The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches

Julia S. Cheney[1]*
Robert M. Hunt[1]*
Katy R. Jacob[2]*
Richard D. Porter[2]*
Bruce J. Summers*

[1] Federal Reserve Bank of Philadelphia
[2] Federal Reserve Bank of Chicago

October 2012

* The authors wish to thank those who participated in the interviews described in the paper. Thanks also to Anna Lunn and James van Opstal for their assistance and Darin Contini, Fumiko Hayashi, Joanna Stavins, and Rick Sullivan for many helpful conversations. The views expressed here are those of the authors and not necessarily those of the Federal Reserve Banks of Chicago and Philadelphia or the Federal Reserve System. Corresponding authors: Bob Hunt, Payment Cards Center, Federal Reserve Bank of Philadelphia, 10 Independence Mall, Philadelphia, PA 19106; phone: (215) 574-3806, e-mail: bob.hunt@phil.frb.org, and Katy Jacob, Economic Research Department, Federal Reserve Bank of Chicago, 230 South LaSalle St., Chicago, IL 60604; phone: (312) 322-2915, e-mail: kjacob@frbchi.org. This paper is available free of charge at www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/.

The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches

Julia S. Cheney[1]*
Robert M. Hunt[1]*
Katy R. Jacob[2]*
Richard D. Porter[2]*
Bruce J. Summers*

[1] Federal Reserve Bank of Philadelphia
[2] Federal Reserve Bank of Chicago

ABSTRACT

Consumer confidence in payment card systems has been built up over many decades. Cardholders expect to use their cards to execute payment instructions in a reliable and timely manner. Data breaches that degrade the perceived safety and reliability of payment cards may weaken consumer confidence in those systems and potentially cause cardholders to shift to other, and perhaps less efficient, forms of payment. A sizable shift away from payment cards — induced by the consequences of one or more data breaches is unlikely. Even so, the probability of such an outcome is uncertain. In other words, this could be an example of "tail risk" for payment card systems. The authors informally interviewed a number of market participants and several experts to better understand the risks presented by data breaches, the efforts to protect payment card systems against data breaches, and areas where more might be done to secure these systems. In particular, the authors investigated whether existing levels of investment, coordination, information sharing, and management of incentives in securing payment card systems by firms and organizations in the private and public sectors are adequate to confront the threats arising from modern data breaches. The lessons learned from these conversations are described in this paper. These insights may also be helpful in considering the risks that data breaches may broadly pose to retail payments in the United States.

JEL Codes: D14, E42

Keywords: Payment card fraud, data breaches, credit cards, debit cards

I. Introduction and Summary

In this paper, we consider the potential for data breaches that compromise the security of personal and account information to threaten consumer confidence in payment card systems in the United States. In particular, we explore whether a large, well-targeted data breach (or a sequence of breaches over a relatively short period of time) might render inoperable a payment card system (for credit, debit, or prepaid cards), possibly resulting in its being abandoned, temporarily or otherwise, by a substantial number of consumers.[1] We recognize that, given the precautions that are in place in such systems, the probability of a catastrophic abandonment is quite low. But this probability is not zero. Recent events, as well as feedback from the industry, suggest that further study of such potential tail risks could be helpful.[2]

The shutdown or abandonment of one or more of these systems, even if the duration is relatively limited, might amount to a significant disruption in the flow of funds among consumers and businesses and, increasingly, from governments to households in the form of benefits payments.[3] Such transactions might be immediately shifted to alternative means of payment, but doing so could create substantial operational challenges for those payment systems. Sudden shifts away from payment card transactions to other payment methods might also invoke a policy

[1] Credit, debit, and prepaid card transactions account for about 60 percent of the number and 5 percent of the value of noncash transactions in the United States. They account for a much higher share of the value of transactions at the point of sale (POS). Today, with the exception of the remaining checks used to pay recurring bills, debit card purchases and automated teller machine (ATM) withdrawals are the principal means consumers use to access funds in their transaction accounts. See the 2010 Federal Reserve Payments Study: "Noncash Payment Trends in the United States: 2006 – 2009," p. 13 at www.frbservices.org/files/communications/pdf/press/2010_payments_study.pdf and The Clearing House, "Project Compas Executive Summary for NACHA," April 4, 2011.

[2] For the purposes of this paper, we define tail risk to mean that there is uncertainty over the precise probability of the occurrence of a highly unlikely but catastrophic event. We consider the abandonment of payment card systems or instruments as an example of tail risk associated with data breaches.

[3] Governments at all levels are replacing the remaining benefit disbursements that occur via paper check with some form of prepaid card, whose functionality depends on the existing payment card infrastructure. See Susan Herbst-Murphy, "Government Use of the Payment Card System: Issuance, Acceptance, and Regulation," Federal Reserve Bank of Philadelphia Payment Cards Center Conference Summary, July 2012 at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2012/D-2012-Government-Use-of-the-Prepaid-Card-System.pdf.

response to an immediate crisis based on incomplete information — which would be less desirable than a response based on a process of carefully gathering and evaluating all the available information.

In the event of a crisis, the Federal Reserve maintains a legal and electronic infrastructure to provide liquidity to banks facing interbank settlement difficulties as a result of disruptions to the normal clearing and settlement cycles of card systems; however, this liquidity would have to quickly reach consumers and businesses, including nonfinancial firms, that rely on these systems as a means to exchange value and whose payment behavior would be affected by even a temporary disruption in one of the card networks. To allow for efficient payment substitution in support of a smoothly functioning U.S. economy, there must also be multiple reliable ways to make and receive electronic payments.

For all of these reasons, researchers at the Federal Reserve Bank of Chicago and the Payment Cards Center at the Federal Reserve Bank of Philadelphia developed a series of questions and organized informal conversations with a variety of payment system participants, with the goal of better understanding the nature and significance of risks posed by data breaches to payment card systems. More specifically, to examine the adequacy of existing efforts to prevent, manage, and mitigate fraud in card-based payment systems, the Chicago Fed and the Philadelphia Fed researchers conducted 17 industry interviews in 2009. The individuals interviewed represented a variety of perspectives, including those of networks, banks, merchants, processors, independent sales organizations (ISOs), vendors, and information-sharing organizations. This paper documents the insights gained through this exercise, but it does not identify individual organizations or respondents. Ideally, the information learned from these interviews would be helpful to other researchers considering the risks that data breaches may broadly pose to retail payments in the United States, as well as how those risks can be mitigated in the most optimal manner.

In the next section, we provide an overview of the threat that fraud poses to the smooth operation of payment card systems in the United States. Then, we discuss specific measurements of losses due to payment card fraud, as well as the current scale and character of data breaches in the financial industry. After providing this background information, we summarize our industry interviews and discuss the lessons learned from them.

II. Accounting for Payment Fraud

Payment fraud can be broadly defined as any activity that uses confidential personal (and often financial) information for unlawful gain. For example, A masquerades as B and uses B's credentials to illicitly take B's funds or to obtain credit under B's name. Such fraud can occur with any type of noncash payment method, including credit and debit cards, checks, and automated clearinghouse (ACH) transactions. Payment fraud can be committed knowingly by a consumer (first-party fraud), or consumers can be victimized by others operating within financial institutions or as part of criminal enterprises (third-party fraud).[4]

Fraud is a threat to the payments system's efficiency because it degrades operational performance and increases costs — not only for the parties whose payments are compromised but also for all participants in the system.[5] Payment networks are potentially vulnerable to fraud at a number of points along the transaction chain. As a result, banks and other payment system operators and private firms using the payment system incur significant expenses to protect against fraud. In turn, criminals naturally opt to exploit the weakest links in payment chains.

[4] For a general discussion of payment fraud, see the special edition of the Federal Reserve Bank of Chicago's *Economic Perspectives* published in the first quarter of 2009: www.chicagofed.org/webpages/publications/economic_perspectives/2009/1qtr2009_part1_amromin_porter.cfm.

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

When successful, payment card payment fraud, which we focus on in this paper, can give rise to adverse consequences for participants at different points along the payment chain. For example, when a criminal steals a payment card and uses it (or its information) to make a purchase, the legitimate cardholder's liability for the fraudulent transaction is limited by statute or regulation. It is downstream participants such as the card-issuing bank and the merchant that are likely to incur losses on fraudulent transactions.[6]

Although the cost of fraud losses might be limited by investing in stronger protections against criminal use of a stolen card, it is neither possible nor efficient to eliminate payment fraud entirely. Rather, in striving to achieve efficiency, payment system operators and users must balance the costs of preventing and mitigating fraud against the full set of costs that fraud generates, including, but not limited to, the actual monetary loss to society.[7] Ideally, individual participants would actively monitor the risks that their choices create.

An important input into this calculation is the confidence that private actors have in the payment methods they use. For example, consumers have come to expect that payment card systems will reliably and securely complete payments as instructed. Today, these systems are widely used to receive income and benefit payments, to purchase goods and services, and to pay bills. Over time, payment card systems have displaced more costly paper-based systems, especially for purchases made at the point of sale (POS). Card systems have also been essential in facilitating payments in new sales channels, such as the Internet, where the buyer and seller do not transact in a face-to-face environment.

Without sufficient confidence among the parties involved, payment card systems cannot operate efficiently for all of them, nor will these systems be profitable to their owners. Card

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

[7] The full set of costs includes nonmonetary costs incurred by consumers, such as the opportunity cost of time spent to verify transactions and replace compromised payment cards and, in the case of identity theft, to monitor and confirm the validity of credit accounts opened in the victim's name.

networks operate more efficiently in an environment where their services are offered ubiquitously and large numbers of consumers and merchants agree to use them. The presence of strong network effects in established card payment systems contributes to their resilience in the face of temporary shocks.[8] At the same time, these network effects imply that a sufficiently large shock to public confidence in a payment card system might result in a sufficiently large shift of transactions to other (potentially less efficient) forms of payment that cannot easily be reversed. This shift would reduce the value of the payment card network because a reduction in the number of active cardholders may, in turn, lead to fewer merchants or businesses willing to incur the cost to accept payment card transactions.

Consumer payment systems usually function so smoothly that it is easy to underestimate their complexity. This complexity is due, in part, to the number of parties involved in completing a payment, the high degree of coordination required among these parties, and the ongoing investments that are required to ensure reliable performance. For example, a card-based payment transaction in the United States will involve 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 various banks participating in a payment network); a payment network; one or more processors; a telecommunications company; and other third parties.[9] Coordinating the activities of all these participants is a crucial payment system function,

[8] By network effects, we mean in this context that a payment method will be more attractive to consumers when there are more places that accept that particular method of payment. Moreover, merchants and other businesses will be more willing to incur the costs of accepting payment cards when they know that many of their customers are ready and willing to use them.

[9] For more details on the acquiring function, see Ann Kjos, "The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges," Federal Reserve Bank of Philadelphia Payment Cards Center discussion paper, October 2007 at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2007/D2007OctoberMerchantAcquiring.pdf.

and such coordination takes on special significance in protecting the system from fraud and preserving the public's confidence in the system.[10]

Moreover, with relatively few exceptions, no single government entity has an exclusive or comprehensive regulatory or supervisory jurisdiction over U.S. retail payment systems or payment providers. The Board of Governors of the Federal Reserve System issues certain retail payment regulations, especially regarding checks. The recently established Consumer Financial Protection Bureau (CFPB) has jurisdiction over most federal consumer protection regulation for electronic payment transactions. As a prudential regulator, the Federal Reserve Board, as well as other federal financial supervisors, conducts exams, and these exams can entail a review of the financial institution's payment system security precautions, including those of its business partners.

Further, some of the organizations involved in operating networks and providing payment services to the public are banks, but many are not. Thus, additional regulators can be involved. For example, nonbanks operating under state money-transmitter licenses are subject to state agency supervision. In addition, the CFPB may determine, by rule, that certain nonbanks in markets for consumer financial products and services are larger participants and therefore subject to CFPB supervision.[11] A variety of state laws also address consumer rights in instances of identity theft or a data breach.[12]

---

[10] For card-based systems, the coordination function is performed by the networks, that is, American Express, Discover Financial Services, JCB (Japan Credit Bureau) International, MasterCard Worldwide, and Visa Inc.

[11] The CFPB has supervisory (for example, examination) 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. 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 example, the CFPB adopted a rule on July 16, 2012, to begin supervising consumer reporting agencies (for example, credit bureaus or credit reporting companies) that have more than $7 million in annual receipts. To view the CFPB press release announcing its rule, see www.consumerfinance.gov/pressreleases/consumer-financial-protection-bureau-to-superivse-credit-reporting/.

[12] For additional details see Philip Keitel, "Legislative Responses to Data Breaches and Information Security Failures," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper, 2008 at

Local, state, and federal law enforcement agencies investigate instances of fraud, identity theft, and data breaches. Consumer payments, whether made domestically or abroad, are potentially exposed to fraudulent activities orchestrated from anywhere in the world and, therefore, may fall under the investigative jurisdiction of foreign authorities. Therefore, regulation, supervision, enforcement, and investigation of retail payments and fraud in payment systems may be the responsibility of a variety of agencies at the international, federal, and state or local level.

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 six years ago, they 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. For more information about the PCI Security Standards Council and PCI DSS, see box below.

PCI Security Standards Council

The PCI Security Standards Council is composed of representatives from its five founding global payment card networks — American Express, Discover Financial Services, JCB (Japan Credit Bureau) International, MasterCard Worldwide, and Visa Inc. These companies have agreed to incorporate the PCI Data Security Standard in their respective data security compliance programs.

All five payment card networks share equally in the council's governance, have equal input into the PCI Security Standards Council, and share responsibility for carrying out the work of the organization. Other industry stakeholders are encouraged to join the council as participating organizations and review proposed additions or modifications to the standards.

The PCI Security Standards Council Board of Advisors (currently 20 members) is composed of representatives of participating organizations. This cross-industry group is chartered to ensure that all voices are heard in the ongoing development of PCI security standards; this group has representation from across the payment chain — from merchants, financial institutions, processors, and others — as well as from around the world.

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

Enforcement of compliance with the PCI DSS and determination of any noncompliance penalties are carried out by the individual payment card networks and not by the council.

Sources: For more information, see the PCI Security Standards Council website at www.pcisecuritystandards.org./.

Several of these networks have also recently announced plans to support migration to an EMV payment infrastructure in the United States as a means to further increase the security of payment card transactions.[13] While these plans are specific to the individual network, the announcements suggest that the networks informally tried to develop plans with similar key dates and milestones to encourage merchants and issuers to adopt EMV payments. Nevertheless, there is an ongoing discussion about whether the existing levels of investment, coordination, information sharing, and management of incentives in securing payment card systems by firms and organizations in the private and public sectors are adequate to confront the threats arising from modern data breaches.[14] We explore the costs and consequences of data breaches in greater detail in the next section.

III. Measuring Payment Fraud and Data Breaches

A rough estimate of aggregate fraud losses related to U.S. payment cards was about $3.56 billion in 2010.[15] In recent years, fraud losses borne by credit card *issuers* have fluctuated in the range of 5 to 10 cents per $100 of transaction value. As a cost of doing business, these losses are not comparatively large, since they equate to roughly one-tenth of the charge-off rate associated with

[13] See Visa Inc.'s press release, "Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments," August 9, 2011; MasterCard Worldwide's press release, "MasterCard Introduces U.S. Roadmap to Enable Next Generation of Electronic Payments," January 30, 2012; and Discover's press release, "Discover Implements 2013 EMV Mandate in U.S., Canada and Mexico," March 15, 2012. EMV stands for Europay, MasterCard, and Visa; it is a global standard for the interoperation of chip-based payment cards with POS devices and ATM. For more information on the EMV standard, see www.emvco.com.

[14] For a discussion related to this topic, see Julia S. Cheney, "Heartland Payment Systems: Lessons Learned from a Data Breach," Federal Reserve Bank of Philadelphia Payment Cards Center discussion paper, January 2010 at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf.

[15] See www.nilsonreport.com/pdf/news/112111.pdf. Also see Richard Sullivan, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Federal Reserve Bank of Kansas City *Economic Review*, 2010, at www.kansascityfed.org/Publicat/Econrev/pdf/10q2Sullivan.pdf. Sullivan's estimate of fraud losses is based on the sum of direct losses borne by card issuers; POS merchants; and merchants in Internet, mail order, and telephone transactions.

credit losses on these cards. For debit and prepaid cards, in 2009, the industry-wide fraud loss to all parties to a transaction was about 9 cents per $100 of transaction value, with issuers and merchants incurring about 5cents and 4 cents of that total, respectively.[16] In addition, an issuer will incur many other indirect costs related to efforts to detect and prevent incidences of fraud on its cards and to mitigate fraud losses. Indirect fraud costs are also borne by merchants and, in some instances, by consumers.

A primary focus of this paper is on the consequences of data breaches, both in terms of the direct fraud losses incurred by card-issuing banks, merchants, and consumers and in terms of public confidence in payment card systems. According to Verizon's *2012 Data Breach Investigations Report*, across all industries and categories in 2010, there were approximately 855 data breaches in the U.S. In total, those breaches may have compromised as many as 5 million card accounts.[17]

Ordinarily, only a small percentage of compromised payment card records ever result in fraudulent transactions.[18] But there are other indirect costs associated with a data breach, which can be substantial. For example, according to one 2009 survey by the Ponemon Institute, the average cost to firms responding to a data breach is about $200 per record compromised.[19] Our

[16] The credit card fraud losses are from the *Nilson Report*, various issues. In 2010, the Federal Reserve Board surveyed issuers subject to Regulation II (Debit Card Interchange Fees and Routing). The data on debit and prepaid card fraud loss are for the 2009 calendar year and represent total fraud losses, as reported by the issuers, for PIN (personal identification number) debit, signature debit, and prepaid card transactions. The Board of Governors of the Federal Reserve System also published data for PIN debit, signature debit, and prepaid debit fraud losses separately. See *Federal Register*, Vol. 76 (2011), p. 43480 and the Federal Reserve Board, "2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions," June 2011.

[17] This estimate is based on Verizon's estimate that these breaches involved 174 million potentially compromised records, but that only about 3 percent of those involved payment card data. See www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

[18] See Julia S. Cheney, "An Update on Trends in the Debit Card Market," Federal Reserve Bank of Philadelphia discussion paper, June 2007, pp. 8-9.

[19] This statistic is from the Ponemon Institute's "2009 Annual Study: Cost of a Data Breach." About two-thirds of this cost results from attrition of existing customers and less success in obtaining new ones. See www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf.

very imprecise estimate, based on the 2009 survey by the Ponemon Institute and the 2012 data breach report by Verizon, is that the indirect costs of payment card records compromised in 2010 might be as high as $1 billion.

Recent payment card data breaches are particularly notable for the sophistication of techniques employed by criminals. In recent years, breaches have occurred at large card processers such as RBS WorldPay, Heartland Payment Systems, and Global Payments, at merchants such as T. J. Maxx, Hannaford, and Sony, and at third-party vendors such as Epsilon and RSA.[20] In many of these cases, breaches are not detected at the time of intrusion into the system, in part because the hackers wait for an opportune time to monetize the compromised information. But when they do act, recent experience suggests that they move quickly and, at times, employ a sophisticated (and possibly international) criminal organization. For example, in 2008, the RBS WorldPay breach resulted in a number of prepaid payroll cards being compromised. These cards were used to obtain $9 million in cash in 12 hours from automated teller machines (ATMs) located in several dozen cities around the world.[21]

It is important to note that data breaches that result in payment fraud can occur at nonfinancial firms, such as at universities and hospitals. Data breaches at any firm that collects and stores personal data can provide criminals with sufficient information, such as an individual's

[20] For a detailed account of the breach at Heartland, see Julia Cheney, "Heartland Payment Systems: Lessons Learned from a Data Breach," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper, 2010 at: www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf. Less is known about the breach at Global Payments, but see Robin Sidel, "Card Processor: Hackers Stole Account Numbers," *Wall Street Journal*, April 2, 2012. For information about the Epsilon and RSA data breaches, see www.cbsnews.com/8301-31727_162-20050575-10391695.html and www.massdataprivacylaw.com/data-breach/rsa-data-breach-the-result-of-successful-spear-phishing/, respectively.

[21] See Brian Krebs, "Data Breach Led to Multi-Million Dollar ATM Heists," *Washington Post*, February 5, 2009, at voices.washingtonpost.com/securityfix/2009/02/data_breach_led_to_multi-milli.html.

name, address, and Social Security number, to commit financial fraud.[22] This information can be used to compromise security protocols at financial institutions (resulting in account takeover) or to obtain credit in the victim's name (new-account fraud). Both are examples of *identity theft*.

Identity theft is an important aspect of payment fraud with potentially severe consequences for victims, including not only monetary loss but also a time-consuming process to revalidate credit and other transactional accounts.[23] The fear of identity theft is one reason why consumers might collectively react to an unprecedented rash of data breaches by losing confidence in a particular payment method and switching to a substitute method. In 2010, the Federal Trade Commission (FTC) received more than 250,000 complaints about instances of identity theft.[24] In 10 percent of those complaints, consumers alleged that new credit card accounts had been opened in their names. In 7 percent of those complaints, consumers alleged a takeover of one or more of their existing accounts. A survey of consumers reports that as many as 11 million adults have at some point been a victim of identity theft.[25]

There is some qualitative evidence that consumers' concerns about data security can influence their choice of payment provider and methods of payment. According to a survey conducted by Gartner shortly after the 2008 RBS WorldPay data breach mentioned previously, 13 percent of respondents said that increased fears that financial data are not secure have been a

[22] The 2012 Verizon report found that the majority of records compromised in 2010 contained personal information. The majority of all data breaches (54 percent) occurred among restaurants and hotels, but relatively few records are stolen this way. Retailers and financial firms also accounted for a significant share of breaches (20 percent and 10 percent, respectively).

[23] According to Javelin Strategy & Research's *2011 Identity Fraud Survey Report*, it took victims an average of 33 hours to resolve issues related to identity fraud. See eWeek.com, "ID Theft Declined in 2010 but Average Losses Increased: Survey," February 10, 2011 at www.eweek.com/c/a/Security/ID-Theft-Declined-in-2010-but-Average-Losses-Increased-Survey-814461/. For the full Javelin report, see Javelin Strategy & Research's website at www.javelinstrategy.com/research/Brochure-209.

[24] See the Federal Trade Commission's 2011 edition of the *Consumer Sentinel Network Data Book* at ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf.

[25] See Javelin Strategy & Research, "Identity Fraud Survey Report," February 2012. For further information on identity theft, see Stacey Schreft, "Risks of Identity Theft: Can the Market Protect the Payment System?" Federal Reserve Bank of Kansas City *Economic Review*, Fourth Quarter 2007: www.kansascityfed.org/Publicat/ECONREV/PDF/4q07Schreft.pdf.

factor in their decisions about which stores and financial companies they use. In addition, concerns about security led 59 percent of respondents to change how they shop and pay online.[26]

Further, a recent paper by Kahn and Liñares-Zegarra (2012) examining nationally representative survey data found that incidents of identity theft increased the adoption of money orders, traveler's checks, online bank bill payments, and prepaid cards while also boosting the number of cash and credit card transactions. The authors also reported a decrease in the use of checks after "mixed incidents" of identity theft. Mixed incidents refer to the subset of consumers who report being a victim of identity theft as well as knowing other victims. Notably, these results reveal changes in the adoption and use of particular types of payments after an identity theft incident.[27]

Such behavior is interesting in light of the significant regulatory and contractual protections from losses resulting from fraudulent transactions afforded to consumers in the U.S.[28] These protections against monetary losses do not eliminate the less apparent costs associated with the pain and suffering consumers face (time costs, forgone financing opportunities, etc.) as a result of identity theft.[29] Accordingly, data breaches and identity theft appear to have an influence on consumer payment behavior, notwithstanding the legal protections that are in place for consumers.

---

[26] CardLine, "Data Fears Influencing Habits," *American Banker,* March 16, 2009.

[27] Charles M. Kahn, and José Manuel Liñares-Zegarra, "Identity Theft and Consumer Payment Choice: Does Security Really Matter?," February 14, 2012; available at SSRN: http://ssrn.com/abstract=2005694.

[28] These protections are defined in the Fair Credit Billing Act and the Electronic Fund Transfer Act and in "zero liability" policies created by private payment networks. For details, see Mark Furletti and Stephen Smith, "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper, 2005, at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2005/ConsumerProtectionPaper_CreditandDebitCard.pdf .

[29] See Julia S. Cheney, "Identity Theft: Do Definitions Still Matter?," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper, August 2005, at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2005/identity-theft-definitions.pdf.

To summarize, payment fraud is an ongoing concern for payment system participants, both for the card issuers and merchants that bear most of the actual fraud losses and for processors, networks, and others that have an inherent interest in maintaining confidence in the payment system in which they participate. Some fraudulent activity is the result of data breaches that occur both within and outside retail payment systems. There is some evidence that data breaches have created concerns about security in the minds of at least some consumers—concerns that, at the margin, may affect their choice of payment providers or methods.

Our experience to date suggests that data breaches have not caused consumers in any great number to lose confidence in card payments and switch to alternative means of payment. However, questions remain about the adequacy of investment, coordination, information sharing, and management of incentives in securing payment card systems against increasingly sophisticated data breaches and the broadening scope and organization of criminals who commit these crimes. In the next section, we describe the results of 17 interviews examining these questions.

IV. Interview Topics and Results

Our conversations with payment system participants were loosely organized around three topics: payment trends and fraud (especially related to data breaches), liability (for fraud losses) and incentives (to prevent fraud), and coordination and information sharing. In the next sections, we introduce each of these topics and describe the insights gained about them from our conversations with the interviewees.

a. Payment Trends and Fraud

Modern data storage systems, online information sharing, and the growing number and variety of firms using or offering access to payment card systems have increased the potential points of entry that might be exploited by sophisticated criminal organizations. The technology to secure

those access points has improved over time, so the larger question is whether, on net, payment card systems are more or less vulnerable than in the past.

For example, today, more organizations may have a business need to retain personal consumer financial data, and any of these firms may be a potential target for criminals. Financial institutions must consider the data security practices of these firms when using them for payment-related services. Another characteristic of today's payment system is the demand by consumers for around-the-clock payment servicing, in the form of supporting either transaction processing (for example, online purchases) or access to account management functions (for example, online banking). To the extent that meeting this need requires alternative access points (such as the Internet or a mobile device) or alternative service providers (such as online security firms or cellular providers), the number of potential points or places at which data can be compromised increases. Potential access points must be made more secure to manage the increased risks. And if one access point is nevertheless penetrated, the amount of data potentially at risk must be limited in order to control the potential scale of the damage.

In this complex environment, market participants and regulatory, supervisory, and oversight authorities must determine whether payment methods carry excessive fraud risk; who is liable when payment fraud occurs; how losses are allocated; what consumer protections should be in place; how notification of fraud should be handled; and how standards should be defined to manage the incidence of fraud. Additionally, payment providers must authenticate consumers whom they have never met and authorize electronic transactions from which they might be far removed. And increasingly, they must do this in real time. Carrying out all of these tasks is quite a tall order, but necessary to prevent and mitigate fraud.

1. Interview Results

Many respondents emphasized that as the number, types, and complexity of electronic payments grow, so too do the opportunities for committing fraud. Electronic payments are evolving in the locations or channels in which they might be used by consumers — for example, they can now be made at nonbank financial centers (such as check cashers or retail stores) or even vending machines. In addition, the physical forms of electronic payments are evolving — for example, some consumers can now use contactless cards (payment cards that use chip technology to allow for tap-and-go payments) and mobile devices to execute payments.[30]

Several interviewees stressed that while traditional card payments and transactional environments are important to study for fraud risks, it is also important to consider emerging payment environments. For example, one interviewee noted that ACH networks are moving from relatively safe recurring payments with trusted payees to new forms of nonrecurring payments, which likely carry higher fraud risks because distinguishing between one-time (nonrecurring) payments and fraudulent ones is more difficult. These issues warrant further study. Several other interviewees indicated that mobile payments are an emerging area that bears special attention; the focus should be on gaining a better understanding of the risks to retail payment systems and investigating whether these may be different from the risks in more traditional card-initiated payments.[31] Another interviewee pointed to the gradual adoption of contactless payment cards in the United States. This interviewee said that while the back-end processing remains the same as in contact environments, an inappropriately configured contactless front end (for example, with weak encryption) at the point of sale might increase fraud risk.

[30] Traditionally fraud has been measured, managed, and mitigated within each independent payment channel (for example, checking and ACH). In recent years, payment providers have recognized a growing interdependence in fraud management across channels, since criminals have learned to exploit vulnerabilities detected in one channel to extract information or value in others.

[31] For an in-depth discussion of mobile payments issues, see "Mobile Payments Industry Roundtable Summary, January 27-28, 2010," at www.frbatlanta.org/documents/rprf/rprf_events/mobile-payments-roundtable-summary.pdf. Also see Darin Contini, Marianne Crowe, Cynthia Merritt, Richard Oliver, and Steve Mott, "Mobile Payments in the United States: Mapping Out the Road Ahead," Retail Payments Risk Forum White Paper, March 2011, at www.frbatlanta.org/documents/rprf/rprf_pubs/110325_wp.pdf.

Interviewees also highlighted changing consumer payment preferences and noted that these changes have a material bearing on the ongoing development of fraudriskmanagement systems. For example, according to one interviewee with a large merchant, in 2003, PIN (personal identification number) debit accounted for only 10 percent of its total transactions, compared with 35 percent in 2009. Thus, static four-digit PINs designed for use at on-premise and later off-premise ATMs are now being used at a much larger number of POS terminals in very different and diverse physical environments.[32] As payment methods change and new types of payments or new types of providers emerge, security systems must adapt to these developments. Several interviewees discussed the challenge of balancing risk mitigation and support for innovation in the constantly evolving electronic payment system.

Along similar lines, interviewees held a consensus that criminals' ability to rapidly change their tools and adopt new tactics may significantly increase the threats posed to the payments system. Most interviewees noted that the management of fraud risk must be at least as dynamic as the adoption and use of new tools, techniques, and tactics by those engaged in fraudulent activity. Interviewees agreed that making one-time assessments of a company's systems and satisfying minimum security standards at one point in time were hardly sufficient. Hackers are committed to finding new ways to compromise systems and steal personal and card data, so weaknesses must be uncovered before they can be exploited.

Moreover, as certain types of organizations tighten security, criminals respond by changing their targets and points of attack. For example, one interviewee mentioned that payment processors and merchants are not the only targets for illegally obtaining payment information; payroll processors and other firms need to be aware of the problem as well. In

[32] One company provided the example of PIN pads at gasoline pumps as a new type of physical acceptance environment for PIN payment cards. This company noted that new ways had to be considered (and some developed) to effectively limit PIN payment card fraud in this environment. For example, gas stations may use zip code verification during the authorization process at the gas pump machines.

addition, fraudsters recognize that institutions are tightening the security of data at rest, which are stored in internal systems. Thus, criminals have begun targeting vulnerabilities present when data are moved (or transmitted) either between payment nodes or within a company's internal systems.

Several interviewees said that companies cannot ignore threats that may result from a shortfall in internal controls or communication. Some interviewees noted an increase in internal fraud — that is, fraud committed by company employees or contractors.[33] Access controls and tracking mechanisms are important tools in limiting this risk. Similar issues arise among independent firms along the payment chain. One interviewee said that, for example, a lot of effort has been put into front-end security, where the payment transaction is made. However, some interviewees stated that much work still needs to be done in the communication between the merchant and the processor.

b. Liability and Incentives

As consumers, merchants, and payment providers struggle with the issue of payment fraud, we recognize that entirely eliminating fraud is not realistic. Rather, the goal ought to be to encourage the adoption of risk-management practices that strike a balance between excluding unduly risky payment options and rigidly dictating payments choices. Collaboration within and among companies is a necessary aspect of successful payment fraud management, as security is expensive to achieve and maintain. In order to be effective, payment fraud prevention and mitigation efforts need to include all parties touching the payment transaction. To do this, the parties' incentives must be properly aligned.

In our interviews, we asked whether the current incentive structure for payment card systems best addresses data security risks. For example, do current network rules assign a larger share of liability for losses to those participants most able to take actions to minimize those losses

[33] This observation is consistent with a rising trend in the share of breaches that involve internal employees, over the years 2004-09 as reported in Verizon's 2012 *Data Breach Investigations* Report (Figure 10, p. 16). The share of fraud events resulting from insiders fell significantly thereafter.

for the system as a whole? And if the current rules fail to achieve this, are there incentive problems at the network level or is there another explanation?[34] If incentive problems exist, what is the nature of these problems?

1. Interview results

Merchants, banks, networks, and processors all share responsibility for protecting a payment system against data breaches, but the extent to which these responsibilities are adequately balanced was a frequent point of discussion during our interviews. A number of interviewees contended that incentives to prevent fraud are misaligned. This sentiment was particularly strong among participants on the merchant and acquiring side of payment card processing. According to a number of interviewees, merchants have a vested interest in protecting data in order to maintain their reputations and brands as well as to avoid charge-backs, which occur when firms fail to comply with network rules. However, these interviewees noted that merchants do not feel that they have ownership over the fraud mitigation system with which they must comply, and they often feel that blame for fraud is somewhat arbitrarily placed on them. One merchant interviewee stated that "the payment system is not our system."

Other interviewees stated that the current system of shared liability, wherein both issuers and acquirers have some liability for fraud losses, appears to be effective: Incentives to prevent and mitigate fraud in that system have kept direct credit card fraud losses relatively modest for almost a decade. That said, these interviewees noted that this apparent level of success in managing fraud losses may limit the incentive to develop new innovative security measures, especially if they are expensive. For example, one representative from a large bank said that his organization assessed its fraud mitigation tactics as being successful and considered the addition

[34] These incentive problems are discussed in greater detail in R. Anderson and T. Moore, "Information Security Economics – and Beyond," mimeo, Computer Laboratory, University of Cambridge. For a theoretical explanation of the potential incentive problems, see William Roberds and Stacey Schreft, "Data Breaches and Identity Theft," *Journal of Monetary Economics* 56:7 (2009), pp. 918-29.

of more sophisticated authentication procedures to be unnecessary at that time. However, fraud risks are constantly evolving, necessitating solutions that can predict or respond to new threats.

As part of the discussion about incentives to invest in data security, several interviewees noted that compared with small firms, large firms may have greater financial resources to make investments in data security. For example, our interviews suggested that large banks and big-box merchants may be better positioned financially to develop in-house security systems, to incorporate security products into their business processes, and to meet data security requirements imposed on them by private or public sector actors. Our interviews also suggested that small processors, ISOs, and small merchants are likely to be more cost sensitive than their larger counterparts when considering investments in data security. Several interviewees noted that to the extent that data security costs become prohibitively expensive for these firms, a barrier to entry to payment card systems could be created.

Payment card fraud losses among issuers, as a percentage of transaction value, have remained relatively stable over the past decade. Nevertheless, the data breaches described previously suggest that hackers have developed increasingly sophisticated techniques for identifying and exploiting vulnerabilities. And these experiences indicate that criminals may be able to scale their fraud quickly. As a result, payment system participants are paying increased attention to the risks posed by data breaches.

According to our interviews, most large banks are employing fraud mitigation and data security programs that may be proprietary or other programs provided by third-party vendors and processors (or a combination of the two). Merchants, acquirers, and processors are also employing fraud-prevention and data security systems that may already include or may soon include innovative solutions, such as end-to-end encryption and tokenization.[35]

[35] Encryption involves masking the valuable private information so that it is too expensive to decrypt it even when the information is illicitly intercepted. Currently, the most powerful form of encryption available in browsers is 128-bit encryption. Tokenization involves masking the valuable information,

Several interviewees stressed that incentives are also important for consumers in order to combat fraud. Some merchants feel that consumers lack sufficient incentives to protect their own data because of statutes or regulations that limit consumer liability for fraudulent transactions and zero liability rules and other protections offered by banks and card networks. According to this perspective, the problem is one of moral hazard. Put another way, even if consumers are best positioned to prevent fraud (by protecting their personal and account information), they may not be sufficiently motivated to do so because they bear little of the costs resulting from fraudulent transactions, except in the case of identity theft.[36] Indeed, some interviewees argued that strong consumer protections from fraud losses might explain the relatively modest consumer reactions to large data breaches observed to date. Nevertheless, an interviewee from a large bank stated that a policy of shifting liability to consumers could backfire, since consumers might move away from payment cards that do not offer zero liability.

A number of interviewees expressed a related concern about the level of security associated with online payments initiated using consumers' computers. Several interviewees indicated that consumers' computers can be the weakest link in the data security chain. Setting security standards for personal and corporate computing is one way that the public sector could get involved to make consumer electronic payments safer. For example, one option suggested was to put additional responsibilities on Internet service providers (ISPs) for ensuring greater security in personal and corporate computing.[37] One interviewee also suggested that a restricted

---

such as a credit card number, with a token. The token might be, for example, an arbitrary number or combination of numbers and letters. Without the token look-up key, the random information has no value if it is stolen.

[36] While liability incentives for consumers are limited by the various protections offered, there is some recognition that identity theft is an entirely different matter. Consumers appear to have a general, albeit basic, understanding that they are largely responsible for restoring their good credit standing in the case of identity theft and that such a restoration is often quite expensive in terms of both time and money.

[37] The Australian government developed a framework to address the problem of compromised personal computers (PCs). In 2005, the Australian Communications and Media Authority (ACMA) developed the Australian Internet Security Initiative (AISI), which works with ISPs and consumers. AISI is a free service provided by the ACMA that monitors data feeds on compromised Australian PCs. The agency sends a list

domain, such as .bank, could add protection by offering greater controls and more regulated entry into businesses facilitating payments via the Internet.

Despite comments by some interviewees that incentives to prevent and mitigate fraud are misaligned, a number of interviewees also mentioned companies that have advanced fraud protection strategies. Indeed, some companies exist for the sole purpose of providing banks and others with security solutions.

Some interviewees argued that the provision of fraud protection is a profitable business that can offer a competitive advantage. For example, banks, merchants, networks, and processors may be able to advertise better security as a differentiating factor between them and their competitors. The ability to convey such a message may also act as an incentive for other companies to innovate. This is an example of using market dynamics to improve incentives to invest in better security. But there may also be a downside to this approach. Some interviewees contended that if establishing a competitive advantage in fraud prevention proves to be important, private firms may be reluctant to rapidly share their know-how and lessons learned from their own experiences combating fraud attacks. The result would be an uneven level of defenses across the industry.

c. Coordination and information sharing

As noted earlier, an aspect of the evolution of electronic payment systems in the United States over the past few decades has been a movement toward a more open environment, with multiple parties (including nonbanks) processing or "touching" cardholder information. These parties include, at a minimum, both card-acquiring and card-issuing banks, a number of independent payment networks (card networks, ACH networks, and PIN-debit-only electronic benefit transfer

---

of customers with compromised PCs to the ISP, which is required to notify the customer. The ISP may contact the customer by phone or letter and provide advice to fix the problem, but in some cases, it may even disconnect a customer to contain the spread of a malware threat.

[EBT] networks), payment-card-accepting and other merchants, and third-party processors. These parties also include nonbank intermediaries and providers of alternative financial services.

In the United States, the resulting industrial structure has become more complex, and the participants have become highly differentiated. Both developments may make effective coordination more difficult to achieve over time.[38] By contrast, European payment markets are relatively more concentrated and, therefore, may present an easier path to coordinating data protection policies. In addition, the network participants in Europe may be less specialized than those we observe in the U.S. But it is also the case that European regulatory bodies have played a more active role than their U.S. counterparts with respect to supporting coordination on data security in payment systems.[39] But the European approach has its drawbacks, too. Adopting monolithic security solutions also poses certain risks. For example, if the security design is breached, the breach could be exploited almost immediately and at about the same scale as the payment system itself.

In the United States, there are examples of specially designed efforts in both the public[40] and the private sector[41] to share information related to identity theft and payment fraud. One

[38] Coordination may include efforts to share information among payment system participants as well as efforts to move participants toward better data protection practices.

[39] For more detail on the evolution of regulatory structures in the EU and the U.S., see Terri Bradford, Fumiko Hayashi, Christian Hung, Simonetta Rosati, Zhu Wang, and Stuart E. Weiner, "Nonbanks and Risk in Retail Payments: EU and U.S.," in Eric M. Johnson, ed., *Managing Information Risk and the Economics of Security* (Springer Publishing, forthcoming).

[40] For example, the FTC maintains the Identity Theft Clearinghouse, which provides law enforcement agencies with direct access to detailed incidence data recorded as part of the complaints and also allows the FTC to share aggregate data with consumers, other government agencies, and industry constituencies. For additional examples of identity theft information-sharing efforts, see Julia S. Cheney, "Identity Theft: Where Do We Go From Here?," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper, April 2004, at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/events/conferences/2004/IdentityTheft_042004.pdf.

[41] Early Warning Services is an example of a limited liability bank-owned company that essentially is a private sector data-sharing initiative. Its services include verifying identity and authenticating account holders' information as well as screening potential new and existing customers for a prior history of fraud or account abuse. For more information on Early Warning Services, see www.earlywarning.com/about2.html.

example is the Information Sharing and Analysis Centers (ISACs) established under a presidential directive to improve information sharing about physical and cybersecurity threats. Several industry sectors, including the financial services industry, established ISACs in response to this mandate. The Financial Services Information Sharing and Analysis Center (FS-ISAC) provides an increasingly comprehensive information distribution system that allows a broad array of financial services companies, financial regulatory agencies, law enforcement and intelligence agencies, and nonbank firms integral to the financial sector to exchange information and receive alerts related to fraud, cybercrime, and data breaches, in a real-time or nearly real-time environment.[42] In addition, many U.S. states now require public disclosure of data breaches and notices sent to individuals whose records have been compromised. State laws establishing such requirements are designed primarily to mitigate harm to consumers after breaches have already occurred. Still, features such as credit report monitoring and credit freezes can help detect or prevent subsequent fraud attempts.

While FS-ISAC has played an important role in facilitating information sharing among firms in the financial services industry, data breaches can still occur at firms outside of this industry, and the data stolen in these breaches can result in financial fraud. Very rapid and detailed information sharing by breached parties across industry sectors might also help identify vulnerabilities before sensitive data are stolen from others and reduce the amount of information stolen. Additionally, speedy and thorough information sharing may lead to firms and industries quickly sharing best practices in response to a particular type of compromise. There are signs of ample demand for improved information sharing. In a recent survey, 93 percent of antifraud

[42] According to the FS-ISAC's website, the FS-ISAC "was established by the financial services sector in response to 1998's Presidential Directive 63. That directive — later updated by 2003's Homeland Security Presidential Directive 7 — mandated that the public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect the U.S. critical infrastructure." For more information about FS-ISAC, see www.fsisac.com/about/. Other industries have also established ISACs. For example, the communications sector and the electric sector have formed ISACs.

professionals agreed that information sharing helps prevent fraud, and 78 percent would like to see more information sharing.[43]

Today, in the United States, the mitigation of fraud risk in payment card systems is largely coordinated by network rules. These rules are determined by each network and must be adhered to by financial institutions (and their agents) that issue branded payment cards or acquire transactions made with those cards, merchants that accept payment cards, and third parties that process those cards. The revenues and profitability of payment card networks are generally increasing in transaction volumes. As a result, payment card networks have strong incentives to ensure the integrity of these electronic payment systems. In theory, they should also be able to shape the means of coordinating the incentives among their member institutions. Potential levers include technological standards, loss allocation rules, and variations in interchange rates, to name just a few.[44]

Further, as indicated earlier, the five major card networks have coordinated to establish uniform standards for data system security through the Payment Card Industry Data Security Standard. PCI DSS is the set of data security standards that all card network participants, including issuers, merchants, and processors, are required to meet.[45] (As of June 30, 2012, 97 percent of Level 1 merchants, 93 percent of Level 2 merchants, and 60 percent of Level 3 merchants were compliant with PCI DSS. Compliance among Level 4 merchants, however, remained "moderate.")[46] Unfortunately, several recent data breaches have occurred at firms

---

[43] See RSA Conference, eFraud Network Forum Program Committee, *2009 Online Fraud Benchmark Report*, April 15, 2009, p. 5, at https://365.rsaconference.com/docs/DOC-1895.

[44] The Federal Reserve Board's Regulation II applies to debit card issuers with consolidated assets of $10 billion or more and allows debit card payment networks to vary interchange rates for transactions below the maximum interchange fee permitted by the Board's standards.

[45] For more information on PCI, visit the PCI Security Standards Council's website at www.pcisecuritystandards.org/.

[46] Level classifications vary by transaction volume. According to Visa's website, Level 1 merchants process over 6 million Visa transactions per year. Other merchants may be required to meet Level 1 PCI compliance requirements at Visa's sole discretion. Level 2 merchants process between 1 million and 6

designated by auditors as being PCI compliant; such breaches naturally raise the question of whether PCI standards offer sufficient data protection for critical electronic payment systems. The networks and others have emphasized that PCI compliance is not a static concept; it is something that must be continuously monitored and addressed. Those within the industry continue to evaluate the effectiveness of the PCI standards, and the PCI Security Standards Council is working to improve upon the original requirements.[47]

Next, we describe the industry's views on whether the complexity of U.S. retail payment markets presents a barrier to private sector coordination of efforts to address data security issues. We also explore how policymakers might support such coordination efforts.

1. Interview Results

Most interviewees stated that an increased level of cooperation among payment participants is needed to enhance security. They offered specific suggestions for improvement, including mechanisms to share best practices and coordinate with law enforcement. Some interviewees said that the public sector could play a role in facilitating information sharing in the payment card industry, although opinions differed on whether the government has the necessary legal authority or whether further action is required to support such a role. At a minimum, one representative from a large financial institution argued that the federal government had an opportunity to improve processes for shutting down Internet sites selling stolen consumer data. Another representative from a large bank stated that current information-sharing mechanisms are

---

million Visa transactions per year. Level 3merchants process between 20,000 and 1 million Visa e-commerce transactions per year. Level 4 merchants comprise those that process fewer than 20,000 Visa e-commerce transactions and all other merchants that process up to 1 million Visa transactions per year. For more details, see http://usa.visa.com/merchants/risk_management/cisp_merchants.html. The compliance rates for the different merchant levels are available at http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf (accessed on October 3, 2012).

[47] For example, in October 2010, the PCI Security Standards Council released version 2.0 of PCI DSS. See "PCI Security Standards Council Releases PCI DSS 2.0 and PA-DSS 2.0," PCI Security Standards Council, press release, October 28, 2010. (www.pcisecuritystandards.org/pdfs/pr_101028_standards_2.0.pdf).

sufficient. Although this interviewee acknowledged that cooperation in response to new information might not be immediate, he said a positive spirit of cooperation exists.

The issue of competitive advantage was raised by several interviewees when considering the current state of coordination and information sharing among payment card system participants. Many said that as long as data security is seen as a differentiating factor that can be profitable, information sharing and cooperation will be more difficult to achieve. Despite this concern, several interviewees said that large card-issuing banks share information in a variety of ways, including through network-supported mechanisms and organizations such as FS-ISAC. Our interviewees indicated that information sharing by acquirers and merchants was more fragmented and less coordinated. Some of these companies are hindered by confidentiality or nondisclosure agreements with clients and, thus, are not allowed to coordinate and share information. In addition, one processor interviewee stated that a history of distrust of the payment card networks creates the perception that sharing information and, ultimately, coordinating with the networks may result in adverse consequences for a firm that admits to a data breach or other data security event. Further, some interviewees noted that, in the past, payment card networks did not always share data breach information with acquirers; rather, they shared this information only with card issuers.

Other interviewees noted that some acquirers and processors have prioritized information-sharing efforts. For example, according to our interviews, an information-sharing group was formed following a significant data breach, and details about malware used in this case were distributed to payment card processors. It turned out that this malware had been used by criminals in more than 650 breaches at 300 companies, compromising 200 million payment cards; yet, this particular vulnerability had not been widely understood.

Several interviewees noted that the public sector may be uniquely positioned to play a role in developing a framework supporting greater sharing of information about incidents of fraud and cybercrime within the private and public sectors and between them, as well as across

different industries. They said that government agencies such as the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) are well positioned to disseminate information about cyberthreats or to issue alerts. These agencies could also leverage their positions to get more players to participate in an information-sharing infrastructure.

In addition to information-sharing efforts, coordination is also important in setting standards or best practices for data security. As noted earlier, the development of PCI DSS is an example of a private sector effort to develop data security standards for participants in payment card systems. Several interviewees said that payment card networks are best positioned to design and enforce standards and to develop an effective set of "carrots and sticks" to encourage the various payment system participants to comply with the standards. An interviewee from a large bank noted that determining the right standards is not as difficult as enforcing those standards, specifically noting that the penalties for noncompliance need to be clear and enforceable. At the same time, interviewees disagreed on how successful PCI DSS has been at equitably meeting the needs of the very diverse group of payment system participants. Some merchant interviewees noted that if the standard itself is flawed, meeting a flawed standard defeats the purpose of better securing payment card systems. One interviewee suggested an alternative to PCI DSS, stating that there is a need for federal regulation or standards that would define the data necessary for parties to a transaction to execute the transaction and the parameters for how long the data should be held by those parties.

In regard to designing standards, several interviewees stressed the importance of providing all relevant participants an opportunity to evaluate the standards.[48] For example, these parties may have very different perspectives on the strength of compliance incentives ("carrots and sticks") incorporated into the standards for improving data security.

[48] The box on p. 7 provides a discussion of how the PCI Security Standards Council gets participating organizations involved in the process of evaluating and updating the PCI data security standards. For more detail on the rights and responsibilities of participating organizations, see www.pcisecuritystandards.org/get_involved/rights_responsibilities.php.

Interviewees generally agreed that law enforcement has become much more aware of the complexity of payment fraud and that the industry is learning how to cooperate with the FBI, Secret Service, FTC, and local law enforcement. One interviewee noted that federal law enforcement used to view payment fraud as a one-off event; but today, it recognizes that data breaches may threaten not only payment system security but also potentially the country as a whole (for example, if payment fraud is used to finance terrorist activities). This appreciation for data breach risks was one of the reasons the George W. Bush administration established its Identity Theft Task Force; the Obama administration has continued to focus on these risks, with special attention paid to cybersecurity.

In addition, the increasingly global scope of payment fraud also concerned a number of industry participants. Hackers are able to build and manage databases of compromised accounts across multiple locations, making their activities more difficult to track and their operations more difficult to dismantle. Criminals realize that they can launder money across a variety of international jurisdictions, taking advantage of differences in laws and regulations. Further, they are able to coordinate "money mules" who physically move money and goods around but do not necessarily understand that they are working for a criminal enterprise.

This degree of international activity poses a significant problem for law enforcement. Some of the most sophisticated criminal networks are well adapted for working across national borders, yet a few interviewees noted that state and national law enforcement agencies face more boundaries and less interagency cooperation. One interviewee stated that for fraud and cybercrime solutions to be effective, law enforcement agencies across the globe need to address geopolitical differences. Individual countries are pursuing their own security initiatives, but this

interviewee pointed out that there should be more discussion and collaboration among nations around the world to combat fraud and cybercrime. [49]

Variations in the legal definition of payment fraud are also important to consider, particularly given the global nature of payment card fraud. An interviewee offered this example: A phishing e-mail directs a person to a fake website, one that looks exactly like the real site but is controlled by hackers. This technique encourages the phishing target (the consumer) to visit the fake website and enter personal information. In some international jurisdictions, simply maintaining the fake website may constitute fraud, but in other countries, fraud has not occurred until money is actually stolen. Given such differences, anti-fraud measures may often be more difficult to enforce across borders than within them.

Other issues facing the enforcement of anti-fraud statutes include minimum-value thresholds for fraud cases and overlapping jurisdictions of the various law enforcement agencies. One interviewee said that cases are only likely to be pursued if they involve the theft of $10,000 or more; cases involving smaller amounts are unlikely to be investigated. This interviewee also commented that the government is dramatically under-investing in cybercrime investigations. Another interviewee claimed that having multiple law enforcement authorities with differing jurisdiction over payment fraud can spread resources to fight fraud thin. The consensus among participants in these interviews was that more resources both in law enforcement and in the regulatory community are required.

[49] The Federal Reserve Bank of Atlanta's Retail Payments Risk Forum addressed the need for improved international coordination among law enforcement organizations in its November 2011 payments conference, "The Role of Government in Payments Risk and Fraud." For a summary of the conference discussion, see www.frbatlanta.org/news/conferences/11rprf_summary.cfm.

V. Lessons from the Survey Findings

The management of payment card fraud raises a number of difficult questions: Have changes in technology increased or decreased the vulnerability of payment card systems to data breaches that might undermine consumer confidence in them? Do payment card networks, their partners, and their customers have the appropriate incentives to take precautions to avoid card fraud? Are the costs of payment card fraud or of avoiding this fraud borne by the appropriate parties? For example, do nonfinancial firms that retain personal or account data have sufficient incentives to protect this information? Are payment card networks able to make efficient choices about managing fraud risks and to implement antifraud measures in a timely manner? If not, are there reasons to believe that public authorities could facilitate better or timelier decisions? If such a role is appropriate, what information and expertise would government need to have?

The answers to these questions are not simple.[50] Taken as a whole, our interview results convey mixed views on most of these topics and, in particular, on the role that government should play or is capable of playing. At the same time, some general observations can be made with respect to areas of shared concern and insight among the interviewees.

Most interviewees recognized that payment card systems have benefited from dramatic advances in information, computing, and telecommunications technologies over the past four decades. These advances have helped create opportunities for new participants in payment card systems, such as nonbank payment providers, to introduce innovative products and services, such as prepaid cards

[50] For additional discussions of the policy issues related to fraud in consumer payments, see Nour Azzul-Razzak, Katy Jacob, and Dick Porter, "Improving Security for Remote Payments," Chicago Fed Letter No. 293 December 2011, at www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2011/cfldecember2011_293a.pdf. Also see Richard Sullivan, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Federal Reserve Bank of Kansas City *Economic Review* (Second Quarter 2010), at www.kc.frb.org/Publicat/EconRev/PDF/10q2Sullivan.pdf; and Katy Jacob and Bruce Summers, "Assessing the Landscape of Payments Fraud," Chicago Fed Letter No 252 (July 2008), at www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2008/cfljuly2008_252.pdf.

and Internet shopping. At the same time, these additions to the traditional payment card system model present new risks and require a re-evaluation of the security protocols that were developed in the past.

Of course, criminals can also leverage technological advances to develop, test, and deploy their tools quickly. And when they find a promising vulnerability, there is at least the possibility that their attacks will rapidly increase in scale. Several interviewees emphasized the adeptness of thieves to identify vulnerabilities and quickly exploit them. They also noted that the vulnerabilities may include a type of payment system participant and a point in the payment processing chain, as well as a data storage system risk and a software weakness. Any incremental risk that results from innovation should be offset by careful risk management and investments in new defenses, with an emphasis on dynamic and flexible data security approaches rather than static ones. Several interviewees observed that a national focus on the security of the information and communications infrastructure in the United States could result in significant improvements in securing retail payment systems, including payment card systems.

The interviewees expressed very mixed views about the incentives to prevent fraud and to mitigate its consequences among various payment system participants. Respondents generally considered the incentives at their organizations to be better than those in other parts of the transaction chain. This is perhaps an indirect recognition of the interdependence of payment participants in securing the system and the importance of adequate coordination of their efforts.

A number of interviewees stated that the protections afforded to consumers from losses associated with fraudulent transactions limit consumers' incentives to protect their cards, personal information, and computers. Others pointed out that these protections do help to ensure public confidence in card payments and that diluting those protections may increase the likelihood of a mass abandonment of these instruments if a "tail event" as we described earlier were to occur.

There was widespread agreement that a key ingredient in protecting payment systems from fraud is coordination of fraud defenses among participants in these systems. For payment card systems, this coordination function is generally performed by the networks. Many participants

expressed the view that, in the U.S., payment applications have become so diverse and payment firms so specialized that effective coordination is becoming more difficult. Others questioned whether the networks had exactly the right motivations or were sufficiently well equipped to ensure that all payment participants had the right incentives. Such concerns led some interviewees to speculate about an increased role of government as a coordinator. Others wondered whether government was sufficiently nimble or adequately equipped to play such a role.

There was greater consensus about a number of roles in which government either is essential or could likely be more helpful. The first is in its law enforcement capacity, which may require additional resources. Given the international character of many modern electronic payment systems, interviewees recognized that law enforcement efforts must also take on a more international character. This too will require additional coordination —in this case, among governments around the world. Also, interviewees mentioned the need for more comprehensive information about the volume, character, and drivers of payment card fraud and data breaches. In general, interviewees supported expanding the collection and dissemination of data and new research.

Most interviewees also said that the government could play a useful role in facilitating a more rapid dissemination of actionable information about new threats to the security of payment systems. Numerous information-sharing networks already exist, but some of our respondents contended that information exchanges remained too balkanized and too slow in many instances. The U.S. federal government is already an active participant in a number of these exchanges and, in some instances, contributes information obtained through various law enforcement and intelligence channels. [51]

Several respondents suggested that the government can play a special role as both a participant and a facilitator of the exchange of actionable information about data breaches because it

[51] Recently, Congress has been considering a number of cybersecurity bills that aim to increase the dissemination of actionable information obtained in the public sector as well as improve incentives for private actors to share the information they have. For further details, see Edward Liu, Gina Stevens, Kathleen Ann Ruane, Alissa M. Dolan, and Richard M. Thompson II, "Cybersecurity: Selected Legal Issues," Congressional Research Service Report to Congress, No. R42409, 2012.

may be uniquely positioned to address private-sector incentives in markets where security may be a source of competitive advantage. If maintaining a reputation as a secure provider of payment services is good for business, then firms will have incentives to invest in appropriate procedures and technology. But the desire to maintain a competitive advantage may act to discourage private actors from sharing information about the nature of any new threats they are experiencing. Government does not face this trade-off. In addition, by acting as an important source of information while insisting on reciprocity, government can tip private-sector incentives in the direction of sharing more information — and sharing it sooner.[52]

VI. Conclusion

Our electronic payment networks have evolved in such a way that they now provide greater flexibility, convenience, and efficiency for consumers, businesses, and governments. At the same time, these advancements can lead to opportunities for fraudsters, including the potential for large-scale data breaches. To manage these new risks, payment system stakeholders must continue to make security an integral part of providing retail payment methods. Our interview results suggest that to enable the smooth and efficient operation of the complex U.S. retail payment system, payment system participants need to find more ways to cooperate, share relevant information, and innovate to stay ahead of criminal gangs that perpetrate payment fraud using an array of sophisticated tools and procedures.

[52] This is analogous to the role that private credit bureaus play. In the U.S., reporting to a credit bureau is not mandatory. Yet hundreds of thousands of organizations find it worthwhile to share their information in exchange for the ability to use information provided by all members.