putting the onus on Ocean Bank, where PATCO held its account. By contrast, in 2013, a federal court in Missouri ruled against Choice Escrow and Land Title, stating that it was liable for $440,000 lost through corporate account takeover. The ruling stated that the company's bank, BancorpSouth Bank, had asked the firm on two occasions to initiate "dual control," a security mechanism requiring two authorized employees to sign off on certain transactions, but the company refused. This ruling implies that corporations can be held liable for payment fraud resulting from corporate account takeover if appropriate measures to avoid fraud are not taken. That is, when the corporate customer is found to have rejected commercially reasonable security measures, it may incur ultimate liability (Lemos, 2013).

That said, according to industry sources we interviewed directly, banks might still choose to settle in cases involving corporate account takeover, even if they did not have any explicit liability because fraud litigation is so expensive and reputational risk is so high for banks. Large banks have more resources than their small counterparts to develop extensive internal controls and hire law firms to develop private contracts with corporate customers so that fraud litigation might be avoided. Moreover, small financial institutions often don't have enough staff in their risk-management areas, and these functions are, therefore, outsourced (though the liability, of course, remains with the banks).

Lastly, consumer ACH transactions are governed by the Federal Reserve's Regulation E and NACHA's operating rules. According to Regulation E, the consumer is not liable for an unauthorized ACH (debit) transaction unless the consumer fails to dispute it within 60 days of the financial institution's transmittal of the statement showing the bogus transaction. Under the NACHA rules, if a consumer disputes an ACH transaction within 60 days of the settlement date, the receiving depository financial institution must recredit the consumer and may return the transaction to the ODFI.[31] Even though Regulation E and NACHA rules start the clock at different times (the statement transmittal date versus the settlement date), both indicate that the consumer will not be liable for an unauthorized transaction if that consumer disputes the transaction within a reasonable time frame, according to the experts we interviewed for this article.

Payment card fraud liability

Payment cards come in three forms: credit cards; debit cards—which are tied to a demand deposit account; and prepaid cards—which are anonymous or linked to a specific named individual and which are available for general use (for example, those branded with a card network logo, such as Visa's) or tied to a closed system (for example, retailer-specific gift cards). Payment cards are susceptible to a variety of fraud attacks. The *2013 AFP Payments Fraud and Control Survey* finds that 29 percent of surveyed firms experienced attempted or actual fraud on corporate or commercial cards in 2012 (Association for Financial Professionals, 2013, p. 5). However, surveys that focus specifically on financial institutions have found higher instances of payment card fraud than those that focus on corporate customers. For instance, in the Minneapolis Fed's *2012 Payments Fraud Survey*, 79 percent of its financial institution respondents that faced attempted payment fraud in 2011 reported signature-based debit cards among the top three payment types with the highest number of fraud attempts (the highest share for any payment type). Also, 36 percent of these financial institution respondents reported debit cards authorized with a personal identification number (PIN) among the top three payment types (less than half of the share reporting signature-based debit cards), and 18 percent reported credit cards among them (Federal Reserve Bank of Minneapolis, Payments Information and Outreach Office, 2012, p. 9).

Payment card fraud occurs when a card is lost or stolen and then used to make unauthorized purchases; criminals can also commit payment card fraud by accessing card and personal credentials to make such purchases without stealing the physical card itself. One well-known type of payment card fraud is the data breach, or theft of personal and account information that can be used to make fraudulent transactions (Cheney et al., 2012). Some of the techniques, such as hacking and deploying malware, that are used to carry out data breaches are described in further detail in box 1 (pp. 110–111).[32] We discuss several specific data breaches that affected payment cards in appendix 2.

Payment card transactions vary by type of card (credit, debit, or prepaid card), but they can also vary by form factor (for example, plastic card versus mobile device). Another key distinction among payment card transactions is whether the card is present or not at the transaction. Debit and prepaid cards often include the option of using either a signature or a PIN for authentication, and credit cards in the United States (which mostly use magnetic stripe technology at present) will soon carry authentication options beyond the signature as a result of the impending implementation of chip-based cards.[33]

Despite these differences among payment card transactions, fraud liability remains relatively constant across card-based transactions from a legal perspective. Fraud liability most often lies with the card issuer. While an issuer might technically be liable, a merchant might still end up paying a significant share of the loss from payment card fraud because of the liability the merchant carries under the private contract with the issuer. (Merchants agree to such contracts, though they often argue that they have no control over the authentication process at the point of sale.) That said, card issuers face incremental unplanned losses due to fraud events, even if the private contracts state that the merchants will ultimately assume liability.

Moreover, there might be multiple merchants involved in any given payment card fraud event; for example, if a data breach occurs at a merchant location but card information is used to make fraudulent purchases at another merchant, there are no chargeback rights for the merchant where the card was actually used. Our interviewees suggest that often, card issuers choose to absorb the fraud losses and quickly make the consumer whole because it is quite time-consuming and expensive to shift liability. Much of that shifting happens on a case-by-case basis through negotiations; some card issuers, such as small banks and credit unions, have few resources with which to deal with these extensive negotiations.

According to Douglass (2009), both public laws and private card network rules protect cardholders from liability for fraud losses associated with credit and debit card transactions. Both the laws and rules reallocate liability for such losses to other parties involved in the transactions. The Truth in Lending Act (TILA), which is implemented by the Federal Reserve's Regulation Z,[34] and the Electronic Fund Transfer Act (EFTA), which is implemented by the Federal Reserve's Regulation E,[35] protect consumers from bearing the brunt of fraud losses in connection with credit cards and debit cards, respectively. Under TILA and Regulation Z, the credit card holder's fraud liability is capped at $50 for all unauthorized transactions. The credit card holder has no liability after the card issuer has been alerted to the loss or theft of the credit card. The EFTA and Regulation E place a floating cap on a debit card holder's fraud liability based on when the card issuer is notified of the loss or theft of the debit card. Both Regulation Z and Regulation E offer meaningful liability protection, even when consumers fail to report cards lost or stolen.[36]

Fraud liability for prepaid cards varies depending on the specific features of the cards. Most reloadable prepaid cards linked to specific named individuals offer some Regulation E consumer protection, although not all of them do; and the law does not require that they do except for payroll cards. The status quo might change: In 2012, the CFPB issued an advance notice of proposed rulemaking on the subject of extending Regulation E coverage to general-purpose reloadable prepaid cards.[37] Prepaid gift cards are not subject to the consumer liability rights and protections afforded by Regulation E, and issuers of prepaid gift cards generally do not afford fraud liability protection to prepaid gift card holders. However, these cards are not reloadable, are usually anonymous, and do not function as bank account substitutes in most cases. According to payment industry experts we interviewed, in the case of network-branded reloadable prepaid cards, such as Visa-branded ones, fraud loss is still borne by the bank that issues the cards as a matter of contract (that is, the card network rules require that the card issuer protect holders of reloadable prepaid cards linked to specific named individuals from liability for unauthorized transactions, and the contracts further detail the specifics of who will make the customers whole after fraud occurs). According to our interviewees, many prepaid card issuers rely on third-party processors and program managers to handle the operational aspects of their card-issuing programs. Such card issuers often use liability-shifting language and associated indemnity clauses in contracts with these third parties to protect themselves from fraud losses.

Liability for payment card fraud losses is generally determined for merchants and financial institutions through payment card network rules. These rules technically bind only the card networks' member institutions—that is, card-issuing banks and card-acquiring banks, or acquirers (which convert payment card receipts into bank deposits for merchants). Acquirers generally pass on their liability to their merchants in accordance with private contract agreements. Rules may vary for chargebacks; but in general, for card-present transactions, issuers bear liability for unauthorized transactions, while for card-not-present (CNP) transactions, acquirers (ultimately, merchants) bear liability for unauthorized transactions (Levitin, 2010).

Douglass (2009) argues that such disproportionate liability for card issuers and merchants may generate risks that might otherwise be easily reduced or avoided: Given the minimal liability consumers face for payment card fraud, they may not exercise the same degree of care in protecting against payment card fraud that they would if they were held liable for lost funds (for example, as they are with their own cash). However, increasing consumer liability for payment card fraud may undermine confidence in the card networks and result in reduced transaction volumes, making it an unlikely option for improving efficiency in the overall payment system. That said, increasing merchants' liability for card-present transactions and card issuers' liability for card-not-present transactions may be viable solutions to reduce payment card fraud.

Levitin (2010) argues that raising the card issuers' liability for CNP transactions would reduce fraud at the least cost; however, Levitin does not argue for changes to loss allocation for fraudulent card-present transactions, since his analysis finds that the private card-present rules seem sensible for the most part. Levitin notes that card issuers have been historically reluctant to assume fraud risk for CNP transactions, which were first allowed at the request of merchants in the 1970s; merchants concluded that the gains from CNP transactions outweighed the fraud risk they faced, so they agreed to assume liability for fraudulent mail and telephone orders. Levitin contends that the current CNP liability rules do not account for the dramatically changed circumstances—namely, the widespread occurrence of CNP Internet transactions. Merchants require whatever information the card networks or issuers require, but merchants still have little ability to verify this information or prevent online CNP fraud on their own. However, card issuers' ability to prevent CNP fraud has improved because their ability to verify card transaction information has changed so markedly. For the verification process, card issuers can require the cardholder to transmit additional information that is more difficult for fraudsters to come by with only the physical card (such as the cardholder's zip code or telephone number). Moreover, issuers can now use statistical fraud prevention tools, referred to as neural networks, which can identify anomalies in particular consumers' spending behavior, based on transaction histories, geography, merchant type, and other factors. The neural networks' speed enables issuers to halt suspicious transactions at the stage of authorization. Given these advances are already in place for issuers, Levitin concludes that issuers can prevent more fraud at the least cost in CNP transactions and therefore should bear more of the liability for fraud committed in such transactions; increasing issuers' liability for CNP fraud may lead to even greater security measures being put in place. Additionally, he states that because e-commerce is so well established, the card issuers would not abandon the payments market even if they were required to bear more of the costs for unauthorized CNP transactions.

As things stand today, merchants face tough choices related to collecting additional authentication information for CNP transactions. As we stated before, merchants ultimately bear fraud risk for most CNP transactions at present. Hence, merchants must make calculated decisions in balancing the inconvenience of asking their customers for additional information with the added protection that may result from sending that information to issuers for verification.

Existing laws fairly clearly assign primary liability for payment card fraud affecting consumers: In the majority of cases, the card issuer generally must absorb this liability from its consumer cardholders. However, as payment card transactions have become more complex (with multiple parties now commonly involved in these transactions), liability has more often been determined through private contracts. This state of affairs means that liability allocation is determined on a case-by-case basis. That said, the majority of industry experts interviewed for this article contended that contracts generally allocate payment card fraud liability more equitably than the law, which tends to be focused on negating consumer liability.

The role of the public sector

Undoubtedly, some level of fraud is inevitable in the retail payment system. In an environment where payment methods are constantly evolving, some level of fraud is a cost of bringing innovations to market and of doing business in general. While striving to achieve efficiency, payment system operators and users must balance the costs of preventing and mitigating fraud against the costs of fraud, including, but not limited to, the actual monetary loss.[38] Ideally, this balancing will take into account the risk individual participants in the payment system may create as well as their own capability to reduce that risk. If payment system participants are able to easily reallocate their losses to other parties (via private contract, for example), these participants might have a disincentive to implement the most effective fraud-reducing strategies. Further, to lessen the overall impact of fraud events on consumers and businesses, penalties for engaging in risky behavior must be adequate. Enforcement of the penalties must be robust enough to create an environment where all actors will behave in ways that lead to the lowest level of acceptable fraud risk.

While fighting fraud on several fronts, the public sector has played a vital role in establishing the rights and responsibilities of payment system participants as they pertain to fraud. Next, we provide recommendations for how the public sector can continue to do this in the rapidly changing payments environment of the twenty-first century. The recommendations that follow are far from being comprehensive. They contain examples of how the public sector might use its unique position and influence to help improve our understanding of the payment fraud problem (including the liability issues) and bring about product and regulatory innovations that address it; the ultimate goal of such public sector contributions would be to help better align the incentives for all payment system participants to reduce fraud.

Research and education

Today, most data on payment fraud are collected and analyzed by private firms with specific research outcomes in mind. Therefore, it is difficult to obtain objective and accurate publicly available data on payment fraud. Surveys done by organizations such as the Association for Financial Professionals have focused on subcategories of payment system participants (merchants and small financial institutions, for example) and have sometimes had small sample sizes because of resource constraints. More-objective research measuring payment fraud across a wider range of participants or, ideally, the entire U.S. payment system is needed, and this research needs to be disclosed to the public. In the UK, for example, the national government regularly collects payment fraud data and calculates cost estimates for fraud, eventually disclosing this information to the public; some argue that this information from the British government provides incentives to UK payment system participants to communicate with each other and prevent future fraud. If all participants in the U.S. payment system had information that explained the nature and scope of the payment fraud problem (that is, its size, cost, and other features), this information could help align their incentives to reduce fraud. Moreover, Moore (2010, p. 108) notes that when regulators lack information about the possible harm, (ex ante) safety regulation to address a problem such as payment fraud does not work that well.[39] The kind of research that we are recommending here would provide the information necessary to make regulation more effective.

Given this recommended goal, what types of specific data should be collected? Data on fraud incidence for different payment methods (that is, for all types of payment cards, checks, ACH debits and credits, and wire transfers) at both the bank and end-user levels are not readily available to the public; thus, reliable estimates of fraud costs to all payment system participants for these channels are scarce. The Board of Governors of the Federal Reserve System, a combination of Federal Reserve Banks, or another public entity could collect such data for objective research. The aim would be to understand the volume (incidents and dollar amounts) of fraud for different channels and to get a better sense of total fraud costs (including prevention and investment costs, not just losses). Gaining such insights on specific channels would help better align all parties' incentives to behave optimally to reduce fraud in those channels—and across the payment system as a whole (as participants shift over to channels deemed safer or as each channel's security is improved). As Moore (2010) implies, if we do not know the true cost of fraud, it is difficult to suggest changes to the current liability structures. Some progress has been made in this direction—for instance, the forthcoming *2013 Federal Reserve Payments Study* will include questions about payment fraud, which should yield valuable information.[40]

Another obstacle in combating payment fraud is the lack of education on liability issues for consumers and corporate customers. This complication is especially important for the check market, where consumers might be liable for losses due to fraud. Promotion of account alert services to consumers could help stem fraud in the retail payment market. In the corporate space, federal regulators of banks could contribute to customer education by promoting programs such as positive pay and negative pay. Banks use positive pay programs to match the checks that companies issue with those presented for payment.[41] Negative pay (also called reverse positive pay) requires the check issuer to monitor its account and notify the bank when it declines to pay a check.

One problem that arises out of the variety of rules and contracts that govern payment fraud liability is that depository institutions might not understand the extent of their liability in a number of scenarios. Bank examiners could routinely ask bank representatives if they understand liability assignation as a part of the examination process. This is especially beneficial in the check space because liability rules were written for paper instruments, although almost all checks are now processed electronically. Bank representatives sometimes express confusion over fraud liability because of this change to the product. For example, liability for fraud committed through an imaged check transaction is not presently covered by existing check law, so confusion about liability may arise if such fraud occurs; in other words, check law is silent on liability in this scenario, so a private contract outlining liability would be needed to bring more clarity to the situation.

In a 2011 supplement to 2005 guidance on authentication in a web-based banking environment,[42] the FFIEC outlines the responsibility of banks to educate small business customers about Regulation E liability rules. This guidance includes "an explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access" (Federal Financial Institutions Examination Council, 2011, p. 7). Judging from recent incidents of corporate account takeover and other similar fraud events, we note that small business customers are still sometimes unaware that they are not protected from payment fraud losses under Regulation E—which covers retail customers, not corporate customers. Bank examiners need to ensure that banks are providing appropriate customer education, per FFIEC guidelines. As we indicated earlier, assigning liability for losses due to fraud can be quite challenging in cases involving corporate account takeover; case law does not clearly indicate where liability lies, as the courts have ruled in favor of banks in some cases and corporate customers in others.

Product and service development

Check fraud involving paper checks persists; however, an alternative payment method that includes the attributes of the check (such as ubiquity, remittance information, and compatibility with corporate accounting systems) is presently absent. Thus, the public sector could become more active in developing and promoting an electronic payment order (EPO) product—that is, an entirely digital check.[43] The introduction and widespread use of an EPO would enhance check processing in several ways. Currently, check processing is almost exclusively electronic, but the front-end process remains rooted in paper of some sort. Because there is no paper check to image, exception handling could be greatly reduced with EPOs. Additional security features, including digital records, electronic signatures, and biometric authentication, could be used with EPOs, significantly enhancing security protocols over what is being used in today's paper check world. At the same time, current check controls, such as positive pay, could continue. Because the paper portion of the check would be eliminated, there would be extensive cost savings by switching to an EPO platform.

Besides assisting in the development of an EPO, the public sector could also help develop a unified, nonproprietary directory of consumer and business account information—which would facilitate the move to different types of electronic payments. For example, establishing this directory would make it possible to create a ubiquitous immediate funds transfer (IFT) system in the United States. IFT is a convenient, certain, secure, and low-cost means of electronically transferring money between bank accounts with no or minimal delay in the receivers' receipt and use of funds.[44] Its widespread availability in the United States could provide benefits to many payment system participants beyond the speed by which the transactions would be settled. Because paper payment instruments are generally more costly and more susceptible to fraud than their electronic counterparts, an IFT alternative could lead to significant reductions in payment-processing-related costs and fraud overall. Additionally, many businesses, especially small firms, continue to rely on paper checks to make and receive payments because of the detailed account information collected via checks. Establishing a central directory would remove the need for small firms to rely on paper checks to get such information and store it for future use (thereby reducing the number of repositories of sensitive information). A central directory of account information could also facilitate the ubiquitous routing of ACH credits (which have no return risk, unlike ACH debits). Reducing check reliance and enhancing ACH credit routing would lead to more-efficient electronic business-to-business payments. Moreover, a central directory would reduce the potential for individual error in providing, receiving, or storing sensitive information. Such a directory would enable any individual to make a payment to another person or entity without needing to know or store the other party's account information, which would potentially make the transaction faster and safer than it would be otherwise. The public sector could make a large positive impact by helping the payments industry to develop a unified, nonproprietary directory for multiple payment channels, but it would also need to help secure it adequately as it could become a target for fraudsters.

Facilitating rules, regulations, and standards development

As payment innovations, such as online and mobile banking, have emerged and become popular, the public sector has facilitated the development of rules, regulations, and standards for payment system participants to combat fraud in these new channels. We explain recent examples of the public sector's involvement in bringing about regulatory innovations that match payment innovations. Then, we make recommendations for the public sector to get involved further to help establish new and improved rules, regulations, and standards for twenty-first-century payments.

The FFIEC's 2005 guidance and 2011 supplement, which we touched on before, are key public sector contributions to improving payment security standards. In 2005, the FFIEC issued guidance for financial institutions. Overall, the guidance recommends that financial institutions conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing online financial services. The guidance specifically recommends the use of authentication methods that depend on more than one factor—that is, two or more of what a user knows, has, or is (as explained in note 2 of box 1, p. 111)—to determine the user's identity; the FFIEC deemed single-factor authentication (for example, the lone requirement of a password) to be "inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties" (Federal Financial Institutions Examination Council, 2005, pp. 1–2). On June 22, 2011, the FFIEC published additional guidance recommending the use of "complex device identification" instead of "simple device identification." As described by the FFIEC, complex device identification employs methods that do not easily permit the fraudster to impersonate the legitimate customer. In the 2011 supplement, the FFIEC explains this identification method uses "one-time cookies" (small information-gathering files, loaded onto the user's personal computer by the bank, that expire if removed from that particular computer) to create a customer's electronic "fingerprint." This digital fingerprint is based on a number of characteristics—such as personal computer configuration, Internet protocol address, and geolocation. In contrast, the type of cookie used for simple device identification could be moved to a fraudster's computer, permitting the criminal to impersonate a legitimate account holder. So, the FFIEC recommended this change (Federal Financial Institutions Examination Council, 2011, p. 6).

Along the lines of what the FFIEC has done, other public sector entities could help shape payment security standards to help reduce fraud. For instance, there are current systems in place to validate that a person is real and an account is real, but no effective, ubiquitous solutions that tie the two types of authentication together. Just as the public sector might serve as a catalyst for creating an account directory system that would facilitate the creation of an IFT system, it could play a role in promoting products or rules that could marry the two types of authentication. At present, ASC X9 Inc. is the main industry body pushing for more-robust authentication standards. While bank regulators and other public sector entities themselves should promote universal standards that will provide continuity across the payments landscape, they can also encourage such private sector efforts that share similar objectives.

Further, to reduce confusion over liability issues, public sector bodies should update regulations governing payments to reflect the current state of the market. For example, the Board of Governors of the Federal Reserve System (2011b) proposed amendments to Regulation CC that would "apply Regulation CC's collection and return provisions, including warranties, to electronic check images that meet certain requirements." Currently, some electronic check transactions are not clearly covered under the law, as explained in our overview of check fraud liability; this leads to confusion over liability issues in certain cases.[45]

Finally, as the regulatory environment continues to evolve, public sector agencies are likely to pay even greater attention to consumer protection, competition, and criminal issues related to payment fraud. Increased cooperation with legal authorities that specialize in contract law may be beneficial in facilitating the development of rules, regulations, and standards that clarify fraud liability. As payment fraud becomes more international in nature, the U.S. public sector will need to engage in cross-border cooperation with regulatory and policing bodies not only to enforce existing laws and rules but also to improve upon them.

Conclusion

The U.S. retail payment system has a decentralized governance structure. Further, the United States currently lacks a uniform set of consumer disclosures, error resolution techniques, and liability allocation structures for retail payments. Indeed, we document that fraud liability for retail payments in the United States is determined through a piecemeal set of laws, regulations, and private contracts, largely formed in the past for various reasons but operating in the present often under vastly different circumstances. The lack of both a cohesive governance structure and uniform set of rules for all payment types is even reflected within specific industry players; indeed, firms often strategize about security and fraud liability issues with respect to business silos or product lines instead of their entire businesses. Furthermore, research and policy discussions are rarely about the payments industry as a cohesive entity, but instead tend to focus on certain industry segments.

Although many consumers or business customers seek to make their payments in the most convenient and efficient manner, they might not be aware of the vast differences of their rights and responsibilities among the various payment methods. The complexity of these various rights and responsibilities may be further compounded by the fact that certain payment types are converging (for example, hybrid payment cards access both prepaid funds and a line of credit). So, in today's market, the separation of laws and regulations by payment type might not make as much sense as it did in the past.

This state of affairs has led to confusion and inefficiencies in the marketplace. Some legacy payment methods, such as checks, continue to operate under laws that have not been fully updated to reflect the digital reality of those payment methods today. Other methods, such as payment cards, are subject not only to new regulations that might alter security incentives but also to new delivery channels (such as card-not-present transactions via mobile devices) that alter liability structures for fraud. Moreover, as criminals begin to use methods such as account takeover to steal funds from firms and individuals, participants using payment channels such as the ACH system have experienced uncertainty because case law has thus far determined liability in contradictory ways. Some payment methods protect consumers from liability almost entirely, affecting their sense of having "skin in the game" in regard to fraud prevention. Even in cases where liability is very clearly defined, losses might be reallocated through private contracts, leading to disincentives for firms to implement the most effective fraud-reduction strategies. Together, these observations highlight the need for a more cohesive approach to preventing and mitigating payment fraud; channel-specific or case-specific approaches are not sufficient.

Even without the legal and regulatory harmonization that would bring clarity to issues surrounding payment fraud liability, a variety of steps can be taken to reduce confusion over such issues and help align all payment system participants' incentives to reduce fraud. Currently, individual firms and payment associations have been managing these complex issues surrounding payment fraud through a variety of means, including self-governance, private agreements, standards creation, and the development of best practices. In conjunction with those efforts, the public sector—which develops, implements, and enforces the laws and regulations concerning payment fraud liability—can play a more prominent role in managing payment fraud than it has in the recent past. Effective public sector efforts can include measuring fraud across the entire U.S. retail payment system; educating banks, businesses, and consumers about payment fraud; working with the industry to develop products and services, such as an EPO and a directory of consumer and business account information; and facilitating the development of rules, regulations, and standards that are more in step with the rapidly changing payments marketplace.

NOTES

[1] By retail payments, we generally mean small-value payments (such as those made in the goods and services market)—as opposed to large-value payments (such as those made via systemically important payment systems, including transactions in the interbank money market).

[2] For instance, in the United States, a card-based payment transaction involves some or all of the following parties: a cardholder; a merchant or biller; a card issuer, or simply an issuer; a card-acquiring bank, or an acquirer (which converts payment card receipts into bank deposits for merchants); an electronic switch (which routes transaction information among banks participating in a payment network); a payment network; one or more processors; a telecommunications company; and other third parties.

[3] The interview subjects, who represent a wide range of industry players, are anonymous. The interviews were conducted during the first and second quarters of 2013.

[4] At the Federal Reserve Bank of Chicago's Payments Conference held in October 2012, Cleveland Fed President Sandra Pianalto articulated the Federal Reserve System's new multiyear direction with regard to payment policy; Pianalto (2012) stressed the need to ensure "the speed, efficiency, certainty, security, fraud resistance, and market responsiveness of the U.S. payments system." Following this announcement, the Federal Reserve moved forward with its new payment policy agenda. In September 2013, the Federal Reserve issued a public consultation paper requesting comments on making improvements to the payment system; areas of focus include standards development, the exploration of a real-time payments system, the conversion of paper payments to electronic payments, and payments security; see Federal Reserve Banks (2013).

[5] The CFPB has supervisory authority (for the purposes of ensuring compliance with many federal consumer protection statutes) over nonbanks of all sizes in the residential mortgage, private education lending, and payday lending markets. Additionally, the CFPB may, by rule, define a set of nonbanks that it determines are "larger participants" in markets for consumer financial products and services and establish supervisory authority over these firms. For further details, see Consumer Financial Protection Bureau (2012).

[6] For additional details, see Keitel (2008).

[7] For example, in the private sector, five payment card networks—American Express, Discover Financial Services, JCB (Japan Credit Bureau) International, MasterCard Worldwide, and Visa Inc.—initially established individual data security standards for payment system participants. About seven years ago, these networks joined forces to create a unified set of standards—the Payment Card Industry Data Security Standard (PCI DSS or, more simply, PCI)—to better secure payment card systems, and they founded the PCI Security Standards Council. See also appendix 1.

[8] NACHA was previously known as the National Automated Clearing House Association.

[9] In economic terms, fraud, like pollution, creates externalities. If fraud is largely absent, one can operate more freely with less caution. However, when fraud is rampant, one must operate much more vigilantly (a relatively more expensive course of action).

[10] The actual allocation of losses will depend on the circumstances of the transaction and payment card network rules.

[11] The Bank Secrecy Act is formally known as the Currency and Foreign Transactions Reporting Act of 1970. For more details about this law concerning the detection and prevention of money laundering, see www.fincen.gov/statutes_regs/bsa/.

[12] For more details on OFAC, see www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

[13] See American Bankers Association (2011) and www.stopcheckfraud.com/statistics.html.

[14] For more details on the Check Clearing for the 21st Century Act (Check 21), which was enacted in 2003, see www.federalreserve.gov/paymentsystems/regcc-faq-check21.htm.

[15] The text of the UCC is available at www.law.cornell.edu/ucc.

[16] The concept of comparative fault—as discussed in sections 3-406(b) and 4-406(e) of UCC articles 3 and 4, respectively—can shift liability to the check issuer, or drawer. If both the bank and account holder have failed to exercise ordinary care, they both can be liable for losses based on their respective determined fault for the fraud event. Banks do not have to physically verify each check.

[17] Regulation CC (12 CFR 229), along with its recent amendments and compliance guide, is available at www.federalreserve.gov/bankinforeg/reglisting.htm#CC.

[18] For more information on the substitute check, see www.federalreserve.gov/pubs/check21/consumer_guide.htm#whatis.

[19] Regulation E (12 CFR 205), along with its recent amendments and compliance guide, is available at www.federalreserve.gov/bankinforeg/reglisting.htm#E. The NACHA operating rules are available by free membership at www.achrulesonline.org.

[20] See, for example, 2010 and 2011 correspondence from The Clearing House deputy general counsel to the Board of Governors of the Federal Reserve System, available at www.theclearinghouse.org/index.html?f=072995.

[21] According to ECCHO rules (as of November 2012), specifically, section XIX(P)(3), "as between two or more Members that are parties to a Claim, it shall be presumed for all purposes related to the Claim that the Related Physical Check or Electronic Image was altered with respect to the dollar amount or payee, unless the Member against which the Claim is brought proves by a preponderance of the evidence that the Related Physical Check or Electronic Image is not altered, such as evidence that the Related Physical Check is a counterfeit/fraudulent item or that the Related Physical Check is as issued by the drawer." This and other ECCHO rules are available via free membership at https://www.eccho.org/cc/index.php?p_sector=cc_rules&p_matter=cc_login_rules.

[22] See §229.2 of Regulation CC, available at www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=635f26c4af3e2fe4327fd25ef4cb5638&tpl=/ecfrbrowse/Title12/12cfr229_main_02.tpl.

[23] Authors' calculations based on data from Association for Financial Professionals (2013, p. 9).

[24] For more information on corporate account takeover, see Castell (2013). Also, NACHA has developed a Corporate Account Takeover Resource Center, whose details are available at https://www.nacha.org/CorporateAccountTakeoverResourceCenter.

[25] Javelin Strategy & Research (2013, p. 32). This report provides estimates on the impacts of account takeover; 36 percent of account takeovers impacted credit card accounts, and 33 percent impacted checking and savings accounts (Javelin Strategy & Research, 2013, p. 35).

[26] See the NACHA operating rules, available by free membership at www.achrulesonline.org.

[27] ACH returns are ACH debits returned to the originating depository financial institution (either unpaid or for a refund) by the receiving depository financial institution for any reason, including insufficient funds, an incorrect bank account number, and lack of authorization per the payer. The last reason may be due to fraudulent activity.

[28] NACHA—The Electronic Payments Association (2012, p. 1).

[29] ACH debit blocks refer to the practice of disallowing regular ACH debits without specific advance permission from the payer. ACH positive pay is a fraud detection service; it lets customers safeguard against fraudulent activity by filtering or blocking unauthorized ACH transactions according to criteria set by the customers.

[30] For more information on this interagency body, see www.ffiec.gov/about.htm.

[31] See the section on the liability of the consumer for unauthorized transfers (§205.6) in Regulation E, available at www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=635f26c4af3e2fe4327fd25ef4cb5638&tpl=/ecfrbrowse/Title12/12cfr205_main_02.tpl. And see the NACHA operating rules, available by free membership at www.achrulesonline.org.

[32] Hacking and deploying malware are among the most common techniques used for data breaches (Verizon RISK Team, 2013, pp. 6, 25–26).

[33] The EMV (Europay, MasterCard, and Visa) standard—which enables the interoperation of chip-based payment cards—will soon be in use in the United States; for more information on the EMV standard, see www.emvco.com. However, the advent of EMV, which many argue provides more-secure payments than the magnetic stripe system, will not mean that magnetic stripe payment cards will immediately disappear from the marketplace. Analysts expect both types of cards to coexist for some time. Moreover, there are very promising technologies by which security can be significantly enhanced for magnetic stripe cards, but they have not been able to achieve sufficient market penetration to reach critical mass thus far.

[34] Regulation Z (12 CFR 226), along with its recent amendments and compliance guide, is available at www.federalreserve.gov/bankinforeg/reglisting.htm#Z.

[35] See the section on the liability of the consumer for unauthorized transfers (§205.6) in Regulation E, available at www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=635f26c4af3e2fe4327fd25ef4cb5638&tpl=/ecfrbrowse/Title12/12cfr205_main_02.tpl.

[36] Card networks often reinforce consumer protections by requiring card issuers to offer zero liability protection to their consumer holders of credit cards and debit cards (as well as general-purpose reloadable prepaid cards linked to specific named individuals). However, consumers must operate within certain guidelines, prescribed by the payment card networks, to avail themselves of zero liability protection (for example, they must exercise reasonable care in protecting against unauthorized transactions and must report unauthorized transactions in a timely manner).

If a credit card is lost or stolen and used fraudulently, the maximum consumer liability for fraudulent charges is $50. In most cases, even the $50 is absorbed by the card issuer because of prevailing zero liability policies. If the consumer reports the loss or theft of his credit card before it's used, he is not held liable for any loss. Also, if the credit card itself is not stolen but account information is illegally obtained, the consumer is generally protected from liability. The consumer is slightly more liable for debit card fraud under the law, although the rules vary based on the situation (and, as with credit cards, payment card networks' zero liability policies require the card issuer to absorb this liability in many circumstances). If the consumer loses his debit card or it has been stolen, he must report the loss within two business days in order for the loss limit to remain $50 under Regulation E; otherwise, he might be liable for up to $500. Finally, if notification of the lost or stolen debit card is not given by the consumer to the issuer within 60 days after receiving a statement showing unauthorized withdrawals, the consumer could be liable for all losses occurring after that 60-day period.

[37] For details, see http://files.consumerfinance.gov/f/201205_cfpb_GPRcards_ANPR.pdf.

[38] The costs of fraud include nonmonetary costs to consumers—for example, the opportunity cost of time spent to verify payment card transactions and replace compromised cards or to monitor and confirm the validity of credit accounts opened in the victim's name after identity theft has occurred.

[39] Moore (2010, pp. 107–108) discusses the conundrum of ex ante safety regulation versus ex post liability regulation. He notes that the Gramm–Leach–Bliley Act obliges banks to protect the security and confidentiality of customer information. An alternative to this proactive ex ante regulation would be to assign ex post liability for fraud to the responsible party. Some legal experts have examined the trade-offs between the ex ante regulatory regime and ex post liability regime and find that the best results are achieved when both are used simultaneously. But ex ante regulation is not very effective without reliable, accurate research explaining the true nature and scope of the problem (for example, payment fraud).

[40] Specifically, this upcoming 2013 study—which will be the fifth in a series of triennial studies conducted by the Federal Reserve System to explore the payments landscape of the United States—asks for information on the number and value of unauthorized check payments, ACH credits and debits, debit and prepaid card transactions, credit card transactions, and ATM cash withdrawals. For further details on the planned study, see www.frbservices.org/fedfocus/archive_perspective/perspective_0313_01.html.

[41] For details, see www.positivepay.net.

[42] See Federal Financial Institutions Examination Council (2005, 2011).

[43] For details on this EPO product, see Jacob et al. (2009).

[44] For more on IFT, see Jacob and Wells (2011).

[45] The proposed changes to Regulation CC are in Board of Governors of the Federal Reserve System (2011a).

APPENDIX 1: KEY PAYMENTS INDUSTRY ORGANIZATIONS

In this appendix, we describe some of the key payments industry organizations that help establish standards for retail payments in the United States.

Accredited Standards Committee X9 Incorporated

The Accredited Standards Committee X9 Incorporated (ASC X9 Inc.) establishes, maintains, develops, and promotes standards for the financial services industry. It is an organization accredited by the American National Standards Institute (ANSI). Some of ASC X9's projects involve developing e-commerce standards, such as better online security. Membership is open to all U.S. companies and organizations in the financial services industry.

ASC X9 Inc. is composed of its board of directors and four subcommittees of experts in the financial services industry. The four subcommittees are X9AB (payments), X9C (corporate banking), X9D (securities), and X9F (data and information security). Within the subcommittees, working groups are organized on an as-needed basis. Any member with category A membership (ASC X9's top membership level) is on ASC X9's board of directors and has the ability to participate on all subcommittees and working groups. Such members are also allowed all voting privileges on international standards (via an ANSI-accredited U.S. Technical Advisory Group) and ASC X9 policy. For further information, go to www.x9.org.

ECCHO

ECCHO (Electronic Check Clearing House Organization) is a not-for-profit national clearinghouse that is owned by its more than 3,000 member financial institutions. Membership is open to all financial institutions, and there are membership classes to serve institutions of all sizes. Created to use electronics to enhance the check payment system, ECCHO is the national provider of private sector image-exchange rules. There is no law governing the exchange of check images (only the legal recognition of substitute checks and their legal equivalency to original checks are provided by Check 21 legislation); hence, ECCHO's clearinghouse rules provide a common, multilateral agreement among its members in order to address this deficiency in check law.

Changes to ECCHO rules are approved by its board of directors. The changes are based on recommendations from its operations committee, which includes members and representatives from community banks, credit unions, large banks, processors, settlement providers, and sponsoring organizations. For further information, go to www.eccho.org.

NACHA

NACHA (formerly the National Automated Clearing House Association) is a not-for-profit organization that manages the development, administration, and governance of the ACH network. Primary functions include rulemaking for the ACH network, facilitating the development of new payment applications, identifying and implementing risk-management initiatives, and responding to regulatory and government relations issues. NACHA represents over 10,000 financial institutions via regional payments associations and direct membership.

The NACHA operating rules provide the legal foundation for the exchange of ACH payments. Proposals to create and develop rules are presented by NACHA members or key parties (for example, the U.S. Department of the Treasury). The proposals are reviewed by the Rules & Operations Committee. If the proposals are accepted, the committee assigns a Standing Rules Group to them for further development. NACHA's voting members are the ultimate decision-makers for changes to the operating rules. For further information, go to https://www.nacha.org.

PCI Security Standards Council

The PCI (Payment Card Industry) Security Standards Council was formed in 2006 by five global card networks—American Express, Discover Financial Services, JCB (Japan Credit Bureau) International, MasterCard Worldwide, and Visa Inc. The five founding global payment brands have agreed to incorporate the Payment Card Industry Data Security Standard (PCI DSS or, more simply, PCI) as the technical requirements for their respective data security compliance programs.

All five card networks, as well as strategic members, share equally in the council's governance, have equal input into the council, and share responsibility for carrying out the council's work. Other industry stakeholders are encouraged to join the council (as strategic or affiliate members and participating organizations) and review proposed additions or modifications to the standards.

The PCI Security Standards Council's board of advisors is composed of representatives of participating organizations. This cross-industry board is chartered to ensure that all voices are heard in the ongoing development of the security standards; this board has global representation from across the payment chain (including merchants, financial institutions, and processors).

Participating organizations are eligible to nominate candidates for the board of advisors and then vote for them.

Enforcement of compliance with the PCI DSS and determination of any noncompliance penalties are carried out by the individual card networks and not by the council. For further information, go to https://www.pcisecuritystandards.org/index.php.

APPENDIX 2: EXAMPLES OF DATA BREACHES AFFECTING PAYMENT CARDS

In 2012, there were 621 confirmed data breaches, resulting in 44 million compromised records (Verizon RISK Team, 2013, p. 11). The majority of the data breach attacks were made by agents outside of the firms compromised (92 percent); they took advantage of firms' security vulnerabilities to access their systems and information assets (Verizon RISK Team, 2013, p. 19). According to the U.S. Software Protection Initiative (SPI), a security vulnerability is defined as the combination of a system flaw (or susceptibility), an attacker's access to the flaw, and an attacker's capability to exploit the flaw.[1] In 2012, two of the most common methods that attackers used to exploit such flaws and steal vast amounts of personal and account information were hacking and deploying malware, which were involved in 52 percent and 40 percent of data breaches, respectively (Verizon RISK Team, 2013, pp. 6, 25–26; see also our box 1, pp. 110–111, for more details on hacking and malware).

A prominent example of a hacker attack was the one on Global Payments—a payment card processor. Global Payments publicly acknowledged in March 2012 that it had suffered a data breach. Subsequent investigations estimated the breach of payment card data may have started as early as June 2011. Global Payments confirmed that information from at least 1.5 million accounts had been stolen. However, others suggested that information from at least 7 million card accounts had been compromised. Stolen consumer information included account numbers and other data that could be used to make counterfeit cards, but did not include Social Security numbers, addresses, and cardholders' names. However, small merchants' personal and payment information may have also been stolen. This incident led both the Visa and MasterCard networks to remove Global Payments from their lists of approved transaction processors (Wolfe, 2012; Schwartz, 2012; Sidel, 2012; and Johnson, 2012).

In June 2011, Citigroup reported that a cyberattack on Citi Account Online, its consumer website, had enabled hackers to view the names, account numbers, transaction histories, and contact information (for example, email addresses) of over 200,000 cardholders. Using legitimate accounts, hackers logged on to the site reserved for cardholders. They then jumped between accounts by inserting new account numbers that were differentiated by only a few digits into a URL in the web browser's address bar. While Social Security numbers, birth dates, card expiration dates, and security codes were not compromised, the stolen contact information could be used to elicit more information through targeted attacks—for example, through phishing (Schwartz and Dash, 2011; and Wagenseil, 2011).

Payments industry firms are not necessarily the only victims of hacking incidents; a variety of other types of firms are being hacked, leading to the theft of personal and account information that may later result in fraudulent transactions. In June 2012, hackers breached LinkedIn, the popular professional networking website, and stole more than 6 million users' passwords, which were exported to a Russian hacking forum. Since individuals may use the same password for multiple online accounts, the harvested passwords could be used by hackers to gain access to users' email, bank, or corporate accounts containing even more valuable information. It is not yet known how the hackers accessed the passwords, but to decrypt them, the hackers employed dictionary attacks (Perlroth, 2012b). In a similar case, Yahoo! confirmed in July 2012 that a file containing over 400,000 user names and passwords to accounts for Yahoo!, Google, AOL, Comcast, and other companies was stolen. Criminals claiming responsibility for the attack stated that they stole the passwords using a Structured Query Language (SQL) database injection, which exploits how webpages communicate with back-end databases (after such an injection, attackers can issue commands to a database to harvest data). After posting all of the stolen information online, the hackers claimed that their actions should serve as a wake-up call, not as a threat, to those in charge of security at Yahoo! and other similar companies (Perlroth, 2012a). Another very well-known hacking incident occurred when the computer system of TJX Companies Inc., the parent company of T.J. Maxx and Marshalls, was breached; at least 46 million payment card numbers were stolen (Jewell, 2007). Other recent incidents of data hacking include those at the shoe and clothing retailer Zappos (24 million customer accounts accessed), Sony's video gaming and entertainment network for its PlayStation console (77 million user accounts and possibly credit card numbers accessed), and a website devoted to Google's operating system for mobile devices called Android Forums (1 million user credentials accessed) (Greenberg, 2011, 2012; and Protalinski, 2012).

One well-known example where malware was used to commit a cybercrime is the 2008 data breach of Heartland Payment Systems—an electronic transaction processor for small and midsized businesses. In 2009, the processor disclosed details of the breach: 130 million credit card and debit card accounts had been compromised via malware planted on the company's payment processing network. Stolen data included names, card numbers and expiration dates, and magnetic stripe data, which could be used to make counterfeit cards (Krebs, 2009b; and Vijayan, 2010).[2]

In closing, we want to highlight two disturbing aspects of some of these recent data breaches. For one, breaches can occur so surreptitiously that the host under attack may not be aware that it has been compromised until well after the initial breach. The Verizon RISK Team (2013, p. 52) finds that in 2012, two-thirds of the confirmed data breaches went undetected for months or even years. For another, about three-quarters of these breaches required criminals to have only low levels of sophistication (for example, the use of brute force or phishing) in order to be successful (Verizon RISK Team, 2013, p. 49). These findings imply that while data breaches might be fairly simple to initiate, they remain difficult to detect.

[1] See www.spi.dod.mil/tenets.htm.

[2] For more details on this breach and the company's response to it, see Cheney (2010).

REFERENCES

American Bankers Association, 2011, *2011 Deposit Account Fraud Survey Report*, Washington, DC, December, available for purchase at https://www.aba.com/Products/Surveys/Pages/2011DepositAccount.aspx.

Association for Financial Professionals, 2013, "*2013 AFP Payments Fraud and Control Survey*: Report of survey results," underwritten by J.P. Morgan, Bethesda, MD, March.

__________, 2012, "*2012 AFP Payments Fraud and Control Survey*: Report of survey results," underwritten by J.P. Morgan, Bethesda, MD, March.

Board of Governors of the Federal Reserve System, 2011a, "Availability of funds and collection of checks; proposed rule," *Federal Register*, Vol. 76, No. 58, March 25, pp. 16862–16976.

__________, 2011b, press release, Washington, DC, March 3, available at www.federalreserve.gov/newsevents/press/bcreg/20110303a.htm.

__________, 2005, "Collection of checks and other items by Federal Reserve Banks and funds transfers through Fedwire and availability of funds and collection of checks," *Federal Register*, Vol. 70, No. 227, November 28, pp. 71218–71226, available at www.gpo.gov/fdsys/pkg/FR-2005-11-28/pdf/FR-2005-11-28.pdf**.**

Castell, M., 2013, "Mitigating online account takeovers: The case for education," Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, survey paper, April, available at www.frbatlanta.org/documents/rprf/rprf_pubs/130408_survey_paper.pdf.

Cheney, J. S., 2010, "Heartland Payment Systems: Lessons learned from a data breach," Federal Reserve Bank of Philadelphia, Payment Cards Center, discussion paper, No. DP10-01, January.

Cheney, J. S., R. M. Hunt, K. R. Jacob, R. D. Porter, and B. J. Summers, 2012, "The efficiency and integrity of payment card systems: Industry views on the risks posed by data breaches," *Economic Perspectives*, Federal Reserve Bank of Chicago, Vol. 36, Fourth Quarter, pp. 130–146, available at www.chicagofed.org/digital_assets/publications/economic_perspectives/2012/4Q2012_part2_cheney_etal.pdf.

Consumer Financial Protection Bureau, 2012, "Defining larger participants in certain consumer financial product and service markets," *Federal Register*, Vol. 77, No. 33, February 17, pp. 9592–9608.

Douglass, D. B., 2009, "An examination of the fraud liability shift in consumer card-based payment systems," *Economic Perspectives*, Federal Reserve Bank of Chicago, Vol. 33, First Quarter, pp. 43–49, available at www.chicagofed.org/digital_assets/publications/economic_perspectives/2009/ep_1qtr2009_part7_douglass.pdf.

Federal Financial Institutions Examination Council, 2011, "Supplement to 'Authentication in an Internet banking environment,'" supplement to guidance, Arlington, VA, June 28, available at www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20%28FFIEC%20Formated%29.pdf.

__________, 2005, "Authentication in an Internet banking environment," guidance, Arlington, VA, October 12, available at www.ffiec.gov/pdf/authentication_guidance.pdf.

Federal Reserve Bank of Minneapolis, Payments Information and Outreach Office, 2012, "*2012 Payments Fraud Survey*: Summary of results," report, September 17, available at www.minneapolisfed.org/about/whatwedo/payments/2012_Payments_Fraud_Survey_Summary.pdf.

Federal Reserve Banks, 2013, "Payment system improvement—public consultation paper," Federal Reserve Financial Services, September 10, available at http://fedpaymentsimprovement.org/wp-content/uploads/2013/09/Payment_System_Improvement-Public_Consultation_Paper.pdf.

Federal Reserve System, 2011, "The *2010 Federal Reserve Payments Study*: Noncash payment trends in the United States: 2006–2009," report, Washington, DC, April 5, available at www.frbservices.org/files/communications/pdf/press/2010_payments_study.pdf.

Federal Trade Commission, 2013, "Telemarketing sales rule; proposed rule," *Federal Register*, Vol. 78, No. 131, July 9, pp. 41199–41225, available at www.gpo.gov/fdsys/pkg/FR-2013-07-09/html/2013-12886.htm.

Greenberg, A., 2012, "Zappos says hackers accessed 24 million customers' account details," *Forbes*, January 15, available at www.forbes.com/sites/andygreenberg/2012/01/15/zappos-says-hackers-accessed-24-million-customers-account-details/.

__________, 2011, "Sony hacker may have accessed 77 million users' data, possibly including credit cards," *Forbes*, April 26, available at www.forbes.com/sites/andygreenberg/2011/04/26/sony-hacker-may-have-accessed-77-million-users-data-possibly-including-credit-cards/.

Jacob, K., A. Lunn, R. D. Porter, W. Rousse, B. Summers, and D. Walker, 2009, "Digital checks as electronic payment orders," Federal Reserve Bank of Chicago, Financial Markets Group, policy discussion paper, No. PDP 2009-5, November 17.

Jacob, K., and K. E. Wells, 2011, "Evaluating the potential of immediate funds transfer for general-purpose payments in the United States," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 292a, November.

Javelin Strategy & Research, 2013, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, report, Pleasanton, CA, February, available for purchase at https://www.javelinstrategy.com/brochure/276.

Jewell, M., 2007, "Data theft believed to be biggest hack," *Washington Post*, via Associated Press, March 29, available at www.washingtonpost.com/wp-dyn/content/article/2007/03/29/AR2007032902629.html.

Johnson, A. R., 2012, "MasterCard removes Global Payments from approved vendor list," *4-traders*, via Dow Jones Newswires, May 2, available at www.4-traders.com/MASTERCARD-INC-17163/news/MasterCard-Removes-Global-Payments-From-Approved-Vendor-List-14308060/.

Keitel, P., 2008, "Legislative responses to data breaches and information security failures," Federal Reserve Bank of Philadelphia, Payment Cards Center, discussion paper, No. DP08-09, December, available at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2008/D2008DecemberLegislativeResponsesToDataBreaches.pdf.

Krebs, B., 2009a, "Data breach led to multi-million dollar ATM heists," *Security Fix*, blog, *Washington Post*, February 5, available at http://voices.washingtonpost.com/securityfix/2009/02/data_breach_led_to_multi-milli.html.

__________, 2009b, "Payment processor breach may be largest ever," *Security Fix*, blog, *Washington Post*, January 20, available at http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html.

Lemos, R., 2013, "Lawsuits bring clarity to SMBs in corporate account takeovers," *Dark Reading*, April 22, available at www.darkreading.com/smb/lawsuits-bring-clarity-to-smbs-in-corpor/240153406.

Levitin, A. J., 2010, "Private disordering? Payment card fraud liability rules," *Brooklyn Journal of Corporate, Financial & Commercial Law*, Vol. 5, No. 1, Fall, pp. 1–48.

Marcus, D., and R. Sherstobitoff, 2012, "Dissecting Operation High Roller," McAfee and Guardian Analytics, white paper, June 26, available at www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.

Moore, T., 2010, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection*, Vol. 3, Nos. 3–4, December, pp. 103–117.

NACHA—The Electronic Payments Association, 2012, "Risk management strategy: Executive summary," report, Herndon, VA, October, available at https://www.nacha.org/sites/default/files/files/Risk_and_Compliance/Risk_Management_Tools_and_Resources/NACHA%20Risk%20Management%20Summary%20Exec%20Summary%20Oct%202012.pdf.

Nair, D., and J. Dye, 2013, "Exclusive—Indian card processor in $45 million heist is ElectraCard: Sources," Reuters, May 11, available at http://in.reuters.com/article/2013/05/11/usa-crime-cybercrime-india-idINDEE94A04620130511.

Perlroth, N., 2012a, "Yahoo breach extends beyond Yahoo to Gmail, Hotmail, AOL users," *Bits*, blog, *New York Times*, July 12, available at http://bits.blogs.nytimes.com/2012/07/12/yahoo-breach-extends-beyond-yahoo-to-gmail-hotmail-aol-users/?hp.

__________, 2012b, “Lax security at LinkedIn is laid bare,” *New York Times*, June 10, available at www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html.

Pianalto, S., 2012, “Collaborating to improve the U.S. payments system,” presentation at the 12th Annual Payments Symposium, Federal Reserve Bank of Chicago, October 22, available at www.clevelandfed.org/for_the_public/news_and_media/speeches/2012/pianalto_20121022.cfm.

Protalinski, E., 2012, “Android Forums hacked: 1 million user credentials stolen,” *ZDNet*, July 12, available at www.zdnet.com/android-forums-hacked-1-million-user-credentials-stolen-7000000817/.

Schwartz, M. J., 2012, “Global Payments breach: Fresh questions on timing,” *InformationWeek*, May 4, available at www.informationweek.com/security/attacks/global-payments-breach-fresh-questions-o/232901419.

Schwartz, N. D., and E. Dash, 2011, “Thieves found Citigroup site an easy entry,” *New York Times*, June 13, available at www.nytimes.com/2011/06/14/technology/14security.html.

Sidel, R., 2012, “Card-data breach may be wider than first reported,” *Wall Street Journal*, May 3, available by subscription at http://online.wsj.com/article/SB10001424052702303877604577382522160414052.html.

Strohm, C., and E. Engleman, 2012, “Cyber attacks on U.S. banks expose computer vulnerability,” *Bloomberg*, September 27, available at www.bloomberg.com/news/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html.

Verizon RISK Team, 2013, *2013 Data Breach Investigations Report*, New York, available at www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

Vijayan, J., 2010, “Heartland breach expenses pegged at $140M—so far,” *Computerworld*, May 10, available at www.computerworld.com/s/article/9176507/Heartland_breach_expenses_pegged_at_140M_so_far.

Wagenseil, P., 2011, “Citigroup data theft so easy anyone could have done it,” *TechNewsDaily*, June 14, available at www.technewsdaily.com/6911-citigroup-data-theft-so-easy-anyone-could-have-done-it.html.

Wolfe, D., 2012, “Global Payments reports merchant data also affected in breach,” *American Banker*, June 12, available by subscription at www.americanbanker.com/issues/177_113/global-payments-data-breach-merchant-applications-1050090-1.html.

Zetter, K., 2012, “How ‘Flame’ malware hijacks a computer,” interview by I. Flatow, *Talk of the Nation*, National Public Radio, June 8, available at www.npr.org/2012/06/08/154587988/how-flame-malware-hijacks-a-computer.