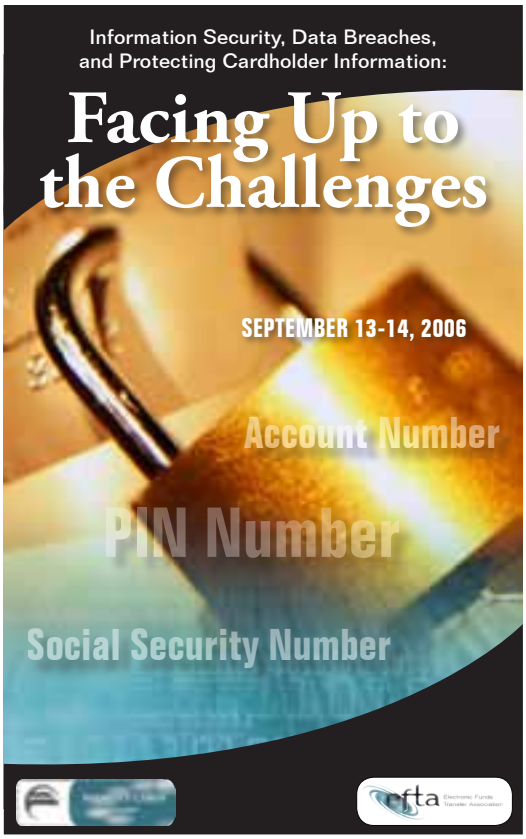
CONFERENCE SUMMARY



Information Security, Data Breaches, and Protecting Cardholder Information:

Facing Up to the Challenges

September 13-14, 2006

PAYMENT CARDS Center

FEDERAL RESERVE BANK OF PHILADELPHIA

Information Security, Data Breaches, and Protecting Cardholder Information:

Facing Up to the Challenges

September 13-14, 2006

James C. McGrath*
Ann Kjos

Summary

On September 13 and 14, 2006, the Payment Cards Center of the Federal Reserve Bank of Philadelphia and the Electronic Funds Transfer Association (EFTA) hosted a conference entitled "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges." The two-day event was designed to bring together a diverse set of stakeholders from the U.S. payments industry to discuss a framework to guide industry practices and inform public policy. In attendance were individuals from the major payments networks, card issuers, and banks, as well as consumer and merchant representatives and regulators. Conference participants emphasized that the industry must address two fundamental issues: (1) increasingly dangerous threats to sensitive consumer information and (2) public perception and understanding of the risks from data breaches. These challenges are related but need different solutions. A consensus emerged that while the situation is not yet dire, it is serious. All payments stakeholders must be ready to work together to devise solutions today so that the benefits of the electronic payments system are uninterrupted in the future.

** Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: james.c.mcgrath@phil.frb.org. The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.*

TABLE OF CONTENTS

I. Introduction

On September 13 and 14, 2006, the Payment Cards Center of the Federal Reserve Bank of Philadelphia and the Electronic Funds Transfer Association (EFTA) hosted a conference entitled "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges." The two-day event was designed to bring together a diverse set of stakeholders from the U.S. payments industry to discuss a framework to guide industry practices and inform public policy.[1] In attendance were individuals from the major payments networks, card issuers, and banks, as well as consumer and merchant representatives and regulators.[2]

The conference sessions addressed two fundamental questions. First, what can be done to more effectively ensure data security throughout the entire payments chain? Second, should a breach occur, what are the appropriate actions that should be taken to protect consumers and mitigate risks associated with any compromised data?

These issues have come to the fore as a variety of breaches from a number of firms have been widely publicized in the media. Consequently, they have become a topic of debate in Washington and state capitals across the country. Breaches threaten to undermine a fundamental underpinning of the payments industry: consumer confidence in the industry's ability to protect and safeguard sensitive customer information. A related discussion covered the concurrent need for hard data to critically evaluate the severity of the perceived threat and to increase public understanding of the real nature of the threat. Intertwined were discussions as to how these issues might be reflected in the emerging legal and regulatory framework.

Charles I. Plosser, president of the Federal Reserve Bank of Philadelphia, opened the conference on Wednesday afternoon. Plosser focused the audience's attention on how advances in technology and changes in regulation are changing the payments landscape. These changes are of interest to a variety of participants and stakeholders, including the Federal Reserve System. Plosser introduced Bruce J. Summers, director of Federal Reserve Information Technology (FRIT), whose keynote address elaborated on these implications.

Summers oversees the area of the Federal Reserve responsible for standards and information architecture used throughout the Federal Reserve System. He described how the fiduciary responsibilities of commercial banks and the Federal Reserve Banks have grown along with the advent of electronic banking and the increased reliance on information technology. Summers framed his discussion of security by examining best practices for safeguarding information security in three forms: information "at rest," that is, stored on a bank's computer; information "in transit," that is, on the move over networks; and "information traveling," that is, on a laptop or other movable storage device.[3]

Summers's address was followed by a panel discussion, "Baseline Issues for Payments Participants: Setting the Stage," which incorporated perspectives of banks, merchants, networks, and technology providers. The panelists warned that consumer confidence is under siege because of real and perceived threats. At the same time, while fraud does exist, widespread misunderstanding of the practical issues is a comparable concern. Panelists suggested that these problems should be addressed concurrently, but they emphasized that they involve different solutions and different incentives.

H. Kurt Helwig, executive director of the Electronic Funds Transfer Association, opened the second day of the conference, emphasizing that security can serve as a key business differentiator. He observed that the companies attending the conference are well aware of security's importance and take the issue very seriously. Nevertheless, they also agree that they must do a better job communicating two things: what customers can do to help in the fight and what companies are doing internally to protect customer data. Communicating this message is critical, he warned, because losing consumer confidence may threaten the underlying payments business itself.

These insights would be echoed throughout the day's sessions. In particular, Orson Swindle, senior policy advisor and chair of the Center for Information Policy Leadership at Hunton & Williams, a major international law firm, expanded on these themes with

[1] For the conference agenda, see Exhibit 1, on page 23.

[2] For a list of the institutions represented at the conference, see Exhibit 2 on page 24.

[3] Summers's comments are explored in more detail on page 6.

a keynote on the second morning of the conference: "The Sky Is Not Falling — But It Could."[4] Swindle emphasized that the payments industry is predicated on the free interchange of information. This openness has brought about great innovation, but it increasingly presents unique risks. He called on conference participants to apply sound principles and solutions, many of which already exist, to ensure that customers' data are protected. Doing so, he argued, can be a competitive advantage.

Swindle's address was followed by a panel, "Ensuring Data Security," which delved into concrete technologies, solutions, and best practices that can be brought to bear to address the problem. The panelists related the increased sophistication of fraudsters who continue to challenge increasingly rigorous solutions. The industry finds itself playing a game of cat and mouse, but at the same time, the panelists argued that there are viable practices and procedures that can provide a defensible data protection strategy.

Two afternoon panels concluded the conference. The first, "After a Breach: Protecting Customers and Consumers," focused on what to do if and when a breach occurs. Panelists emphasized that early planning is critical; the most robust data security program must be accompanied by a well-defined action plan in the event that the unthinkable occurs. Among the issues discussed were the role and shape of notifications, consumer sentiment and understanding, and the implications for payments providers.

The second, "Legal and Regulatory Perspectives," attempted to place the issues raised throughout the conference into the emerging legal and regulatory framework. The panelists contrasted state and federal initiatives, discussed trends in regulation and enforcement, and addressed the degree to which the regulatory environment has been a constructive partner in designing solutions.

To close, Peter Burns, director of the Philadelphia Federal Reserve Bank's Payment Cards Center, summarized several of the conference's key themes. He noted that effective industrywide solutions are imperative. These must be built around the correct incentives, should include the full range of stakeholders, and should encourage collaboration. A compelling business case exists for effective security; the challenge will be to develop and explain it. Burns noted that the Federal Reserve can contribute to this effort by convening the right people and encouraging a frank and open debate, as was evident during the discussions that took place over the course of the conference.

II. Wednesday's Keynote Address: Bruce J. Summers

Bruce J. Summers opened the conference with a keynote address entitled "Fiduciary Responsibilities in the Era of Electronic Banking: A Central Banker's Perspective."[5] In his remarks he described how the evolution of electronic processes and the impact of information technologies have expanded the concept of fiduciary responsibility for all financial institutions, including the Federal Reserve Banks. While acknowledging clear differences between the Federal Reserve and private-sector banking institutions, Summers emphasized that the Fed and financial institutions have many issues in common when it comes to considering the challenges associated with information security. He framed his discussion of data security practices at the Federal Reserve by considering data in three distinct environments.

Summers briefly outlined the Federal Reserve's responsibilities, including conducting monetary policy, supervising and regulating banking institutions, and maintaining the stability of the financial system. For the purposes of this discussion, he focused on the Fed's role as a provider of payment services and the impact advances in information technology have had on redefining the Fed's own sense of fiduciary responsibilities.

Like all financial institutions, the Federal Reserve Banks have had a long-standing focus on their responsibility for protecting financial assets under their stewardship. The age of electronics, however, has broadened these fiduciary responsibilities to incorporate the security of information assets as well. He argued that all financial fiduciaries, including central banks, need to embrace the concept of "electronic

[4] A detailed discussion of Swindle's comments starts on page 7.

[5] Summers joined the Federal Reserve System in 1974 and has been the director of Federal Reserve Information Technology (FRIT) for the past 10 years, overseeing the central bank's IT environment in a period of dynamic change. FRIT is responsible for the Federal Reserve System's information technology architecture and standards. It also provides technology services to the 12 Federal Reserve Banks and the Board of Governors. Before Summers assumed responsibility for IT, his career with the Federal Reserve included a broad range of business management positions.

vaults" to protect information assets in the same way that steel vaults have long been employed to protect physical assets. The technology used to secure information in an electronic vault, such as cryptography, can be costly, leading to important funding and budgeting decisions. Summers noted that weighing these investment decisions against the potential costs of not doing so are concerns common to all institutions entrusted with customer information, whether they be private banks, other businesses, or the Federal Reserve.

In describing the challenges of ensuring data security, Summers framed the issue by categorizing data into three broad states: data-at-rest, data-in-transit, and data-on-travel. Data at rest — that is, data residing on computers or other devices inside an organization — present a particular risk because of the data's vulnerability to insider threats, often the hardest threats to protect against. Summers pointed out that to protect data at rest from insider threats, institutions need technology solutions and human resource practices that focus on data security. At the Fed and other institutions, practices such as internal network segmentation and the doctrine of least privilege are used to protect data at rest. Finally, strong methods for authenticating the identity of those with access to the data are also critical mechanisms for protecting data at rest.

Summers stated that security of data in transit — information traveling over networks — is in some sense the most straightforward challenge to address.[6] Summers noted that strong encryption systems along with strong authentication methods go a long way toward ensuring the security of information traveling over networks.

Data on travel — on a laptop or other transportable storage device — presents a relatively new challenge. Data are no longer stored just on computers; they're also stored on thumb-drives, PDAs, cell phones, and so forth. To address these new challenges, the Federal Reserve has policies that define appropriate use of data and how and where the data can be transported. Hard-disk encryption and limitations on user-administration privileges are two examples of Fed practices aimed at protecting data on transportable storage devices.

In closing, Summers reiterated that in the era of electronic banking, the importance of protecting information assets has been elevated to at least the same level as traditional concerns about protecting physical assets, and arguably, protecting electronic information presents a more complex challenge. Summers emphasized the importance of recognizing the business value of meeting information security issues in three ways. First, just as money belongs in a physical vault, sensitive information belongs in an electronic vault. Second, data must be protected at rest, in transit, and on travel. Third, we need to think about security holistically; it involves both people and technology.

Summers's comments highlighted data security as a fiduciary responsibility of the Federal Reserve and, even more broadly, of financial institutions and other payment providers. Moreover, he emphasized that the recent movement toward electronic payments has introduced a different set of risks than those found in the traditional paper-based system. The themes developed in these opening remarks were addressed more specifically in the conference discussions that followed.

III. Thursday's Keynote Address: Orson Swindle

Orson Swindle[7] opened the second day of the conference with his keynote address, "Information Security: The Sky Is Not Falling – But It Could." In his remarks, Swindle emphasized that while we may not be in a crisis with respect to data breaches today, the risks to the financial services industry are indeed real. Swindle addressed several issues that were subsequently echoed throughout the conference: the costly consequences of compromises, the need for solutions that emphasize collaboration and cooperation among participants all along the payments chain, and the role of government agencies. He concluded by urging that efforts to address data security also take into account the critical role that the free flow of information has in

[6] Securing data in transit may be less straightforward in the private sector, where there is often a more extensive processing chain with multiple parties using several networks. Many participants referenced the Payment Card Industry Data Security Standard (PCI) throughout the conference as an important mechanism for ensuring compliance with data security standards all along the card processing chain.

[7] Prior to joining the Center for Information Policy Leadership at Hunton & Williams, LLP, as the senior policy advisor and chair of information security projects, Swindle had a distinguished career in public service. He served in the Reagan administration from 1981 to 1989, first with the Department of Agriculture, then as assistant secretary of commerce for development. From 1998 to 2005 he served as one of the five commissioners of the Federal Trade Commission.

the modern economy and in enhancing public welfare.

Swindle began with the assertion that data security measures "may be costly to employ, but more costly not to." He described several of the direct financial costs that a firm whose data security has been compromised might face, including stock market effects,[8] exposure to fines from card networks and government agencies, and the direct costs associated with notifications, card replacement, and customer service support. In addition, Swindle explained that, given cause, the Federal Trade Commission (FTC) is empowered to order firms to undergo annual security audits for up to 20 years following a breach, an obviously onerous and costly exercise.

Swindle argued that while these direct financial costs should serve as significant motivating factors for individual firms, a potentially greater cost to the industry may result from a loss in consumer confidence. Should consumers lose confidence in the safety of electronic payments and commerce, they might abandon these channels and revert to less efficient means of making purchases and payments. He characterized this risk in terms of an "opportunity cost" in that e-merchants and payment providers risk losing the opportunity to regain the abandoned transactions.

In protecting data security, Swindle emphasized that the system as a whole is only as strong as the weakest link. A data compromise can occur anywhere in the payments chain but will affect all stakeholders. He urged conference participants, in their search for solutions, to develop strategies that incorporate collaboration and cooperation among all stakeholders.

While acknowledging the efforts of Congress to create federal standards for responses to data breaches, Swindle focused on two other important roles government can play. In the first case, government agencies – including the Federal Reserve – are appropriate parties to help facilitate information sharing and encourage collaboration among payments industry stakeholders. Second, as data breaches and resulting fraud have become international issues, it is critical that the U.S. government take the lead in ensuring cooperation and coordination among national law enforcement agencies and governments.

[8] He noted that typical market-value declines of 9 to15 percent follow a public company's announcement of a breach.

In all of the discussion about data security, Swindle urged that we not lose sight of the importance that data and information technologies play in our modern economy. Information is a valuable and powerful resource that has led to any number of welfare-improving innovations. Going beyond the familiar example of the payment cards industry where competency in managing information is at the heart of business model innovations, Swindle provided another provocative example from the medical research field. As he described, medical research breakthroughs depend heavily on the ability to access and analyze data on as many trial subjects as possible and across as many states, regions, or nations as possible. As this example illustrates, we need to be vigilant in protecting sensitive information but we must also recognize that the free flow of information is often a critical element in welfare-enhancing innovation.

Swindle closed by asking conference participants to acknowledge the increasingly dynamic nature of the challenge and to think beyond the current environment and address information security issues by looking forward five to 10 years. He called for innovations to protect consumer information and emphasized the importance of maintaining consumer confidence through open and clear communication. Consumers need to know that the industry is concerned, making changes and taking precautions to protect their information. Swindle stressed that "we all have a role to play and we need to get it right." Swindle's address brought a sense of urgency to the issues surrounding data security and set an effective framework for the second day of the conference.

IV. Background

The national media have frequently and widely publicized security breaches, and these reports have attracted the attention of policymakers and caused unease and confusion among the public. While data breaches are indeed a serious issue that industry participants and consumers must confront, they are often poorly understood. The conference discussions were oriented toward teasing out the actual extent of the risk, discussing containment and mitigation strategies, and exploring where and how regulatory involvement may be constructive.

A unifying theme that emerged was that payment industry stakeholders have two related but dis-

tinct problems to address and these problems call for different kinds of solutions. First, there is a growing, real threat to the security of information used within the payment system. Second, growing public concern about these issues threaten consumer confidence in the payment system. If consumers lose confidence in the safety of the system because of legitimate concerns or overreactions to poorly understood media accounts, the industry may lose its flexibility in developing and applying innovations that could ultimately improve the efficiency of payments. Moreover, since payments are a "two-sided platform market," the risks flow in both directions. As panelist Tom Arnold, of PSC, warned, merchants themselves could lose faith in certain electronic-based payment instruments and may ultimately be hesitant or unwilling to adopt these payments innovations.

Both of these problems threaten to undermine the very foundation of the payments industry. The payment system has been built on the open and rapid transmission of data between payment providers and consumers. Both adverse public reaction and stopgap regulatory interventions could increase frictions in this process, participants argued, reducing efficiency and increasing costs.

In summary, there are very real risks and substantial misunderstanding about threats to data security. Yet, as conference participants noted, solutions to many of these threats already exist. Successfully addressing the problem will require a holistic approach and long-term involvement, and even if the risks cannot be completely eliminated, they can be controlled. It is incumbent upon all participants in the payments system to work together to ensure that this happens. At the same time, some payments participants emphasized the need to use media and marketing proactively, to encourage safe practices, and to explain how the industry is working to protect consumers' data.

This paper will echo many of the findings of the conference. While the paper is broadly organized along the same lines as the sessions over the two days, it does not offer a verbatim transcript. Rather, it seeks to integrate insights from the various panelists, speakers, and the audience into a thematic exploration of various aspects of data breaches and their consequences. It begins with a brief discussion of the costs of data breaches to consumers and to firms and includes an in-depth look at the concept of identity theft to establish a consistent vocabulary to be used throughout the rest of the paper. Data breaches do not necessarily lead to identity theft, nor are they the only means by which identity theft may occur. However, because the two concepts are frequently associated, at times incorrectly, defining terms clearly is useful. The paper then addresses the extent of the problem, what can be done to prevent data breaches, and how to respond if one does occur. Finally, it addresses challenges associated with disclosures and closes with a consideration of the role of government and opportunities for the Federal Reserve and other agencies to further contribute to the debate.

V. Framing the Issues

Data breaches and their consequences have become more prominent in the press — in part because of recent state and federal regulations requiring their disclosure — though not necessarily better understood. California's Senate Bill 1386, which was enacted in August 2002 and became effective in July 2003, has become a benchmark for data breach notification. It has effectively required firms that do business in California to notify consumers when a data breach has occurred, regardless of whether the information lost has fallen into the wrong hands, is suspected to have been used illegally, or has contributed to identity theft.[9] The California market is sufficiently large that if consumers there are affected, a breach likely has consequences nationwide. Thus, the California notification requirement has served as a de facto notification requirement to customers across the country.

According to a study conducted by the Ponemon Institute and the law firm of White & Case, LLP, 23 million consumers recall receiving a breach notification in the past year. Another survey reveals that 52 million consumers had their personal information breached in approximately 100 separate incidents in 2005 alone.[10] However, such large numbers are difficult to interpret. Some individuals may be double counted and some incorrectly identified. Most important, data breaches vary in their potential to cause

[9] http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[10] VigilantMinds, Inc., "State Security Breach Legislation," February 2006. (http://www.vigilantminds.com/files/vigilantminds_state_security_breach_legislation_summary.pdf)

damages. The loss of account numbers without names and addresses, for example, is potentially less damaging than a data file that cross-references that data file with Social Security numbers.[11] Because of these complications and others, increased emphasis on notification and subsequent media coverage have raised as many questions as they have answered.

One of the recurring subtexts of the conference was the difficulty that consumers, policymakers, and even some in the payments industry itself have in agreeing on terminology to describe the consequences of data breaches. Or they may confuse the report of a data breach with actual fraud. Additionally, media reports will often lump many substantively different frauds under the catchall of identity theft, but as many conference participants noted, doing so may confuse the discussion and make it more difficult to fashion effective solutions. In some cases, policymakers themselves have struggled with the lack of consistent terminology, compounding the difficultly in formulating constructive regulation.

The term data breach has come to mean simply the breach or loss of computerized data that includes personal information. However, since much hangs on how the data are defined, how they are breached, and who may have gained access, discussions of data breaches, especially within the government and regulatory community, may help to refine and qualify this simple definition.

Such breaches can occur through a number of channels; most, according to a recent Ponemon Institute study,[12] arise from lost or stolen computer hardware or media;[13] fewer come about through deliberate system hacks, viruses, Trojan horses, or similar technological assaults. Importantly, as Lynne B. Barr, of Goodwin Procter, noted, the occurrence of a data breach does not imply that the company involved has been negligent.[14]

After a breach, whether it was caused by chance or deliberately, the compromised information could potentially be used to perpetrate fraud, including that associated with identity theft. Identity theft becomes important in the discussion of data breaches because it is one of the most highly publicized, yet least understood consequences, as well as arguably the most serious potential consequence for consumers.

Next, this summary will consider the consequences of data breaches to consumers, focusing particularly on identity theft. It then considers the consequences of data breaches for firms and financial institutions, before examining the evidence regarding the connection between identity theft and data breaches.

VI. Data Breaches, Identity Theft, and the Impact on Consumers

Data breaches affect consumers in two principal ways. First, consumers are subject to uncertainty, confusion, and potentially a loss of confidence in the payments system when they hear about data breaches. If they do receive a breach notification, they often struggle to understand what it means and how it could be relevant to their own situation. This process can take time and cause anxiety. Second, consumers could become victims of identity theft, which could lead to much more aggravation and cause real financial losses.

A baseline definition of identity theft can be found in the Identity Theft and Assumption Deterrence Act of 1998, in which identity theft is described as a range of illegal activities that use a person's personal information to perpetrate a crime. While that definition remains true, it begs a more nuanced understanding, since the definition covers crimes ranging from those involving a lost or stolen credit card, to sophisticated schemes to surreptitiously open new accounts in a victim's name. While conference attendees disagreed somewhat over which terms to use, they gen-

[11] Increasingly, these lines have been blurred, since many organizations have been accumulating and storing data with personal identifying information, including Social Security numbers, for which there is an ambiguous business justification. In fact, the California Office of Privacy Protection reports that 85 percent of the security breaches in its survey involved Social Security numbers, exposing those victims to considerable risk. See California Office of Privacy Protection, "Recommended Practices on Notice of Security Breach Involving Personal Information," April 2006.

[12] Ponemon Institute, "2006 Annual Study: Cost of a Data Breach," October 2006; available at http://www.vontu.com/uploadedFiles/global/2006_Cost_of_Data_Breach_Report_V_2.pdf.

[13] Or in the terminology applied by Bruce Summers, "data on travel."

[14] As Joel Winston, of the Federal Trade Commission, would note, data breaches per se do not violate the law. A company can take reasonable precautions and still be victimized. However, the failure to adequately secure consumer data can be grounds for being found in violation of the "unfair or deceptive practices" standard of the Federal Trade Commission Act and possibly the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act.

erally agreed on a three-tier hierarchy of identity theft categories to refine the concept further. For the purposes of this summary, the terms payment card fraud, account takeover fraud, and true name fraud will be used.[15] Definitions do matter because the causes and consequences of these different types of fraud can be starkly different.

Payment card fraud is generally the least damaging type of fraud for the consumer. It involves criminals stealing payment cards or account numbers of existing accounts to purchase goods or services. In this type of fraud, consumers retain control over the account relationship. It is often quickly discovered by card issuers' fraud detection software or as consumers review their statements, and thus the scope of the fraud is limited. Because federal law and card network policies limit liability for fraudulent purchases, consumers have very few out-of-pocket expenses. They can be issued a new card and the fraud is contained.

In contrast, account takeover fraud is more insidious. Rather than making a few illicit purchases, in such frauds, criminals have access to more detailed consumer information, allowing them to attempt to take complete control of a credit or debit account and entirely deplete it. They even occasionally cloak their activities by changing the billing address so that they can benefit from extra days or weeks of unnoticed fraudulent activity.

For consumers, true name fraud is even more insidious. Here, criminals use a consumer's personal identifying information, or PII, to create new credit accounts attached to other addresses without the consumer's knowledge. The consumer will likely not receive any statements or other communication — at least initially — that would indicate that these accounts exist, making detection very difficult until the damage is already done. As panelist Daniel Buttafogo, of Barclaycard US, argued, breaches leading to the loss of personal identifying information can result in the most costly and hard to control fraud. When this happens, consumers will need a lot more hand-holding during the difficult process of cleaning up the damage that could result. Stuart Pratt, of the Consumer Data Industry Association, reported that fortunately, FTC data indicate that fewer than one-third of identity theft cases involve this severe form of fraud. However, the data also suggest that about 1000 people per 100,000 are victims of true name fraud. While less frequent than other crimes such as burglary or robbery, this crime still involves a considerable number of victims.

Consumers face potentially large costs in time and money when they become victims of this crime. For instance, Javelin Strategy and Research reports that the average out-of-pocket expense to true name fraud victims is $422 and they spend 40 hours of their time cleaning up the problem.[16] Fortunately, 68 percent of identity theft victims actually incur no out-of-pocket expenses. However, financial institutions and merchants do pay a price — often a sizable one.

VII. The Impact of Data Breaches on Businesses

For firms, data breaches may cause considerable expense, whether or not identity theft arises. For instance, the Ponemon Institute found that the average cost of a breach, above and beyond any consequences of the misuse of data that may result, was $182 per data record. Per incident, for the 31 breaches covered in the study, this amounts to an average cost of $4.8 million per incident, per firm, and reflects an increase of 30 percent over the costs of a year before.[17]

These costs primarily derive from the company's notification response. Many card issuers whose customers' data may have been compromised often choose the more expensive tack of contacting consumers by phone rather than mail. Further, acknowledging the risk that victims may opt to close accounts, issuers may also offer incentives to customers to discourage them from taking their business elsewhere. Finally, the tab could include fines and restitution ordered by the Federal Trade Commission or banking regulators and

[15] A more extensive discussion of identity theft, these categorizations, consequences, and best responses can be found in the PCC paper by Julia S. Cheney, "Identity Theft: Do Definitions Still Matter?," August 2005. Cheney discusses a fourth type of fraud — fictitious identity fraud — in which criminals may combine legitimate information with made-up information to "create an identity that does not belong to any real person." While this type of fraud can indeed be costly, it was not discussed at the conference. For the purpose of this discussion, these fraud losses, which are generally absorbed by financial institutions or merchants, are addressed in the next section of this summary.

[16] Rubina Johannes, "2006 Identity Fraud Survey Report," Javelin Strategy and Research, January 2006, available at http://www.javelinstrategy.com/products/AD35BA/27/delivery.pdf.

[17] Daniel Wolfe, "Higher Costs for Data Breaches — Both Old and New," *American Banker*, October 24, 2006.

the costs of paying for credit monitoring services for consumers whose data were exposed.[18]

The direct financial costs from data breaches are just the beginning. Organizations may also face regulatory, reputational, and opportunity costs as well. Joel Winston, of the Federal Trade Commission, detailed a number of ways in which financial institutions can be punished in the event of a data breach — from card association penalties to fines imposed by various regulators. There are also ways to penalize nonbank organizations, and most of the penalties flow from the Federal Trade Commission. The FTC has the authority to impose an annual 20-year audit requirement on firms that were subject to a breach and that were found to have failed to adequately secure customer data. Such audits can be rigorous; complying with them for 20 years can be costly.

Finally, as Gray Taylor, from the National Association of Convenience Stores, noted, the damage to a firm's reputation may be the most severe penalty. Even if victims of a data breach do not suffer direct negative consequences such as identity theft, conference participants highlighted the fact that consumers may lose confidence in the organization holding their data. According to the Ponemon Institute, 20 percent of consumers who received notice of a security breach immediately terminated their accounts. This number indicates a potentially severe threat. While changing a long-standing relationship involves considerable frictions, it is very easy to find other providers who haven't appeared in negative media reports.[19] Thus, while a 20 percent decrease in accounts is very serious, Orson Swindle emphasized that the ultimate problem, while not directly measurable, is the opportunity cost of lost business. If consumers lose confidence in the electronic payments system, they may avoid online transactions altogether or revert to greater use of cash or checks. Were this to happen, revenues associated with these lost transactions would never be realized. The policy implications for the continued evolution of a more efficient payment system are also clear.

VIII. The Connection Between Data Breaches and Identity Theft

As discussed earlier, a data breach need not lead to identity theft, and identity theft often arises from compromised data obtained from sources not generally associated with public accounts of data breaches. For example, according to Javelin research, most identity theft fraud arises not from data breaches but rather from data stolen by acquaintances or family members or from lost or stolen wallets or statements.[20] Similarly, a malicious employee with access to consumers' personal identifying information can cause real problems by simply copying relevant information about an individual or groups of individuals. Indeed, according to Bruce Summers and others, this has become a growing concern, requiring organizations to develop new internal access controls.

Complicating matters is the difficulty involved in conclusively tying a given breach to consequent reports of actual identity theft. Additionally, according to Daniel Buttafogo, frictions in the post-breach notification process mean that affected individuals may not know they are at risk until a year or more after the actual data compromise. The upshot of this is that the damaging effects of a given breach may be significantly remote in time from when it actually happened and the communication of the potential risks slow, compounding the difficulties faced by issuers' fraud management teams, law enforcement, and consumers.

However, if the breach does lead to identity theft, the toll can quickly escalate. On one hand, as a recent survey suggests, the odds of a data breach resulting in some sort of identity theft are comparatively small.[21] Indeed, the Javelin study estimates that only 0.8 percent of consumers exposed to a data breach become victims of fraud. At the same time, Javelin estimates that during 2006, approximately 9 million

[18] Firms also bear sizable costs from identity theft. According to the Javelin study, the average cost per identity fraud case has increased from $5,249 to $6,383 over the past two years. If we incorporate the decrease in the annual number of incidents, this means that the total one-year cost of identity fraud in the United States, across all industries, grew slightly between 2003 and 2006, increasing from $53.2 billion to $56.6 billion — a very substantial sum.

[19] The Ponemon Institute has prepared an estimate of the extent of losses due to account churn induced by a data breach. See the Ponemon Institute, "National Survey on Data Security Breach Notification," September 26, 2005.

[20] Rubina Johannes, "2006 Identity Fraud Survey Report," Javelin Strategy and Research, January 2006, available at http://www.javelinstrategy.com/products/AD35BA/27/delivery.pdf. This Javelin report is an update to research originally published by the Federal Trade Commission and Synovate, a consulting firm. It is available at the FTC's website at http://www.consumer.gov/idtheft.

[21] Mary T. Monahan, "Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses," Javelin Strategy and Research, August 2006. http://www.javelinstrategy.com/research

individuals had some portion of their personal identifying information exposed as a result of data breaches. Together, these numbers imply that over 70,000 people could be victimized by data-breach-related identity theft at some point — a not insignificant number.

From another perspective, Javelin estimates that 6 percent of all known identity theft is generated from data breaches. If overall identity theft losses are $56.6 billion, this implies that approximately $3.3 billion of this sum derives from data breach incidents.

Finally, other observers note that recent experiences suggest that fraud resulting from data breaches may be growing and may result in identity theft more often than in the past. For instance, Daniel Buttafogo noted that several incidents have occurred in which the sensitive data encoded on thousands of cards' magnetic stripes have been compromised in a data breach. The loss of this particular kind of data can be especially costly to issuers and consumers, since a sophisticated criminal can use this information to create counterfeit cards to make purchases or ATM withdrawals.

Data breaches expose consumers and firms to risks across a number of dimensions. Thus far, identity theft has been a relatively infrequent consequence of a data breach, but because it is so disruptive for consumers — especially if it is the most pernicious type, true name fraud — it constitutes a real concern. Moreover, virtually all consumers are affected by widely publicized accounts of data breaches, potentially influencing their behavior and confidence in the use of electronic payments.

On the supply side of the payments industry, firms bear many direct incremental costs related to data breach notification and other customer service requirements, and they are further subject to the imposition of fines and potential sanctions by the FTC. They also often suffer from lost productivity due to the need to quickly redeploy resources to contain a breach and mitigate its consequences. Additionally, financial institutions and merchants disproportionately bear the high costs of identity theft, since they, rather than consumers, ultimately bear the expense of fraudulent accounts. Finally, the opportunity cost of lost business constitutes a costly, though difficult to quantify threat.

IX. The Incentive Problem

Clearly, the issues outlined above and discussed in detail during the conference present a very serious challenge to stakeholders in the payments system. However, attendees also argued that some payments participants have not yet done all they can to address this problem. Many technological solutions may already exist, but to date, there have been problems devising effective incentives to induce merchants, issuers, and networks to make the necessary investment and commitment. For instance, the ability exists to process PINs for every transaction, to use chip technology, and to use a private key and data encryption for all transmissions, but these have not been mandated and have seen limited implementation. As Daniel Buttafogo and Gray Taylor observed, many in the payments business responsible for fraud management would welcome enhanced authentication tools such as chip and PIN technology, but the costs are high and it is not clear who is able or willing to pay for this.

Such additional investment has been slow to materialize for a number of reasons. First, by some measures, the payment card industry has done a good job controlling fraud. With credit card fraud holding fairly steady at 7 basis points (0.07 percent), net of chargebacks,[22] the costs associated with this effort are significant. Credit card networks, issuers, and other industry participants have invested substantial sums, over many years, in information technology and procedures to detect and prevent fraud on their systems. The industry's ability to maintain fraud at a relatively low and steady rate is a testament to the efficacy of that investment. Nonetheless, as panelists affirmed, the industry would always like to see lower fraud rates. However, they cautioned that the cost of eliminating the last dollar of fraud, as opposed to the first, would be prohibitively expensive. There are clearly diminishing marginal returns in this struggle.

Yet, if criminals are deterred in one area, they may increase efforts elsewhere. As Avivah Litan, from Gartner, warned, there is the risk that fraud might continue to migrate to more vulnerable sectors, away

[22] Fraud numbers are notoriously difficult to calculate and incompletely understood, perhaps preventing full acknowledgment of the scope of the problem. For instance, while the net fraud loss to issuers has been stable at a fairly manageable 6 to 7 basis points, conference participants noted that merchants and acquirers absorb at least another 5 to 7 basis points of losses and chargebacks. Another, unquantified amount of fraud is handled through direct mediation between consumers and merchants. Thus, a nuanced view of the extent of fraud, looking across all stakeholders, suggests that it remains a serious issue.

from the oversight of the card industry, where it may be even harder to detect, less publicized, and more difficult to eradicate. For instance, if the card industry maintains and increases its robust defenses, fraudsters are likely to turn their attention to other areas such as ACH, checks, and brokerage accounts. At the same time, some have also warned that the U.S. payment card industry, thus far successfully reliant on magnetic stripe authentication technology, may become more vulnerable as card programs abroad implement chip and PIN technology more widely and fraudsters move to the less secure U.S. markets.

Merchants are conflicted. While they may bear the costs of chargebacks, they also look to increase throughput at the point of sale, and thus they may be less inclined to embrace techniques that cause more hassle in the checkout line. Moreover, there are difficult tradeoffs between the customer experience and data security. Lee Manfred, of First Annapolis, noted that some merchants have argued that there are real benefits to the customer experience from saving data. For instance, popular in-store loyalty programs that identify customers at checkout are often built around merchant-based storage of some types of customer information. Yet, in the never-ending quest to speed consumers through the checkout line more quickly, some merchants may be unwittingly creating attractive targets for criminals and increasing their susceptibility to the consequences of human error. All things equal, the more consumer information that is stored, the greater the repercussions if it is compromised.

Russell W. Schrader, from Visa USA, echoed these thoughts but emphasized that all payments system stakeholders benefit from a free and efficient flow of information. For example, instant credit approvals for new store credit applications are valuable to merchants and helpful to consumers, but at the same time, they present a potential security risk. All of these tradeoffs expose the tensions inherent in the campaign to improve security; finding a reasonable balance to accommodate legitimate needs while guarding security is essential.

There is also the free-rider issue. In some cases, the ultimate benefits to an investment in security may not directly accrue to the party making the initial investment. Stated differently, some people have argued that participants in the payment system may rely on investment by other parties rather than doing so internally. Following this reasoning, a given firm may count on others in the industry to make the investment, relying on being able to benefit from the work of others. This reasoning may lead to suboptimal levels of investment overall.

At the same time, many recently publicized data breaches have been occurring outside the financial industry altogether. Conference participants cited incidents at the Veterans Administration, at universities, and at hospitals. Like financial institutions, these entities also have benefited greatly from the ability to access and manipulate large amounts of consumer information, and they too have an interest in maintaining the flow of information. Yet, to the extent that actual losses occur as a consequence of data breaches at these institutions, banks themselves may ultimately bear much of the cost.

There are ways to confront these challenges. Conference participants suggested that one way to modify the incentive equation for nonbanks would be a mandate that consumers be informed about every breach, regardless of scale, scope, or the potential for damage. While such a scheme may not be practical, it would clearly serve as a powerful incentive for all involved in the storage or transmission of sensitive consumer data to actively work to prevent breaches.

Echoing Swindle's comments that data security is good business, conference participants observed that there are also intrinsic reasons for companies to invest in data security technologies and practices. Besides the insurance value provided by enhanced security infrastructure, such tools can be leveraged for other business purposes. For instance, Brian Triplett, from VISA USA, suggested that the same mechanisms used for real-time authentication of a cardholder could be adapted to allow for more secure real-time reward programs at the point of sale.

Consumers also have a role to play, but they, too, face mixed incentives. The substantial consumer protection rights afforded by Reg E and Reg Z, plus those of the networks that limit liability for fraudulent payment card use, caused some conference participants to suggest that these safeguards may serve to dissuade consumers from doing their part.[23] This misalignment is significant, since, ultimately, consumers, who do not generally bear the direct costs of fraudulent transac-

[23] For a more detailed discussion of the problem of incentives in the adoption of best practices in the payments industry, see Mark Furletti, "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Policy Considerations," October 2005.

tions, are in the driver's seat with respect to adopting more secure payment methods. However, in the end, consumers do pay in the form of higher prices that merchants and banks pass on to their customers.

Consumers could contribute to the fight against fraud in a number of ways, with benefits to themselves and to the payments industry. For instance, the Javelin study indicated that consumers who monitored their financial accounts online discovered fraudulent activities in 22 days, with total fraud losses averaging $3,806, compared to 67 days and losses of $6,383, for those who did not manage their accounts this way.[24] Regardless of whether fraud is a result of an actual data breach or due to simple card theft, consumer vigilance and involvement are important. Clearly, it is worthwhile to encourage the use of existing and emerging technological solutions that help to control fraud at the same time that they provide additional benefit to the consumer.

How might consumers respond if asked to play a more prominent role? Evidence regarding consumer preferences and attitudes toward potentially more intrusive security mechanisms is generally inconclusive. Some industry participants report success: Stacie E. McGinn described how Bank of America introduced a "site key" program to better authenticate users for online banking. According to McGinn, consumers regarded this positively, and such innovations in security measures are likely to influence customers' banking choices.

But industry participants foresee asymmetry in consumer attitudes between threats to banking and debit products and those to credit. Conference participants indicated that consumers are willing to use PINs and other technologies to safeguard their demand deposit accounts because doing so protects "their" money. In contrast, they may be less likely to submit to additional conditions on the use of credit cards because these products do not present an immediate threat to their own funds and because issuer and association policies, in addition to the provisions of Reg Z, mean that consumer liability is limited.

Conference participants agreed that the payments industry will need to devise ways to entice consumers to buy into data protection programs. The most robust fraud detection systems and data security programs can be rendered ineffective if carelessness and human error are not controlled. Education and creation of appropriate incentives, along with implementation of less intrusive technologies, will be a starting point.

X. Preventing Breaches

Ultimately, a concerted effort by all stakeholders will be necessary to contend with the threats to the industry. Michael Eubanks, of the Federal Bureau of Investigation, warned that we are past the era of the "hobbyist" hacker. Threats are expanding and becoming more sophisticated as hackers move offshore and become professional. In fact, some criminals know as much about the U.S. banking industry as do knowledgeable insiders, presenting a formidable challenge to even the most well-designed policies. In some respects, fraud management is a game of catch-up.

To address this threat, it may not be possible to outsmart the criminals; rather, organizations can and should work to contain and mitigate the damage that fraudsters might achieve. To do so, implementing a commonsense security program is the first step. An effective data security program starts with a rigorous internal audit of systems and practices.

Joel Winston outlined a commonsense framework for structuring this process: The organization should seek to catalog what information is collected; where it is; whether it is needed; who is accessing it; and whether third parties see it. In general, a guiding principle is to not store data that aren't needed. At the same time, the organization must know who has access to data and be able to justify why they have such access. Finally, firms can benefit from implementing a system to generate an audit trail for sensitive information, allowing personnel to track when data were accessed and by whom.

In addition to reviewing internal data security policies and procedures, Alberto Soliño, from Core Security Technologies, outlined how technological solutions can be applied to gauge and enhance a firm's preparedness for malicious attacks from the outside. Soliño detailed two mechanisms — vulnerability scanning and penetration testing — that can be used to complement a robust information security audit. He explained that vulnerability scans are not intended

[24] This is a disturbing statistic in light of the fact that some reports suggest that consumers may be reluctant to use online banking services because of fears about identity breaches.

to penetrate safeguards or exploit holes but rather are used to detect evidence of vulnerable software, inadequate security patches, or misconfigurations of software. Penetration testing typically follows the scan, during which data security experts will attempt to compromise security using the same advanced tactics as an attacker to evaluate how easily systems are compromised and how much a criminal could exploit in the event security is compromised.

Together, systematizing practices, conducting an audit of internal data-handling procedures and safeguards, implementing an audit trail, and conducting rigorous vulnerability scans and penetration testing can provide a solid foundation for deterring attackers and limiting the damage from data breaches.

XI. Making the Data Useless to Criminals

Going further, Brian Triplett emphasized that the most effective way to control the damage from a breach if it does occur is to "make the data useless" — that is, have infrastructure in place such that even if data are compromised, they cannot be used to access cardholder accounts. To do so, all in the payments industry, Triplett suggested, should look for ways to make transaction-level data dynamic or unique and to encrypt data at the point of sale. This is a more sophisticated approach than merely "replacing a static method with another static method." The approach should allow for flexibility over time and can limit exposure to a single point of failure. If a static method is compromised, all data could be at risk.

In his forward-looking view, Triplett added that any new solutions should minimize the impact to the payment system and be quickly deployable. They should be designed to be minimally intrusive to the consumer while supporting other business drivers as much as possible. Solutions should look to the future and be extensible so that they can accommodate changes in authentication technology or procedures. Above all, new solutions should be aligned with the industry to ensure broad buy-in and they should be globally interoperable in order to maintain the integration of payments internationally.

In general, authorization decisions should be based on more than just card and account data. There should be a mechanism for asking the consumer for more information if a fraudulent transaction is suspected. Addressing the market challenges, Triplett suggested that by targeting high-risk transactions, merchants can avoid adding time or complexity to ordinary transactions by legitimate consumers, thereby minimizing the impact on customers' experience and throughput at checkout.

Additionally, organizations that process payment card transactions should work toward achieving full PCI compliance. Michael Cunningham, from Chase Cardmember Services, explained that the Payment Card Industry (PCI) Data Security Standard is a collaborative effort of the major card networks and issuers to safeguard customer information. Visa, MasterCard, American Express, Discover, and JCB mandate that merchants and service providers meet certain minimum standards of security when they store, process, and transmit cardholder data.[25]

Thus far, the PCI standard has had mixed success. Most observers and industry participants at the conference argued that it is a well-designed, rigorous standard. In fact, Cunningham asserted that there has never been a security breach at a genuinely PCI-compliant merchant. Unfortunately, this standard has yet to be universally accepted, thus limiting its effectiveness. For instance, Visa reports that only 22 percent of its largest merchants were PCI-compliant as of early 2006.[26] This may be the case for a number of reasons — and those same reasons apply to other security-oriented initiatives in the payments arena as well.

Paul Tomasofsky, of Two Sparrows Consulting, ventured that PCI's incomplete adoption may in part be due to the fact that some merchants see PCI as another "card" mandate. In other words, they look upon these recommendations as regulations promulgated from outside the merchant community by organizations that aren't themselves immersed in the complexities and challenges of the retail industry. He further suggested that for many, implementing the PCI stan-

[25] The PCI standard mandates a number of data security practices. For instance, it requires SSL encryption of databases that store or process data, two-factor authentication at POS terminals, a log of all access to credit card data, and a well-implemented firewall. It also prescribes network intrusion testing and annual or quarterly penetration testing conducted by an approved external vendor. More details can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf or at https://sdp.mastercardintl.com/pdf/pcd_manual.pdf.

[26] *Cards International*, "PCI council set up by global payment networks," September 30, 2006.

dards may not be perceived as a profitable undertaking — requiring investment in technology and education — and for smaller merchants, perhaps beyond their capabilities.

On the other hand, Tom Arnold argued, the networks, acquirers, and issuers on the supply side of the payments industry who are promoting the initiative have not done enough to communicate the benefits and means to achieve compliance to processors and merchants. Furthermore, participants suggested that without punitive sanctions and the prospect of fines for noncompliance, market incentives alone may not be sufficient to motivate the holdouts. Yet, Arnold noted, unilateral sanctions imposed by the issuing and acquiring banks and card networks may have unintended consequences. For instance, given the competitive merchant-acquiring landscape, a merchant facing earnest demands to make serious improvements to its information security could sidestep penalties by moving to a new acquiring bank.[27]

Tomasofsky also observed that a number of factors make implementing PCI and more rigorous security practices generally more difficult. Doing so requires the involvement of a firm's key management and the participation of staff from many levels. Turnover and costs of implementation make this tough. Compounding the challenge is the fact that some firms see the secure coding guidelines as vague, and documentation requirements are a hurdle for many firms not accustomed to this sort of discipline. However, with vendor-based solutions emerging, and the recognition that PCI compliance can produce very salient benefits, especially for merchants with less established brands, enthusiasm has been mounting.

Ronald Congemi, from First Data, noted that key differences between the orientations of merchants and financial institutions can account for a different level of commitment to security investments. For banks and other payments providers, money and customer information is effectively their main product; as Orson Swindle remarked, they have "grown up" being good at protecting it. Moreover, despite large differences in size and scope, banks tend to be more homogeneous and far fewer in number than the disparate mix of retailers and processors that plug into the other end of the payment system.

Congemi called for increased involvement from federal entities, particularly the FTC, in order to overcome the coordination challenges. He argued that this body is well suited to encourage national retailing federations and other nonbanks to sit down with banking organizations such as the ABA to work together to find solutions.

Coordination among the various stakeholders is critically important, a goal made more difficult by the fact that they do not always share the same priorities. As Orson Swindle recommended, everyone who touches the data should be taking steps to protect it. Yet, this is made more complicated because banks, which maintain the direct customer relationship, may not know everyone who touches customers' data, posing a significant coordination problem.[28] Brian Triplett spoke for many when he declared that "we're all in this together." Therefore, intelligent and effective solutions must include input from issuers, networks, retailers, government, and consumers, as well as their active participation. A top-down solution imposed by the banking industry or an approach adopted by a subset of parties will not work.

The recent announcement of the PCI Security Standards Council and the release of version 1.1[29] of the PCI Data Security Standard reflect the industry's acknowledgment of this need for broad-based involvement. The council's goal is to accelerate the adoption of the PCI standard, employing several approaches.[30] First, the council intends to streamline the process of attaining compliance and to increase lead times for adopting and implementing the standard. Second, the council will create a consortium of technology providers and consultants who will be available to assist companies in meeting the standards while providing training and certification opportunities. Finally, the council intends to seek input from the diverse stakeholders in the payments industry, inviting companies that partici-

[27] Arnold suggested several strategies that might be effective in addressing this challenge. First, merchant acquiring banks could be required to demonstrate that they have a program in place to bring their merchants into compliance with the standard. Second, they could be required to provide audited counts of the number of merchants that are registered and PCI-certified. Finally, they could be prohibited from signing up new merchants who have been the subject of a security compromise and who have not yet demonstrated their compliance with the PCI standards.

[28] Lee Manfred warned that there are between 25,000 and 50,000 entities in the U.S. that may touch cardholder data.

[29] This standard is available for download at https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm.

[30] http://corporate.visa.com/md/nr/press297.jsp.

pate in the initiative to comment on changes to rules, as well as soliciting their input on the selection of the PCI Security Standards Council's board of advisors.

XII. If a Breach Occurs

Even with the best procedures and safeguards in place, breaches can still happen. What are the responsibilities of payments participants in the event of a breach? What should be disclosed after a breach, when, and by whom?

Susanna Montezemolo, of Consumers' Union, addressed the needs of consumers for information in the event that their private information has been compromised. She noted that today's notifications are often unnecessarily complicated and effectively "written by lawyers, for lawyers." Instead, she urged that notifications be simple and written for the layperson; they should say exactly what information was compromised; and they should explain how consumers can take advantage of their rights under state and federal law for protection against misuse of the data.

Montezemolo argued that notification should come from the entity with which consumers have a financial relationship, such as the card-issuing bank, even if the breach occurred elsewhere in the processing chain.[31] Citing the CardSystems case, she observed that notifications from unfamiliar entities often do not attract the consumer's attention. Others suggested that having the firm responsible for the breach provide notification may not be practical. As Kathy Kauffman, from Capital One, observed, many merchants and processors simply do not have address information for all of their end customers. A related notification problem is that unless notification responsibilities are clear, a consumer could get multiple notification letters from downstream firms, likely with inconsistent details. When this happens, customers could be confused and not realize that multiple notices pertain to a single incident. These various complications led conference participants to argue for a consistent disclosure protocol, understood by all payment stakeholders and by consumers.

After a breach has occurred and consumers have been notified, Montezemolo suggested several strategies that consumers might employ to protect themselves from being victims of identity theft or fraud. First, she argued that consumers should place a fraud alert on their credit file. Fraud alerts are a provision of the FACT Act that require lenders who obtain credit reports from the three credit bureaus to take additional steps to verify the consumer's identity before making a loan or extending credit. An initial fraud alert will be in place on a person's credit report for 90 days. It can be instituted whenever a consumer suspects he or she has been or could be a victim of identity theft. "Proven victims"[32] of identity theft may also opt for an extended alert, which will remain on the credit report for up to seven years.

The FACT Act also entitles consumers to a free credit report every 12 months from each of the three nationwide consumer reporting agencies. These credit reports can be used to monitor credit-related activity. Alternatively, consumers could engage a for-fee credit monitoring service. However, Montezemolo suggested that self-monitoring may be as effective and less expensive.[33]

A more potent tool, allowed by some, but not all, states, is to enact a "security freeze" on the account. Montezemolo indicated that 20 states currently offer no-fault policies by which anyone — regardless of whether they have been victimized — can freeze their credit file. Five states restrict this right to identity theft victims only. Once enacted, security freezes effectively block lenders from accessing the credit report. Fees for these services vary across states: They range from free to $20 to place a freeze and from free to around $10 to lift one. It is generally free to victims of identity theft and sometimes for other special classes (such as the military and the elderly).

Montezemolo argued that, of the two tools, fraud alerts are of less benefit because they put sig-

[31] Montezemolo suggested that in such cases, even if the notification is sent out under the aegis of the financial institution, it would be reasonable for the responsible party to pay for the cost of telling consumers about the breach.

[32] A consumer can achieve this by filing an identity theft report with the FTC and other relevant parties. This process typically has two phases: the first is a report submitted to a local, state, or federal law enforcement agency that details facts such as the dates of the identity theft, the fraudulent accounts opened, the suspected perpetrator, and so forth. The second is typically used in conjunction with the law enforcement report by the credit reporting agency to conduct its own internal investigation. See http://www.consumer.gov/idtheft/.

[33] Indeed, various forms of account and credit self-monitoring appear to generate better results. In its analysis of the consequences of identity theft, Javelin reported that consumers uncover 47 percent of identity fraud cases by examining their financial statements. Doing so results in faster detection and lower costs, both to them and to financial institutions.

nificant onus on the individual and will do little to prevent illicit use of the data. Security freezes, on the other hand, are much more effective — especially for those who have not yet been a victim of fraud. However, they obviously serve as a substantial obstacle to legitimate credit inquiries and can even present problems when consumers apply for jobs or insurance coverage. Montezemolo suggested that one potential means for overcoming this obstacle would be to restrict access to credit reports through the use of PINs. While this strategy would introduce its own concerns about implementation, it would help to preserve much of the convenience of instant credit approvals.

Evidence suggests that consumers' response to security freezes has thus far been limited. Stuart Pratt reports that perhaps 9,000 people in California to date have taken advantage of this sort of protection. Since California has been a leader in making this remedy available, the limited interest in that state is notable. However, it is not clear why more consumers have not responded; some conference attendees suggested that consumers might feel that the remedy is not effective for their particular situation or they may not realize it is available to them or understand how it can be implemented.

XIII. Creating Effective Disclosures

Montezemolo's presentation highlighted the challenges inherent in designing effective data breach notifications that respond effectively to the needs of the different stakeholders in the payment system. Traditionally, state and federal government entities have had a role to play in resolving some of the conflicting points of view in this area. However, conference participants noted that the laws governing these issues are still being developed and show a great deal of diversity. Indeed, 23 states have currently enacted some sort of legislation related to security breach notifications, and another 16 have legislation in process.[34]

Luckily, many of these state laws and proposals generally cover similar themes, and conference participants touched on several areas relevant to effective notification about security breaches. First, what type of data should be subject to breach legislation? For instance, Social Security numbers are typically included, but they alone are often not sufficient in enabling fraud; other data must be included as well. Second, who is responsible for making the notification? Here, much new state legislation resembles the California standard; that is, the notification should be sent by any firm conducting business in the state that believes that personal identifying information under its control has been acquired by an unauthorized person. Another issue to be resolved is whether a breach that involves only encrypted data warrants the same sort of notification as one where unencrypted data are compromised.

Third, how will individuals be notified: in writing, electronically, by phone, or in another manner? Must they be notified if there is no likelihood of reasonable harm arising due to the breach?[35] Finally, how soon must notification take place? The California law calls for the "most expedient time possible and without unreasonable delay." Other states specify a 45-day window.[36]

It appears that a consensus is arising that these points should be addressed generally in legislation dealing with breach notifications. Yet, as Stuart Pratt noted, many existing state laws still suffer from ambiguities and are not consistent across the country, especially in terms of the details related to implementation. Pratt explained that staying abreast of the developments and complying with disparate standards are seen to be considerable challenges for payments providers operating in multiple states. In response, some have called for some type of federal standard to improve consistency and ease compliance.

Others have suggested that a national firm could circumvent the problem presented by the panoply of state laws by seeking to comply with the strictest state law on the books. Leaving aside the policy question — that some states would effectively be setting a federal standard — this may not even be practical. While a given state's law may indeed be the strictest

[34] VigilantMinds, Inc., "State Security Breach Legislation," February 2006.

[35] The Ponemon-White & Case survey indicates that 82 percent of people think it is always necessary to report a breach "even if the lost or stolen data was encrypted, or there was no criminal intent."

[36] Irrespective of how and when the law comes to pass, consumers have indicated the importance they ascribe to effective notification about breaches. The Ponemon-White & Case survey suggested that the quality of the notification and the manner in which it is delivered are crucial if an organization wants to protect its reputation and maintain customers' trust in the event of an actual breach. In fact, the survey results indicated that consumers are four times more likely to close an account if they are not notified in a "clear, consistent, and timely fashion." The survey suggests that telephone calls and personalized letters were three times more effective at preventing customer turnover than electronic correspondence or form letters.

available, it may also have specific provisions that conflict with those of other states.

In recent years, many legislative proposals have come through Congress; Pratt cited five or six that remain active. Of those, two bills offer the promise of a standardized approach to notification language and procedures. One, championed by Senator Arlen Specter, emerged from the Senate Judiciary Committee. Bill S1332 is entitled the Personal Data Privacy and Security Act.[37] The second, HR4127,[38] entitled the Data Accountability and Trust Act, has emerged from the House of Representatives, and it shares many characteristics with the Senate version.[39]

However, more work remains to be done. According to Pratt, the major federal legislation is encumbered with language that addresses issues outside the core problem of data breaches. He also noted that conflicting jurisdictions and the interplay between various congressional committees complicates the legislative process further. Additionally, Pratt observed that the principal federal legislative proposals leave important issues about implementation unresolved, don't define what constitutes a "trigger event," and do not specify how a firm should determine if a breach would be likely to pose a "significant risk" of identity theft. These questions and other remaining differences in legislation may need to be resolved before the resulting framework is effective, intelligible, and viable for organizations that act nationally and internationally.

XIV. Next Steps

Consistent regulation is just one of the challenges in this area that may benefit from the involvement of an impartial entity with national reach. Some conference participants suggested that the Federal Reserve might be able to play an instrumental role as well in several areas. First, it can leverage its relationships with community banks and educators to help communicate the nuances of identity theft to consumers and disseminate information about what can be done to safeguard data.[40] Similarly, the Fed could help to overcome the difficulty in measuring fraud due to disincentives to report, differences in terminology, and the need to coordinate data from a large set of diverse participants.

More broadly, as this recent conference demonstrated, the Federal Reserve is able to convene the "right people at the right time." Paul Tomasofsky commented that by providing a neutral meeting place and motivating discussion, the Federal Reserve and other responsible entities can spur the sort of cross-industry dialog and cooperation that will be needed to fashion credible responses to this problem. Moreover, to the extent that there is a role for regulatory oversight or guidance, the Fed can help to inform policymakers throughout the bank regulatory community.

Third, as Orson Swindle noted, government agencies, including the Federal Reserve, are in the best position to serve as advocates on the international stage. While some payments participants, such as the major card networks, do have a large international presence, even they do not enjoy sufficient leverage to bring together all the parties, including law enforcement and banking regulators, necessary to devise the interoperable solutions needed to confront fraudsters that operate globally.

Finally, the Federal Reserve, in particular, is well placed to lead by example. Bruce Summers highlighted areas where the Fed has taken the lead in building robust and secure systems and practices. Given the Federal Reserve's critical role in the payments infrastructure, these procedures must stand up to the most exacting scrutiny. They may serve as a model for other financial institutions and payments participants.

XV. Conclusion

Over the course of the two days, attendees agreed that data breaches and other security threats are a real, insidious, and growing problem. While the situation is not yet dire, it is serious enough to warrant earnest attention from the many parties that interact with the payment system. However, responses should

[37] This bill has been placed on the calendar of business but has not been scheduled for a vote. It can be viewed in its entirety at: http://www.govtrack.us/data/us/bills.text/109/s/s1332.pdf.

[38] http://www.govtrack.us/data/us/bills.text/109/h/h4127.pdf.

[39] Arguably, business favors the House bill. The bill offers full preemption of state laws about data breaches, as opposed to merely preempting laws related to a consumer's right to modify incorrect credit report information. Additionally, the House version does not require a breach to be reported if there is no "reasonable basis to conclude that there is a significant risk of identity theft." A more detailed analysis of the differences between these legislative proposals and other related bills is available from Consumers Union: http://www.consumersunion.org/pdf/fed_security109.pdf.

[40] As Ron Congemi observed, the Federal Reserve has a long-standing tradition of financial education.

be carefully considered and reflect the fact that there is not one single problem and there is not one single solution. A sentiment echoed several times during the conference is that industry participants really are confronting two problems — actual fraud and consumer perceptions of fraud — that call for distinctly different solutions. It is important to respond to both the actual threat and the legitimate concerns of consumers while helping to inform the public.

Fortunately, many useful tools are already available to respond to actual threats to payments-related data. Technology, investment, education, cooperation, and a standard for best practices are a start. In general, it makes sense to do the simple things first while looking to the future to ensure that quick fixes are not easily thwarted by increasingly sophisticated professional criminals. At the same time, as Alberto Soliño urged, organizations should assume that they will be subject to a breach and plan accordingly. It is too late to put appropriate responses in place after a breach has occurred.

Besides addressing the external threats and internal vulnerabilities, organizations must be prepared to be proactive in interactions with policymakers, consumers, and the media. Good security practices and investments, while costly, can and should be regarded as assets. Judiciously communicating the benefits of these tools to customers is a good way to unlock the value of such investment. After that, education is the next step, in particular, education focused on the different types of fraud associated with data breaches, including identity theft, and the risks associated with each. Additionally, creating an effective and standardized disclosure system and establishing relationships with different constituencies remain important.

These measures are all directed to ensuring that information keeps flowing. As Orson Swindle and other participants emphasized throughout the conference, the very business of payments is built around the efficient transmission and use of information. Security breaches, especially ones that are highly publicized and often misunderstood by consumers and the media, do much to imperil this dynamic. Adequately responding to data breaches and other security threats is costly, but not doing so will be more costly — in terms of both the financial costs today and the opportunity cost of lost business in the future. Organizations unwilling to make the necessary investments today may not enjoy an opportunity to do so in the future.

Exhibit 1:
Conference Agenda

Wednesday, September 13, 2006

Welcome and Introductory Remarks
Peter P. Burns, Federal Reserve Bank of Philadelphia
H. Kurt Helwig, Electronic Funds Transfer Association
Charles I. Plosser, President, Federal Reserve Bank of Philadelphia

"Fiduciary Responsibilities in the Era of Electronic Banking: A Central Banker's Perspective"
Keynote Address: Bruce J. Summers, Director, Federal Reserve Information Technology

Baseline Issues for Payments Participants: Setting the Stage
Moderator: Lee Manfred, First Annapolis Consulting
Panelists: Tom Arnold, PSC Payments and Security Experts
Daniel Buttafogo, Barclaycard US
Avivah Litan, Gartner Inc.
Russell W. Schrader, Visa USA
Gray Taylor, National Association of Convenience Stores

Thursday, September 14, 2006

"Information Security: The Sky Is Not Falling — But It Could"
Keynote Address: Orson Swindle, Senior Policy Advisor and Chair, Center for Information Policy Leadership, Hunton & Williams

Ensuring Data Security
Moderator: Alberto Soliño, Core Security Technologies
Panelists: Ronald V. Congemi, First Data
Michael Eubanks, Federal Bureau of Investigation

After a Breach: Protecting Customers and Consumers
Moderator: Michael Cunningham, Chase Cardmember Services
Panelists: Kathy Kauffman, Capital One
Susanna Montezemolo, Consumers Union

Legal and Regulatory Perspectives
Moderator: Lynne B. Barr, Goodwin Procter LLP
Panelists: Stacie E. McGinn, Bank of America
Stuart K. Pratt, Consumer Data Industry Association
Joel Winston, Federal Trade Commission

Exhibit 2:
Institutions Represented at the Conference

American Express Company
Avenue B Consulting, Inc.
Bank of America
Barclaycard US
Capital One
Chaddsford Planning Associates
Chase Cardmember Services
CheckFree Corporation
Consumer Data Industry Association
Consumers Union
Core Security Technologies
Discover Financial Services
eFunds
Electronic Funds Transfer Association
ePayments
Federal Bureau of Investigation
Federal Reserve Bank of Boston
Federal Reserve Bank of Kansas City
Federal Reserve Bank of Philadelphia
Federal Reserve Bank of Richmond
Federal Reserve Board of Governors
Federal Trade Commission
Fidelity National Information Systems
First Annapolis Consulting
First Data Corporation
First Data Debit Services
Fiserv EFT
Gartner Research
Goodwin Procter LLP
Hunton & Williams, LLP
JP Morgan Chase & Co.
MasterCard International
Metavante Corporation
Morrison & Foerster, LLP
National Association of Convenience Stores
Opus Financials
Palm Desert National Bank
PSC
The Kroger Company
TransUnion
Two Sparrows Consulting
Visa USA
Wachovia Bank, N.A.

Ten Independence Mall
Philadelphia, PA 19106-1574
215-574-7110
215-574-7101 (fax)
www.philadelphiafed.org/pcc

Peter Burns
Vice President and Director

Stan Sienkiewicz
Manager

The Payment Cards Center was established to serve as a source of knowledge and expertise on consumer credit and payments; this includes credit cards, debit cards, smart cards, and similar payment vehicles. Consumers' and businesses' evolving use of electronic payments to effect transactions in the economy has potential implications for the structure of the financial system, for the way that monetary policy affects the economy, and for the efficiency of the payments system.