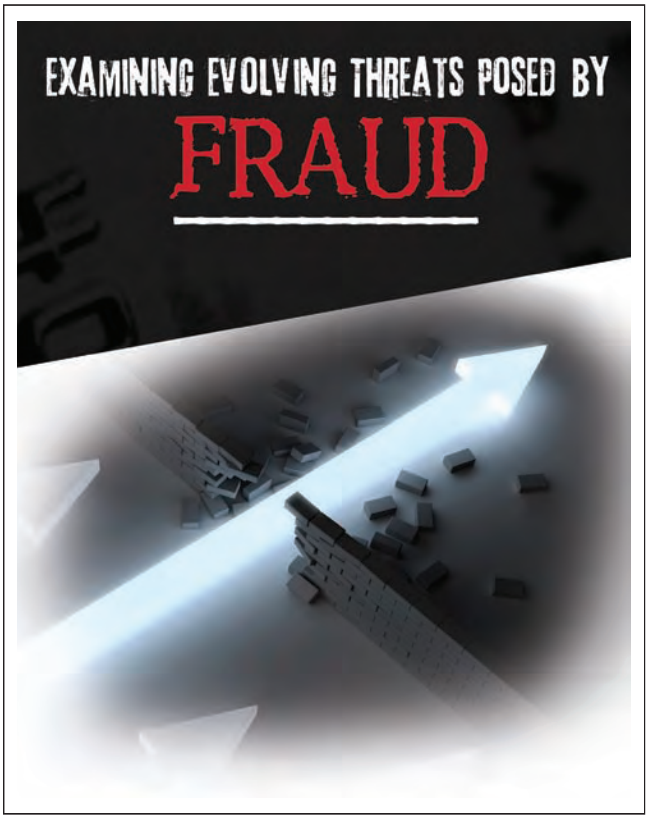
CONFERENCE SUMMARY



# Maintaining a Safe Environment for Payment Cards:

## Examining Evolving Threats Posed by Fraud

April 23 - 24, 2008

PAYMENT CARDS Center
FEDERAL RESERVE BANK OF PHILADELPHIA

efta Electronic Funds Transfer Association

CONFERENCE SUMMARY

# Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud

Susan Herbst-Murphy

## Summary

On April 23 and 24, 2008, the Payment Cards Center of the Federal Reserve Bank of Philadelphia and the Electronic Funds Transfer Association jointly hosted "Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud." The conference included panels representing four key constituencies: issuers, consumers, merchants/acquirers, and networks. The panelists addressed the nature of payment card fraud in the 21st century. This paper summarizes the highlights from the presentations and the discussions that ensued.

*The views expressed here do not necessarily represent the views of the Federal Reserve Bank of Philadelphia or the Federal Reserve System.*

# TABLE OF CONTENTS

## I. Introduction

On April 23 and 24, 2008, nearly 100 interested parties and experts on the topic of payment card fraud convened at the Philadelphia Federal Reserve Bank to attend a conference sponsored by the Payment Cards Center and the Electronic Funds Transfer Association (EFTA). The conference, "Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud," was designed both to continue discussion of topics that emerged from a September 2006 conference on data breaches and to identify new trends and developments that had materialized in the interval. From the discussions during the day-and-a-half conference, the following key themes emerged:

- **Reconsideration of Chip-Card Technology.** The mantra of the past two decades has been that smart cards are "a solution in search of a problem." From opinions voiced at this conference, there may be recognition that the problem to be solved by chip cards has presented itself in the form of mitigating fraud. As more of the world becomes chip-card enabled, fraud has migrated to areas with magnetic-stripe technology or to venues such as the Internet, where physical card presence isn't required. Additionally, the bifurcation of mag-stripe technology in the U.S. and chip cards in other parts of the world poses challenges to global interoperability within the card payment system. While the challenges and limitations of chip cards were noted (infrastructure cost, irrelevant in current card-not-present environments), several panelists and conferees indicated (some even expressed it as "inevitable") that the U.S. may adopt chip technology in the future.

- **Adoption of Payment Card Industry Data Security Standards (PCI-DSS).** After a slow start, merchants have accelerated their compliance with PCI-DSS (more commonly referred to simply as PCI) requirements promulgated by the major credit and debit card networks. However, PCI compliance is not a "one and done" solution, but rather an ongoing process requiring continual vigilance.

- **Sophisticated Fraud Rings Employing Advanced Technology.** The fraudsters of today are organized professionals using much of the same technology employed by legitimate industry. Fraudsters employ variations of models used in the legitimate business world to conduct their activity: databases that mirror credit bureaus; creation of value-added information by matching and appending data elements, similar to what legitimate data aggregators do, but using compromised records; and the sale of information, even using time-sharing techniques such as those employed by lawful enterprises to provide illicit access to data. Sophisticated fraud rings operate in an illegal "parallel universe" to the payments industry, using many of its tools and techniques.

- **Fraud Is Dynamic, Seeks Path of Least Resistance.** Fraud mitigation is often, by definition, reactive as criminals learn to avoid better secured access points and instead target weaker products, channels, and geographies. Recognizing that thieves maneuver across products and channels to perpetrate fraud and that multiservice households expect to be protected against fraud across the entire relationship, full-service financial institutions (FIs) are transforming their fraud management structure to traverse product, channel, and platform silos within their organizations.

- **Growth, Complexity, and Need for Greater Cooperation and Coordination to Achieve Solutions.** Payment card usage has become more universal and more complex. E-commerce and electronic banking have spawned a proliferation of end-points. Greater electronification of information makes the capturing of information vulnerable while the information is "in transit" or "at rest." Increased complexity also means that there is no "magic bullet" that will ameliorate the problem. Mitigating fraud entails multivariate solutions requiring the cooperation and collaboration of all players within the payments chain but recognizes that theft of confidential information occurs from repositories that are outside the financial services domain (e.g., hospitals, colleges, and government entities).

- **Consumers' Role in Mitigating Fraud.** Identity theft and retailer data breaches have been highly publicized in the popular press in recent years, raising awareness among the general public about the risks that can affect individuals. Consumers indicate that they want to be involved in securing their information, but they don't always act in their own best interests (e.g., responding to phishing attacks by providing their personal information). Networks, acquirers, and card issuers are interested in having consumers involved in fraud-prevention strategies, but zero liability protections and other factors pose challenges to achieving this goal. Ideas proposed to better engage consumers in fraud mitigation efforts included education campaigns, interactive communication, and incentives.

## II. Conference Background

The Payment Cards Center and the EFTA co-sponsored a fraud-related conference ("Information Security, Data Breaches, and Protecting Cardholder Information: Facing up to the Challenges") in September 2006. In joining forces for the 2008 conference, the organizers wanted to extend the earlier discussions, going beyond the specific issue of data breaches to deal more directly with fraud-mitigation strategies and challenges. The conference structure was designed to reflect and examine new developments in payment card fraud and industry responses. Recognizing the interdependencies involved, the co-sponsors organized the discussions around the particular perspectives of payment system participants: card issuers, consumers, acquirers and merchants, and the enabling payment networks. (The conference agenda can be found in Appendix I.)

## III. Conference Day One

### Keynote Address

Jon Greenlee, Associate Director, Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation

The conference began on Wednesday afternoon with welcome and introductory remarks by Peter Burns of the Payment Cards Center and H. Kurt Helwig of the EFTA. Michael Collins, an executive vice president at the Federal Reserve Bank of Philadelphia and head of its Supervision, Regulation and Credit Department, introduced the keynote speaker, Jon Greenlee, whose address was titled "Regulatory Perspectives on Payment Card Fraud." Greenlee described how the Federal Reserve and other bank regulators have increased their attention to fraud and operational risk issues in retail payment systems. While large dollar wholesale payment systems have historically been the focus of policymakers concerned about systemic risk, the growing size and scope of retail payment systems have not gone unrecognized. He cited this conference and similar discussions at other Reserve Banks and the Board of Governors as evidence of this growing recognition.

At the heart of the issue is the critical role of consumer confidence in payment systems, especially as payments move to electronic platforms. To the extent that data breaches and related fraud and identity theft threaten consumer confidence in electronic payments, the system as a whole is threatened.

Greenlee noted that while innovation in payments has resulted in greater consumer convenience and enhanced efficiency, there must be a corollary focus on the risk presented by new products, new providers, and new technologies. Innovations and new technologies create additional complexities and involve a growing legion of third-party participants in the payment industry. Greenlee stated that, as a result, there is more information residing outside of banks' "four walls," and because management of that information (and related risk of compromise) is outside of banks' immediate control, the risk-mitigation challenges for FIs are changing.

At the same time, Greenlee also emphasized the importance of risk fundamentals, including communication across functional areas as new products are developed. In his experience, he has found it critical that risk assessment processes cross functional silos to identify any unanticipated consequences associated with new product or new process rollouts. He closed by encouraging conference participants to continue discussions that include all participants in the payment system in a search for collaborative solutions.

## Setting the Stage

**Moderator:**

***Peter Burns***, Director, Payment Cards Center, Federal Reserve Bank of Philadelphia

**Panelists:**

***James Brown***, Director, Center for Consumer Affairs, School of Continuing Education, University of Wisconsin-Milwaukee

***Avivah Litan***, Vice President and Distinguished Analyst, Gartner, Inc.

***Richard Parry***, Senior Vice President, Consumer Risk Management, JPMorgan Chase

***Paul Tomasofsky***, President, Two Sparrows Consulting

Following Jon Greenlee's opening remarks, Peter Burns introduced the conference's first panel by noting that this session was specifically structured to provide a broad overview of key elements in the dialogue about payment card fraud. The session was titled "Setting the Stage" to emphasize that the topics to be discussed were intended to provide a context for the next day's panels and raise general issues affecting all participants in the payment system.

Richard Parry focused his initial remarks on how the proliferation of consumer banking products (e.g., prepaid cards and check electronification) and channels (e.g., Internet and telephone) has affected the basic profile of fraud risk. He first spoke to the proliferation of remote banking access channels in the U.S., emphasizing the need to better understand the links between fraud and specific channels. For example, he noted that while telephone fraud results in higher dollar losses, the Internet poses special threats because of its potential to lose a lot very quickly. With remote channels, FIs focus on securing the session. What Parry described as the "real vulnerability" lies in the validation of customers' identity at the time they open their accounts. The "know your customer" process depends on forms of identification (driver's license or utility bill) that can be easily doctored. So the "gold standard lock on the door" for securing a remote session can be compromised, said Parry, because it's fairly easy for a crook to obtain the "gold standard key."

Further enabling criminals' ability to impersonate a customer, Parry continued, is "social engineering." Parry described a real-life scenario in which a perpetrator made 57 calls over a series of days to the credit card call center, the online banking department, and other areas of a bank in a continuing attempt to gain information to access and control an individual's accounts. Once armed with the information to "become the customer," the fraudster drew down a home equity line of credit through an Internet banking session. Parry used this example to describe how, within a banking organization, actions contributing to fraud are often segregated from the actual experience of fraud. In this case, the credit card call center did not have a direct organizational line to the loss nor did the Internet banking department. The demand deposit account department was involved, since the money passed through that department on its way to the criminal. But the actual financial loss occurred in the home equity loan department, which had no managerial control over any of the areas that had been exploited by the criminals to achieve their objective.

Parry argued that more holistic efforts to prevent fraud are needed across the entire banking organization. He also cautioned against over-reliance on working groups focused on specific pieces of the fraud problem in achieving solutions. "When we look at it that way, we get fragmented solutions," he said.

Next, Paul Tomasofsky shared his views on how changes in industry structure might affect fraud levels and responses. His comments were broadly speculative and fell into three areas: 1) What effect might changes in network ownership have? 2) How might new merchant strategies affect risk exposure? 3) What are regulators doing, or thinking about doing, regarding these changes?

Tomasofsky observed that there are no bank-owned credit card associations anymore. The electronic funds transfer (EFT) networks over which personal identification number (PIN) debit transactions travel have also largely migrated away from the bank-owned model. While not arguing any particular outcome, Tomasofsky suggested that consideration should be given to whether changes in governance structures might lead to increased vulnerabilities. In short, do networks owned by regulated banking companies provide stronger fraud protection than that coming from networks owned by nonbanks? Extending that thought, he then asked whether a potentially less intensive focus on bank ownership interests might alter card network business strategies in ways that might lead to new fraud vulnerabilities. For example, might networks consider opening card issuing to nonbanks, and if so, how would that affect the system's risk profile? Could merchants self-acquire, and if so, would the absence of an acquiring bank in the payment acceptance chain affect system risk? As players compete with each other outside the association model, what additional risks might be introduced?

Tomasofsky went on to say that merchants are actively looking at alternatives that will lower their costs of accepting payments. As they do so, who is focusing on the risks associated with the introduction of these new schemes and new players, including nonbanks? Expanded use of spontaneous ACH debits, remote draft capture, and alternative payment options may lead to lower merchant costs but may also be introducing new fraud risks into the broader payment system.

Furthermore, Tomasofsky observed that many new payment system players and technologies factor into his final point: regulation. PayPal, for example, has grown appreciably in just eight years and has moved from a focus on Internet auction payments to all varieties of Internet payments. Mobile could be next, and Tomasofsky asked if banks will be the players in mobile payments. If they are not, then the question is, "Who will be watching them?" He raised the concern of global fraud risk. U.S. laws don't apply across borders. What vulnerability may exist in the U.S. as other parts of the world adopt chip and PIN at the point-of-sale (POS)? Will fraudsters target the U.S. because its mag-stripe technology makes it vulnerable? The responsibilities and liabilities will become increasingly more complex, occasionally even blurred. Richard Parry interjected that compromise of data while traveling over telecommunication lines (data in motion) has already occurred in Indonesia, and he raised the question of who is liable in that event.

Avivah Litan began her remarks by agreeing with Parry's earlier comments about credentialing, noting that she believes that is one of the two most significant areas of weakness in mitigating the risk of fraud. The other area, she argued, is the migratory aspect of fraud: It moves across organizations, channels, and products. Crooks move from phone to retailers to ATMs. The outlook is challenging. Criminals keep devising new attack methods, using all kinds of sophisticated techniques. Many of the most accomplished criminals come out of eastern European countries and other areas remote from the U.S., where they operate with relative immunity.

Emphasizing the sophistication of today's payment card fraudsters, Litan suggested that illicit operations provide the criminal community with services that mirror legitimate business models. There are Internet sites run by criminal gangs that provide access to stolen confidential information for a finite period of time for a set fee. Litan cited an example where criminals have established a database time-sharing operation, set up on servers in Panama, allowing potential fraudsters to have access to stolen personal information for a defined amount of time, paying a fee for the time-share.

Litan described how criminals exploit other legitimate practices, such as online advertising, in their efforts to steal consumer information. Online users click on what appears to be a legitimate ad. The click activates the download of malware to their PCs, stealing keystrokes, credentials (both graphics and text), and even security certificates stored on PCs.

Litan closed with two points that would be echoed throughout the conference:

1. Now that retailers are storing fewer data, the crooks are more frequently hacking data in motion. As one door is closed to them, fraudsters open another.
2. Litan does not think that publicized retailer data breaches have materially affected consumers' shopping behavior or their use of payment cards. She noted that after the much-publicized breach at TJ Maxx stores (TJX), the retailer reported increased revenue and growth in same-store sales. As part of its post-breach efforts to encourage consumers to return to their stores, TJX held a "discount day." Customers not only returned, Litan reported, but paid for their discounted purchases with their cards. There is no evidence that card use is declining in the face of breaches and reported fraud schemes. In Litan's view, this suggests that consumers feel confident that if their cards are used fraudulently, their banks will absorb the financial loss for them.

James Brown picked up from there by sharing what he refers to as "Brown's Law #1": "The customer always pays; it's just a question of who gets to break the news." The cost of fraud does make its way back to the consumer, but consumers do not act on a cost experienced collectively in the same way as one experienced individually and directly. Because of the "political calculus," Brown does not anticipate changes that would place more liability on consumers. Consumers vote; therefore, consumer protection mandates that have been built into the law institutionalize liability. Holding customers liable is not good politics. Therefore, Brown proposed that positive incentives to reward consumers for behavior that helps to mitigate fraud might have merit.

During the discussion that followed the opening panelists' remarks, a number of comments focused on the need to recognize the many interdependencies inherent in today's electronic payment environment. The discussion highlighted the complex nature of the challenge and made it clear that effective solutions need to include all parties: consumers, issuers, networks, and merchants/acquirers.

## IV. Conference Day Two

### Welcoming Remarks

Charles Plosser, President, Federal Reserve Bank of Philadelphia

Charles Plosser's opening remarks on the second day of the conference focused on the evolving threat of fraud and the importance of cooperation and collaboration among the various segments of the payment card industry in the search for solutions.

Plosser spoke to the increasingly complex security challenges that exist in today's high-technology and electronic-data-intensive card payment system. While noting that electronic payment systems enable efficiency and welfare-enhancing outcomes, he also noted that they expose data to theft "in quantities that would not have been available in previous eras." The perpetrators are well-organized, professional, and well-funded criminal groups, operating domestically and internationally and using advanced technology in their efforts. As Federal Reserve analyses have affirmed, the transformation from paper to electronic payments is continuing apace, creating new challenges and responsibilities for payment system participants. Plosser emphasized that consumer confidence in the payment system is a critical concern, obliging all who touch sensitive information to ensure its safety.

Achieving this, Plosser continued, will require the cooperation of otherwise competitive market participants, in cooperation with law enforcement and data security experts. He recognized that the industry's success in reducing fraud rates has been due in large measure to just such collaboration. He urged continued cooperation, recognizing that "the card payment system's integrity relies upon a set of interdependencies and a shared responsibility," and he warned that the system's divergent constituencies cannot win the battle by operating independently.

Reflecting on the structure of this conference, Plosser noted that an important function of the Bank's Payment Cards Center since its inception has been to create opportunities to bring differing perspectives together in a search for common solutions. "It has been our experience," Plosser observed, "that open and honest discourse … leads to the development of meaningful insights that can help inform relevant policy debates." He concluded by challenging the group to work together constructively in this dialogue to maintain a safe environment for payments.

## Consumer Perspective

**Moderator:**

***Ed Wargo***, Vice President, Customer Relationships, Javelin Strategy and Research

**Panelists:**

***Betsy Broder***, Assistant Director, Division of Privacy and Identity Protection, Federal Trade Commission

***Robert Shiflet***, Global Consumer Fraud Preventions Executive, Bank of America

***Tony Spinelli***, Senior Vice President and Chief Security & Compliance Officer, Corporate Security and Compliance, Equifax, Inc.

In introducing the Consumer Perspective panel, Kurt Helwig echoed Charles Plosser's counsel that consumer confidence is an imperative in the payment card business. Protecting cardholder security and maintaining the integrity of the card payment system are not only the "right" things to do for consumers, but they also serve the business interests of card issuers, networks, merchants, and acquirers.

Ed Wargo took up this point in opening the panel discussion by reporting that a recent Javelin research survey found security to be increasingly important to consumers in their decisions to obtain and use payment cards. Eighty-four percent of respondents to Javelin's October 2007 survey rated "security against ID fraud" as "important" or "extremely important" to those decisions. Survey respondents also indicated that they wanted to be engaged with their bank in anti-fraud solutions. They also said that they would be unlikely to shop at a retailer that had been hacked; however, Wargo went on to say, there are observable differences between what consumers say they will do in surveys, and what actually occurs. He offered the TJ Maxx experience as an example. Similarly, while consumers may say they want security, they also indicate that they do not want to experience inconvenience or disruption when conducting card transactions.

Overall, consumers have been slow to adopt self-protective security products and practices such as credit alert services and Internet shopping security tools. Wargo attributed the somewhat contradictory aspect of consumers' stated and actual preferences to their core expectations of "free, perfect, and now." Survey responses may accurately reflect what consumers prefer in an ideal scenario. In the real world, however, consumers encounter friction in the form of cost, time, and inconvenience that can cause actual behavior to deviate from their stated intentions.

Betsy Broder acknowledged that consumers' low tolerance for friction creates a cost for fraud prevention, but she posited the idea that educational and marketing efforts might be effective in reshaping the public's attitudes. The public is hearing messages, and these messages are affecting their opinions and behavior.

Unfortunately, she told the assembly, sometimes efforts to engage and inform the public can be undermined by the confusing messages it receives. As an example of that type of message, Broder mentioned a published report that used consumer complaint information compiled by the Federal Trade Commission (FTC) to rank banks according to their "customer security." While one of the FTC's missions is to collect complaint information about identity theft and payment fraud, the data are not gathered in a way as to be scientifically representative and were never intended to reflect individual banks' security practices. Some banks are more proactive in making referrals to the FTC, so their customers will be more represented in FTC complaint data than will less proactive banks. Banks with millions of customers are likely to have more customers making complaints to the FTC than will banks with thousands or even tens of thousands of customers.

Unfortunately, the published report did not make these limitations clear and, as Broder noted, produced a ranking of bank safety that most analysts agreed was misleading, at best. As Broder argued, there is a real need to provide information to consumers, but incorrect or misleading information can be counterproductive.

Because of the limits of using customer-initiated reports in analytical work, Broder reported that the FTC is working with the Department of Justice to obtain hard data on 50,000 households that were victims. The characteristics of the DOJ data are expected to facilitate meaningful analysis. The DOJ's activity, however, will not change the FTC's continuing efforts to collect consumer complaint information because, as Broder emphasized, that endeavor remains important to the FTC. Information collected from consumers helps law enforcement to prosecute identity theft and is useful in identifying patterns and enabling searches by ZIP code or other criteria.

Broder next discussed the new "red flag" requirements effective November 1, 2008. These rules require banks and lenders to have procedures and practices in place that would be triggered by warning signs (red flags) of identity theft. Examples of warning signs could include alerts and notifications from various sources, suspicious or unusual activity related to a covered account, and suspicious addresses or documentation. She reflected on events recounted previously where activity taking place in various parts of an organization led to identity theft that culminated in account fraud. Broder said that the adoption of red flag rules should provide institutions with the structure to use what appear to be unrelated activities as indicators of possible ID theft or potential fraud.

Robert Shiflet then described how Bank of America, in response to the type of cross-product, cross-channel activity Broder and others had described, had reorganized its fraud management structure to focus on the total customer relationship. Prior to this change, Shiflet said that Bank of America operated like most other organizations, conducting anti-fraud efforts largely within discrete product areas. As Bank of America observed that newer fraud tactics were taking advantage of this separation of product areas in ways that affected the entire customer relationship, it recognized the need to change its strategic approach to combating fraud. The response was to create anti-fraud efforts that span the enterprise, retaining expertise on individual product fraud while consolidating functional expertise under common management. Of critical significance, Shiflet argued, this enterprise approach is consistent with how consumers view their relationship with a bank. Consumers expect their banks to know their total relationship with the bank and manage accordingly.

Shiflet described the aforementioned challenges of balancing fraud control with the customer experience in managing the customer relationship. He described the particular dilemma presented when account numbers are compromised in a data breach. While a mass reissuance of cards with new account numbers is a highly effective fraud-prevention action, it also creates customer disruption and inconvenience. Shiflet went on to say that, across the industry, 25 to 35 percent of cards are being monitored because of potential compromise, but only a small fraction of those ultimately suffer fraud loss.[1] Rather than mass reissuance, a better response, in his view, is to actively monitor and systematically evaluate for indicators of fraud risk. This "surgical approach," including targeted reissuance along with flagging and monitoring compromised accounts, provides effective fraud control without creating undue disruption and inconvenience for customers.

Bank of America's experience to date with this enterprise approach to fraud management has been encouraging and has led to new collaborative efforts across business lines. At the same time, and echoing some of the earlier comments, Shiflet noted that Bank of America recognizes the im-

[1] Analysis of four data breaches found that even in the breach with the highest rate of misuse, less than one in 1,000 (.098 percent) of compromised identities subsequently experienced fraud. (The National Data Breach Analysis, ID Analytics Inc., 2005)

portance of having its customers more engaged in efforts to mitigate fraud.

Tony Spinelli began his remarks by noting that the scope of consumer data risk is much broader than the information held by banks. Equifax's data suggest that "hacks" of financial services institutions account for only 15 percent of all data breaches, but 55 percent of data lost across all breaches is financially relevant. His message was that all organizations, not just those that are directly a part of the payments chain, must reconsider what information needs to be stored and employ the same high degree of security in protecting that information. In this respect, he concurred with the earlier point made that security in payments is part of a larger societal effort that has to be made to more effectively safeguard personal and confidential information.

Spinelli revisited the theme of customer knowledge and awareness. Two years ago, Equifax conducted a study that revealed that many consumers did not know how to monitor their credit. As a result, Equifax revamped its website to emphasize consumer education. Expecting that consumers' monitoring of their credit information would be a big factor in preventing identity theft, Equifax created website functionality that enables consumers to self-manage their credit monitoring service, clicking options and controls on and off in "real time." Consumers can also perform these functions by telephone.

In response to a question asking what percent of consumers avail themselves of credit reporting, Spinelli acknowledged that it is "fairly low," but he noted that "proactive sponsors" can achieve a response of about 15 percent. The rise in response rate achieved by proactive efforts reinforced Broder's point that consumer engagement can be subject to positive influence. Shiflet interjected that Bank of America has observed that customers who have proactively used a credit bureau service, such as credit monitoring, indicate higher satisfaction with the bank on customer satisfaction surveys.

Spinelli concluded with the observation that when looking at well-publicized data breaches, punishment focuses on companies and not on the malicious individuals. He noted that of 137 known breaches, perpetrators have been prosecuted in only three. Repeating the point raised by Avivah Litan, Spinelli noted that many of these criminals operate outside the United States, making capture and prosecution more difficult.

Interesting observations and inferences were articulated during this panel discussion. Consumer research points to certain contradictions between statement and action. Services designed to help consumers deter fraud were introduced to the market relatively recently, so adoption hasn't occurred in numbers significant enough to provide sufficient fodder for analysis. However, there is evidence that proactive delivery of information to consumers can raise adoption levels. Some behaviors have been quantitatively observed, but underlying reasons have not been identified.

All of this suggests that consumers are in the early stages of understanding today's risk environment, its controls, and what role the consumer can play. Likewise, the industry is in the nascent stages of understanding consumer attitudes and motivations. But the bellwether learning points provided by these panelists suggest untapped opportunity in developing greater understanding of consumer behavior and preferences in this area, informing consumers' opinions and ultimately engaging them in the fight against payment card and other forms of fraud.

## Issuer Perspective

**Moderator:**

***Harry DiSimone***, Founder and CEO, Commerce Advisors, Inc.

**Panelists:**

***James Cichy***, Vice President, Fraud Services, PULSE

***Richard Detura***, Managing Director, Global Consumer Group Fraud Policy, Citigroup

***Alex Mogielnicki***, Senior Vice President, Risk & Knowledge Management, Chase Card Services

After introductions by Harry DiSimone, Alex Mogielnicki launched the discussion by presenting data on domestic fraud trends, emphasizing the U.S. card industry's progress in mitigating fraud over time. Using a graph plotting fraud as a percent of card volume, he demonstrated that domestic credit card fraud trends have shown an impressive decline since 1990, when fraud losses equaled 12 basis points[2] of total card volumes, declining to less than seven basis points in 2006.[3] He noted a series of industry innovations that factored into this decline, including CVV/CVC,[4] fraud scoring tools, terminal-based programs, and compromised account management systems (CAMS). He noted that the industry's successes have not come from a single solution but from the execution of multiple and interacting strategies. As he emphasized, there is no "silver bullet" in fraud management. Instead, efforts to contain payment card fraud must focus on a combination of multiple tools and practices, evolving over time, implemented at different points in the payment chain: at the networks, at merchant locations, at issuing institutions, and also by consumers.

While the industry has made noteworthy advances in controlling fraud, Mogielnicki's view of the future was less sanguine. Citing threats from data compromises, card-not-present transactions, cross-border exposures, social engineering, proliferation of usage channels, and other 21st century realities, Mogielnicki predicted an increase in fraud loss rates over the next two years. His predicted trend reversal will occur because of what he called the "ambient level of risk" existing in today's environment. The payment card industry is introducing new products in new channels and new markets that collectively create vulnerabilities for all participants: issuing and acquiring banks, networks, consumers, processors, and merchants. Vulnerabilities from extra-industry sources are also part of this: Hospitals, libraries, and universities all get hacked. Warehousing of data has facilitated the formation of illicit "identity bureaus" operating overseas. There is software that will produce a random account number with Mod 10 check.[5] Alternative payment choices, such as PayPal, did not exist 10 years ago. E-commerce is growing in significance. There is bifurcation in POS, with the U.S. using magnetic-stripe technology and parts of the rest of the world adopting chip and PIN technology.

The combination of these factors, Mogielnicki asserted, has produced a payment card environment that encompasses more diversity and more complexity than ever before, creating many new challenges for mitigating fraud. Further, he noted that as the pace of change is accelerating, challenges are compounded exponentially rather than arithmetically.

Richard Detura told the group that the domestic trends described by Mogielnicki are also operating globally. He augmented Mogielnicki's point about POS bifurcation by presenting a graph (shown on page 15) that maps chip-card deployment in countries around the world. Canada, Australia, and much of Asia and Europe have implemented chip-card programs or have plans to do so. There are no immediate plans in the U.S. for large-scale chip-and-PIN programs. This map became a catalyst for comments and discussion about chip-card technology for the remainder of the day, as conferees considered the risk implications of this chip/nonchip schism for the U.S. market.

Detura repeated a point made by earlier presenters: that fraud follows the path of least resistance. Counterfeit plastic fraud becomes more difficult when POS is chip-enabled, so consequently, that type of fraud moves to nonchip locations. Because of this, he sees the U.S. as being vulnerable to fraud in a way reminiscent of its situation when other countries adopted CVV/CVC before the U.S., and fraud rose in some cases to the high teens (in basis points of volume). But chip technology doesn't eliminate fraud; it just

[2] A basis point is equivalent to 1/100th of a percent.

[3] In 2006, domestic credit card fraud losses experienced by issuers of American Express, Discover, MasterCard, and Visa were $1.24 billion, or $0.0619 per $100 in spending volume. *Nilson Report*, Issue 876 (March 2007).

[4] Card verification value is a three-digit security number printed on the back of Visa payment cards. MasterCard's equivalent is the card verification code.

[5] Also known as the Luhn algorithm for its creator, IBM scientist Hans Peter Luhn, Mod 10 is a patented checksum formula used to validate a variety of identification numbers, including payment card numbers.

causes it to change form. Experience in the United Kingdom and elsewhere suggests that where chip technology is dominant, fraud migrates[6] to card-not-present channels and across borders to locations with different authorization routines.

Detura's observations of consumer behavior reinforced other comments that cardholders have little tolerance for interruption at the point of sale (POS). They want to be involved in preventing fraud but not if it means POS inconvenience. However, for fraud control tools such as neural networks to be effective, issuers have to be prepared to disrupt a POS transaction. As Detura explained, this is the dilemma facing issuers as they attempt to strike a balance between customer experience and effective fraud deterrence.

James Cichy spoke about debit card fraud, which he said has characteristics similar to credit card fraud, along with some important differences. Debit is affected by the same trends occurring in credit card fraud. Debit, however, experiences more PIN fraud, whereby perpetrators obtain cash rather than merchandise, than is seen on the credit card side. Cichy suggested that the biggest difference is in the customer's mindset about debit fraud. Despite similar network zero-liability rules, cardholders have a higher level of concern when their funds on deposit are used fraudulently compared to fraudulent use of a credit line, which they don't consider "their" money. Debit card fraud, by definition, isn't limited to the card alone. Debit card fraud means a checking, savings, or money market account has also been accessed, which may heighten the concern and inconvenience for the victim. While these concerns exist, Cichy observed that consumers are equally intolerant at having their debit card transactions disrupted as they are about interruptions of credit card transactions. Cichy opined that consumer awareness of zero-liability protection counteracts their anxiety about fraud, even on their debit cards, sufficiently that desire for convenience at POS supersedes other concerns.

Cichy concluded with thoughts about the need for communication and cooperation across organizations in developing strategies to mitigate fraud. As an example, he advocated including fraud and risk specialists on project teams when developing new products or designing major marketing initiatives. Having someone review concepts with an eye to possible fraud risks, he argued, will help to "bake in" fraud deterrence as strategies are being developed.

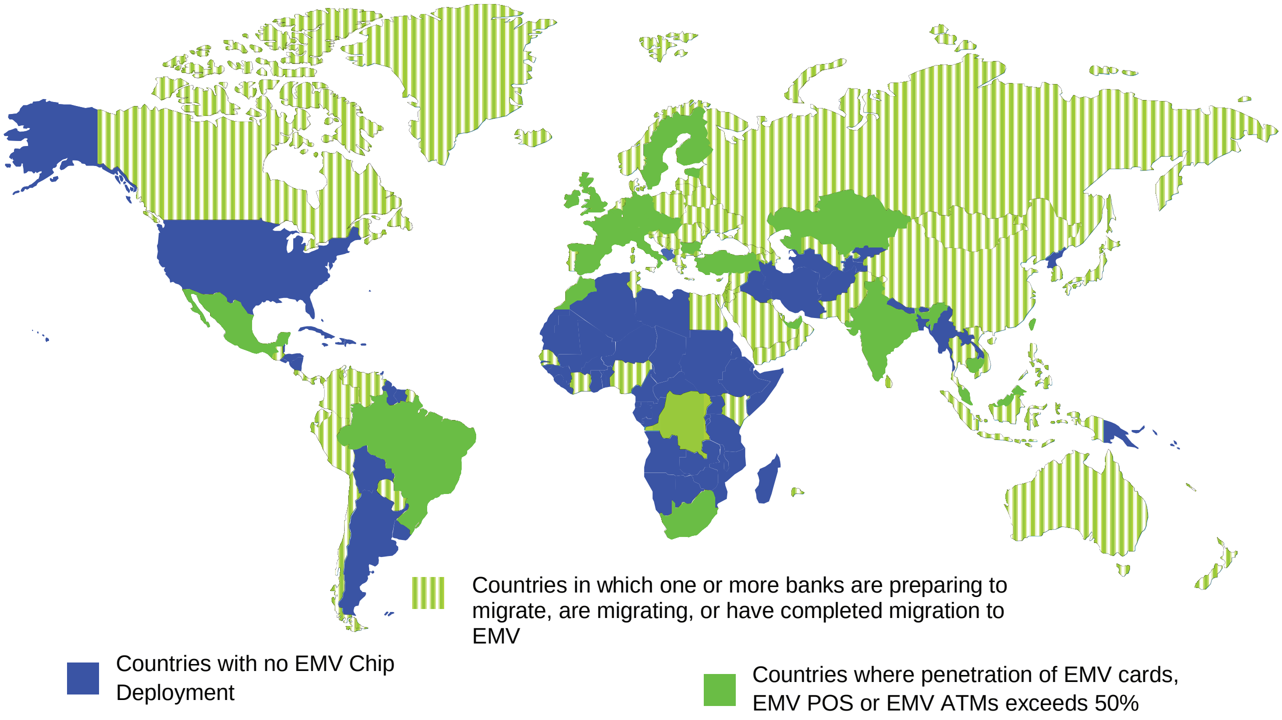
Reflecting on the chip-PIN deployment map presented by Detura, Harry DiSimone posed the compelling question of whether chip-card adoption in the U.S. was "inevitable." This engendered a vigorous discussion among the panelists and members of the audience. One line of discussion concerned the differences between the U.S. and non-U.S. markets. Outside the U.S., major issuers are also major acquirers, so the investment necessary to create a chip-card infrastructure on the acquiring side can be recouped by the organization in the form of lower fraud losses on the issuer side. In the U.S., issuers and acquirers are generally separate firms with distinct revenue structures, where merchants would accrue less value from their investment in new card-acceptance hardware and software.

Another chip-card limitation discussed was related to the card-not-present environment, which Alex Mogielnicki reported accounts for 25 to 30 percent (and growing) of card transactions. Adapting chip-PIN technology to Internet and other card-not-present environments presents obvious challenges. If card-not-present transactions are left unprotected, experience shows that fraud will move from the protected card-present environment to the Internet and other channels where chip and PIN technology is ineffectual.

Participants noted that the countries that have implemented chip technology may cover a lot of geography, but they are not necessarily where the most card transactions take place. Participants also observed that this is a relatively old technology. This led to a discussion about a potential "leap frog" from magnetic-stripe to a more advanced technology, perhaps one with efficacy

[6] Despite its success in decreasing domestic fraud on counterfeit and lost/stolen cards since its adoption of chip and PIN authorization, the U.K. experienced record fraud losses in 2007. Card-not-present fraud grew 37 percent in 2007. Fraud more than doubled that year from counterfeited U.K. cards used outside the country. *Cards &Payments* (July 2008)

## EMV Chip Deployment


Countries in which one or more banks are preparing to migrate, are migrating, or have completed migration to EMV
Countries with no EMV Chip Deployment
Countries where penetration of EMV cards, EMV POS or EMV ATMs exceeds 50%

Source: Richard Detura, Managing Director, Citigroup Global Consumer Fraud Risk Management

in the card-not-present environment, or perhaps one that would deliver additional value beyond fraud mitigation that could help rationalize the investment expense. DiSimone argued that it is very difficult to make the business case[7] for chip technology on the basis of fraud reduction alone, but he raised the question of whether the need for worldwide interoperability would eventually require the U.S. to issue chip cards. While some participants used words like "inevitable" to express their support for chip and PIN deployment in the U.S., there was no clear consensus on whether this is likely to occur any time soon. Nevertheless, the fact that the issue generated such debate led some attendees to propose that resources might be devoted to researching the potential impact of chip and PIN deployment in the U.S. market.

### Network Perspective

**Moderator:**

***Ron Congemi***, Chairman, EFTA

**Panelists:**

***Jodi Golinsky***, Vice President, Regulatory & Public Policy Counsel, MasterCard Worldwide
***Mark O'Connell***, President and CEO, Interac Association and Acxsys Corporation
***Russell Schrader***, Associate General Counsel, Global Enterprise Risk, Visa Inc.

In introducing the panel, Ron Congemi noted the unique position of networks in man-

[7] In its March 29, 2008, issue of *Strategic Commentary*, Speer & Associates, Inc. estimates a cost of over $10 billion to make the U.S. compliant with card network standards for chip cards. The article also reports that countries that have implemented chip cards have been successful in reducing fraud rates, but rates of fraud prior to implementation were measurably higher than current U.S. experience. The article also notes the "long-payback period that is typical in most countries," noting that the Canadian conversion to EMV will cost in excess of $1 billion, with fraud savings projected at "a minimum of $100 million annually once 'chip and PIN' have been fully implemented."

aging the integrity of the card payment system throughout the fraud "life cycle," from prevention to investigation to remediation. He noted that this begins with standards and how they are implemented and monitored. PCI is one set of standards adopted by the networks in their efforts to control fraud.

Jodi Golinsky recapped the evolution of PCI-DSS from its origin as several discrete sets of standards established by individual networks to one common set, established by an open standards body, the PCI Security Council. PCI standards articulate 12 major data security steps, a PIN-entry device security program (PED DSS), a payment application security program (PA-DSS), and a self-assessment questionnaire. Collectively, these provide a "road map" for adoption and compliance. In addition to establishing and enforcing standards, the networks also have an obligation to encourage the understanding and adoption of PCI standards. Two years ago, Golinsky acknowledged, the program was not as widely accepted as the networks would have liked. Since then, communication and education efforts, especially related to data breach risks, have rapidly improved awareness and compliance in the merchant community. The merchant community now, Golinsky noted, no longer asks why they must be PCI-compliant, but rather how they can become so.

However, in the aftermath of breaches at retailers that were believed to be PCI-compliant, some critics have called PCI standards into question. Golinsky responded that MasterCard is not aware of any compromise of a PCI-compliant merchant and emphasized that PCI compliance is a "journey, not a destination"; vigilance, not compliance dates, is critical. And, she concluded, like other efforts to mitigate fraud, PCI is a critical piece but not a panacea; fraud cannot be reduced by any one party or program. It requires holistic efforts by all key stakeholders.

Speaking next, Mark O'Connell concurred that there is no single resolution for dealing with fraud. Although Canada's not-for-profit Interac debit card brand is moving forward this year with chip and PIN, Interac's research shows that chip cards alone won't eliminate fraud. O'Connell reported that as the United Kingdom moves to chip-card technology, it is seeing fraud move across borders, as well as to online and other card-not-present channels. "All wars," O'Connell observed, "are fought on multiple fronts and that is true in the war against fraud."

Canada, with an economy roughly equal to that of California, hopes to learn from and avoid some of the pitfalls encountered by the U.K. Still, it is not depending solely on chip cards and PIN use to reduce fraud. Interac continues to develop rules-based fraud management tools to augment neural network applications.

O'Connell briefly discussed Canada's decision to move forward with chip cards. Canada has no signature debit product. Instead, its Interac EFT network is used to support PIN-POS at Canadian merchants. Beginning in 2000, skimming schemes that captured card numbers along with their PINs subjected the Interac system to annual increases in fraud loss of about 25 percent. As Canada's largest payment brand, Interac had to arrest this trend, and the company decided that chip cards were the solution.

O'Connell acknowledged that differences between the Canadian and U.S. banking, regulatory, payment card, and retailing environments would mean that different rationales would be used if a similar decision were to be made in the United States. For example, he noted that the Canadian government maintains fairly sweeping power to regulate private card networks. Canadian regulations also allow for collaboration and information-sharing among competitors. This cooperation was the cornerstone for the migration to chip cards. While Canada, like the U.S., has a bifurcated issuer and acquirer structure, the conditions in Canada enabled a consensus to form around a common belief that fraud is a collective problem requiring a shared solution.

Returning to the network environment in the United States, Russ Schrader described the following roles and responsibilities of networks in mitigating payment card fraud:

1. *Setting standards*, including PCI, which Schrader described as "essentially an audit,

but an audit for practices that really should be implemented." He commented on the evolving nature of PCI standards as new knowledge makes its way into the revision of standards.

2. *Acting* as a clearinghouse for issuers who call with information about potential fraud they may be seeing and with questions about what others are seeing, and what is being observed centrally at the network.
3. *Investigating* fraud and conducting forensics.
4. *Disseminating information*. Schrader provided CAMS alerts as an example while also noting that merely because a card number appears on a CAMS alert does not mean fraud has happened or will happen. Issuers independently decide how to treat their accounts identified as part of a CAMS alert.
5. *Educating*, through webinars, government testimony, and working with regulators.
6. *Providing alternative means of dispute resolution*. Schrader observed that litigation is "neither a cost-effective nor satisfactory solution on an ongoing basis."
7. *Interfacing with law enforcement*. "These are international cybercrimes," Schrader stated, "and we need to get to the root problem." He reported that Visa has found that collaboration with law enforcement agencies in the Asia Pacific region and Europe has been effective in shutting down off-shore criminal organizations.

In the discussion subsequent to the panelists' remarks, some attendees argued that network rules and standards do not always result in appropriate allocation of costs associated with mitigating fraud. Specifically with respect to PCI standards, some felt that a disproportionate burden falls on merchants. Others suggested that because of the central role played by networks in payment systems, they are in the best position to safely hold transaction information, minimizing the risk of data compromises at the merchant level. All agreed that fighting fraud requires collaboration among all sectors of the industry.

## Merchant Acquirer Perspective

**Moderator**:

***Marc Abbey***, Partner, First Annapolis Consulting

**Panelists:**

***Donald Boeding***, Senior Vice President, General Manager of Merchant Services, Fifth Third Bank Processing Solutions

***Robert Carr***, Chairman and CEO, Heartland Payment Systems

***Mike Herman***, Chief Compliance Officer, Chase Paymentech

As the moderator for the final panel of the conference, Marc Abbey observed that it was somewhat telling that none of the earlier panels had explicitly considered merchants that had been criminally hacked as victims of crimes, although they certainly were. Merchants and acquirers also experience financial loss and potentially diminished reputation from these cybercrimes, and they have strong motivation to reduce their vulnerability to data breaches. He articulated some of the challenges and complexities facing merchants and their acquirers noting that such challenges may not be commonly known and appreciated.

Approximately 6 million merchants in the United States accept payment cards. Many of them have multiple outlets, and many have multiple sales channels (storefronts, websites, and catalogs). Myriad applications are needed to interface with dial terminals, electronic cash registers, mail order, and other platforms. Value-added resellers (VARs)[8] compound the complexity of the merchant processing business by requiring another layer of systems integration for acquirers. Yet, Abbey noted, industry fraud losses have varied within the same range for the last 15 years, an indication that acquirers, along with the rest of the industry, are being proactive in fraud control. Acquirers, he continued, can manage their exposure by opting in or out of industries and environments where risk is highly concentrated. It is well-known, for example, that credit and fraud exposure is higher

[8] Value-added resellers are software companies that offer technology solutions that include a payment interface.

in the airline industry than in other merchant categories. Payment fraud also varies by merchant sales channel, with an estimated 30 percent of card fraud occurring in card-not-present environments. Acquirers can opt in or out of these businesses, depending on their tolerance for risk and their tools to manage it.

There are also different risk profiles among small and large merchants.[9] Donald Boeding's firm acquires for many large merchants. As the acquirer for TJ Maxx, he has also had experience in managing situations in which a large number of data are compromised.

Boeding said that large merchants have made investments in data security and are motivated to proceed with PCI-DSS and not merely because it is a requirement; merchants know that it is good business. The data breach at TJ Maxx reported in early 2007 added to the sense of urgency. Along with the impetus of network deadlines for PCI compliance, high-profile retailer data compromises accelerated the pace of PCI compliance so that Boeding was able to report that, at the time of the conference, 80 percent of the industry's largest (Level I) merchants were PCI-compliant, compared to 30 percent in January 2007.

Still, Boeding questioned whether an entity can ever be absolutely PCI compliant. The status can change in a minute. The standards, he argued, are very black and white, but when you apply them, there are shades of grey.

Robert Carr discussed the challenges faced at the other end of the merchant spectrum among smaller brick-and-mortar locations, often with dial-terminal operations, many doing less than 1,000 card transactions per year. These merchants present a different and, Carr asserted, generally lower risk profile than large, multi-location merchants on wireless networks, doing business over the Internet or in other card-not-present venues. Yet all merchants, Carr stated, are obliged to comply with the same set of PCI standards. A more efficient solution, he observed, would be to define standards that best suit the different merchant environments.

To further emphasize the differences, Carr noted that "small merchants are not small minded, but PCI is not their top-of-mind concern." Small businesses are focused on getting employees to work and getting product stocked. While large retailers employ individuals specifically to manage payment costs and processes, small merchants do not have specialists of this type. Carr revisited the topic of VARs mentioned by Marc Abbey, stating that some VARs have written code into their products that, in violation of network rules, captures and stores payment card information as an auxiliary feature of the software. Many of the small merchants who purchase the VAR's product are not aware that this function exists, nor do they use the stored information. By extension, they are unaware that they are out of compliance with PCI standards.

This situation has transpired because, Carr contended, until recently the networks have not been aggressive in monitoring VAR certification. This has allowed vulnerabilities at these merchant locations. He anticipates that the new requirements established by the networks for certifying software will be a major improvement. These will initially apply to certifying new software, after which software currently in use that is not compliant will be decertified.

In his remarks, Mike Herman agreed with Carr's point that small merchants do not present the same risk nor do they have the same resources for complying with PCI requirements. He further argued that emphasis on large merchants conforms to the 80-20 rule: Concerted efforts to achieve PCI compliance in 20 percent of the system will accomplish central objectives for 80 percent of the transactions.

Adding to the discussion of differences among merchant types and their PCI compliance challenges, Herman introduced another aspect of complexity experienced by multinational mer-

[9] As defined by Visa Inc., merchants fall into one of four size categories determined by number and type of payment card transactions per year: Level I – over 6 million transactions per year; Level II – 1 million to 6 million transactions per year; Level III – 20,000 to 1 million e-commerce transactions per year; Level IV – fewer than 20,000 e-commerce transactions/year and all other merchants processing up to 1 million transactions a year (Visa's website).

chants. These global retailers deal with multi-currency software applications and must have data security structures that reflect variations in requirements by the networks and governments in different regions of the world. Despite all of these challenges, however, Herman stressed that the objectives of PCI-DSS — to ensure that cards remain the most secure form of consumer payment in all environments — must be upheld. He contended that collaboratively developed industry solutions will result in better outcomes than governmental or regulatory alternatives. He also concurred with the comments of others that there is no single perfect way to prevent payment card fraud. PCI plays a critical role, but it is not a 100 percent solution, nor is it a solution 100 percent of the time. It does, he maintained, play a critical role in protecting the integrity of the card payment system.

In the ensuing discussion, there was debate about the application of PCI data protection standards to various merchant categories. Some participants argued that PCI standards represent commonsense security practices that merchants of all sizes — indeed, anyone handling sensitive information — should have in place. Others challenged the view that the needs of small merchants were not being addressed, noting that the PCI process logically focused first on the sources of highest transaction volume and that attention has been given to the special issues facing smaller merchants. A discussion ensued regarding which pieces of transaction information merchants were required to maintain for chargeback purposes (network requirements) versus what is being kept voluntarily by merchants to facilitate returns and exchanges. While no specific proposals were made, there was a sense that all players in the system need to work together to minimize the amount of sensitive data maintained by merchants to conduct business.

## V. Conclusions

While payment card fraud has existed since the introduction of cards into the payment stream, the highly publicized data breaches in recent years have created, in the words of Marc Abbey, an “inflection point” that focused attention on this subject from all fronts. This broadened base of public and industry concern has galvanized action across the entire payments chain. This important development recognizes that perpetrators of fraud do not limit their attempts to exploit vulnerabilities to only one link of the chain. They will hack merchants, phish consumers, and use social engineering to extract information from issuers.

Because fraud occurs in many ways, there is also no “silver bullet” that will radically diminish fraud. The industry’s historical success in controlling payment card fraud has evolved over time as the result of a combination of many tools and practices: card activation, card verification codes, neural networks, consumer education, network alerts, address verification services, and real-time POS authorization, to name but a few. The conference discussion included many examples of how our increasingly complex payments environment and the growing capabilities of criminals are combining to raise the bar in meeting the challenge of ensuring a safe and secure environment for consumers in their use of payment cards. Participants also agreed that effective strategies for mitigating fraud will depend on engaging all stakeholders.

While the subject of chip and PIN deployment has been debated for years, discussion at this event suggested that the tenor of the debate is changing. As more of the world moves toward this advanced authorization technology, there is a growing concern that the U.S. and its magnetic-stripe technology may become a growing target for fraudsters stymied by chip and PIN regimes elsewhere. Conferees recognized the value of chip-card deployment in the U.S. for its potential to control fraud and also as a step toward greater interoperability with other countries that have adopted, or have plans to implement, chip and PIN.

Despite the sense that deployment of chip cards in the U.S. may be inevitable, participants recognized that, to be successful, the technology needs to be adapted to the card-not-present environment, which is where both transactions and fraud are growing. And while chip technology is no longer cutting edge, deployment would still carry an expensive price tag for both issuers and acquirers/merchants, raising the question of whether the industry should look to a more advanced solution if a major investment is to be made.

Awareness also emerged that even with concerted efforts by all segments of the card payment system, the risk of compromised information and the resulting fraud are part of the larger milieu and cannot be completely controlled within the payment card system. Banking-related information can and is obtained for illicit purposes from nonfinancial institutions, such as universities and medical facilities, which collect personal information. Bringing criminals to justice also lies outside the purview of the payment system, but some at the conference recognized the collaboration that exists (and continues to advance) between law enforcement and card industry players. Indeed, since the conference was held, 11 individuals from five countries were arrested in connection with the data theft at TJX and other merchants. While arrest and prosecution will not provide an unqualified deterrent to cyber crime, these arrests do demonstrate that even in complex schemes distributed across several continents and conducted with a shield of invisibility, perpetrators can be identified and captured.

While the conference discussions did not focus on specific proposals, a number of critical insights were explored and new directions for further research identified. As several participants noted, a key element to achieving a successful and productive dialogue was the inclusion of the multiple perspectives represented in the meeting. Successfully addressing the many new challenges in combating fraud in the modern payment card system cannot be done within separate areas of the industry. Better understanding of each other's unique roles in this effort is a critical prerequisite to developing successful solutions.

# APPENDIX I
# Conference Agenda

**Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud**
A conference jointly sponsored by the Federal Reserve Bank of Philadelphia's Payment Cards Center and the Electronic Funds Transfer Association (EFTA)

*Wednesday, April 23, 2008*

**Welcome and Introductory Remarks**
Peter Burns, Federal Reserve Bank of Philadelphia
H. Kurt Helwig, Electronic Funds Transfer Association
Michael Collins, Federal Reserve Bank of Philadelphia

**Keynote Address: Regulatory Perspectives on Payment Card Fraud**
Jon Greenlee, Associate Director, Operations and IT Risk Section, Federal Reserve Board of Governors

**Managing Payment Fraud Risk in a Challenging Environment: Setting the Stage**
Moderator: Peter Burns, Federal Reserve Bank of Philadelphia
Panelists: James Brown, University of Wisconsin
Avivah Litan, Gartner Inc.
Richard Parry, JPMorgan Chase
Paul Tomasofsky, Two Sparrows Consulting

*Thursday, April 24, 2008*

**Welcome**
Charles Plosser, President, Federal Reserve Bank of Philadelphia

**Consumer Perspective**
Moderator: Ed Wargo, Javelin Strategy & Research
Panelists: Betsy Broder, Federal Trade Commission
Robert Shiflet, Bank of America
Tony Spinelli, Equifax

**Issuer Perspective**
Moderator: Harry DiSimone, Commerce Advisors, formerly EVP of Chase Card Services
Panelists: James Cichy, PULSE
Richard Detura, Citigroup
Alex Mogielnicki, JPMorgan Chase

**Network Perspective**

Moderator: Ron Congemi, EFTA  
Panelists: Jodi Golinsky, MasterCard Worldwide  
Mark O'Connell, Interac Association and Acxsys Corporation  
Russell Schrader, Visa Inc.

**Merchant Acquirer Perspective**

Moderator: Marc Abbey, First Annapolis Consulting

Panelists: Donald Boeding, Fifth Third Bank  
Robert Carr, Heartland Payment Systems  
Michael Herman, Chase Paymentech Solutions

**Wrap-Up: What Have We Learned?**

Participants: Panel moderators and conference organizers

## APPENDIX II
## Institutions Represented at the Conference

41st Parameter
American Express
Bank of America
Barclays Bank Delaware
BB&T
Bryan Cave LLP
Cardtronics
Chase Paymentech
Citi Cards
Citigroup
Collis America, Inc.
Commerce Advisors, Inc.
Commerce Bank-Kansas City
CO-OP Financial Services
CUNA Mutual Group
Discover Financial Services
Electronic Funds Transfer Association
Equifax
Federal Reserve Bank of Chicago
Federal Reserve Bank of Kansas City
Federal Reserve Bank of New York
Federal Reserve Bank of Philadelphia
Federal Reserve Board of Governors
Federal Trade Commission
Fifth Third Bank
First Annapolis
First Data Corporation
FIS
Gartner, Inc.
Heartland Payment Systems
ICBA Bancard, Inc.
Interac Association & Acxsys Corporation
Javelin Strategy & Research
JPMorgan Chase & Co.
London Potomac
MasterCard Worldwide
MetaBank
Metavante Corporation
New Jersey Judiciary
NYCE Payments Network, LLC
Online Resources
Paul, Hastings, Janofsky & Walker, LLP
PayPal
PCI Security Standards Council
PSC
PULSE
SWACHA
Transaction Network Services
TransUnion
Two Sparrows Consulting
U.S. Attorney's Office, Eastern District of PA
University of Wisconsin- Milwaukee
US Bank
Visa, Inc.

> “The Federal Reserve Bank of Philadelphia will be widely recognized as a leader and innovator in central bank knowledge and service.”
>
> Charles I. Plosser
> *President*

PAYMENT CARDS
*Center*

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall
Philadelphia, PA 19106-1574
215-574-7220
215-574-7101 (fax)
www.philadelphiafed.org/pcc

**Peter Burns**
*Vice President and Director*

**Bob Hunt**
*Assistant Vice President*

The Payment Cards Center was established to serve as a source of knowledge and expertise on this important segment of the financial system, which includes credit cards, debit cards, smart cards, stored-value cards, and similar payment vehicles. Consumers’ and businesses’ evolving use of various types of payment cards 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.