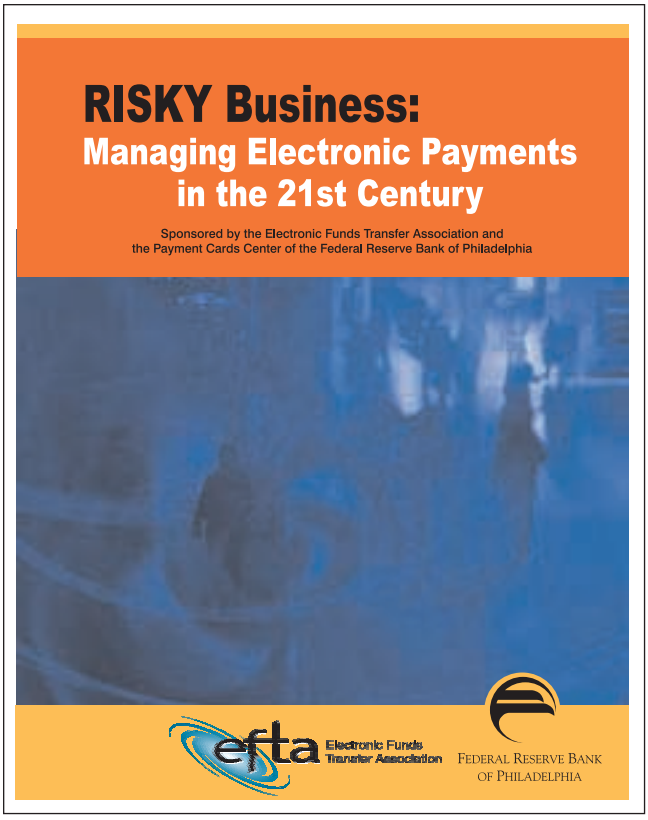
CONFERENCE SUMMARY



Risky Business

Managing Electronic Payments in the 21st Century

June 20 - 21, 2005

PAYMENT CARDS Center

Federal Reserve Bank of Philadelphia

Risky Business

Managing Electronic Payments in the 21st Century

Marilyn Bochicchio
Senior Consultant and ePIC Director
Electronic Funds Transfer Association

Stanley Sienkiewicz
Payment Cards Center
Federal Reserve Bank of Philadelphia

Summary

On June 20 and 21, 2005, the Payment Cards Center of the Federal Reserve Bank of Philadelphia, in conjunction with the Electronic Funds Transfer Association (EFTA), hosted a day-and-a-half forum, "Risky Business: Managing Electronic Payments in the 21st Century." The Center and EFTA invited participants from the financial services and processing sectors, law enforcement, academia, and policymakers to explore key topics associated with the challenge of effectively managing risk in a payments environment that is increasingly electronic. The meeting's goal was to identify areas of potential risk and explore interindustry solutions. This paper provides highlights from the forum presentations and ensuing conversations.

The views expressed here are those of the authors and do not necessarily represent the views of the Federal Reserve Bank of Philadelphia or the Federal Reserve System.

TABLE OF CONTENTS

Introduction

Risk and banking are inextricably linked. In fact, some people contend that managing risk is the essence of banking. For financial institutions, as well as for the organizations that support them, effective risk management is essential to success. Organizations that are unwilling or unable to effectively manage risk diminish their franchises—with potentially painful outcomes for the public and private sectors.

The move from a largely paper-based payments system to one in which electronic payments predominate has created new opportunities for fraud and new risk management challenges for financial institutions. Whereas financial institutions could once dismiss electronic payments risk and its associated costs as a marginal cost of doing business, today the potential implications cannot be ignored.

The challenges to financial institutions are compounded by a new and uncharted environment that includes:

- **Nontraditional industry participants.** Payments processing is no longer a financial-institutions-only business. Although new and nontraditional participants often fill important service voids and push the envelope of innovation, some may lack the experience and capabilities to implement risk management policies and technologies that meet traditional industry standards.

- **Sophisticated criminals.** Today's criminals are technologically and organizationally sophisticated, and they have extensive risk mitigation tools and information at their disposal. The Internet, for example, has eliminated the protective barrier of geography, opening borders for potential electronic payments crime, and created an inherently anonymous environment, adding a new level of challenge to "knowing your customer."

- **Increasingly large databases.** Market-driven scale economies have led to a situation in which a number of firms are managing increasingly large databases and facing the possibility that a single breach could place millions of accounts and customers at risk—and even threaten the viability of major organizations. The potential threat is heightened by a high level of interdependency among industry participants, further expanding the possibilities of systemic risk and the potential to erode consumer confidence in the banking system.

- **Speed of change**. The speed of change in the processing of electronic payments challenges the ability of the legal and regulatory communities to keep pace.

- **Focus on short-term profitability.** Intense competition and a focus on short-term profitability have the potential to undercut the principles of sound risk management. At what point do bottom-line pressures influence risk-management-related decision-making?

The meeting's goal was to bring together a diverse group of industry leaders involved in electronic payments processing to identify areas of potential risk, address best practices to manage the risk and prevent fraud, and gain widespread support for collective action to further safeguard the integrity of the system.

Welcome

Peter Burns, Vice President, Federal Reserve Bank of Philadelphia, and Director, Payment Cards Center
H. Kurt Helwig, Executive Director, EFTA
Anthony M. Santomero, President, Federal Reserve Bank of Philadelphia

Peter Burns opened the conference by welcoming attendees to the Federal Reserve Bank of Philadelphia. In his remarks, he emphasized the Bank's commitment to supporting industry efforts to address topical issues such as those to be covered during "Risky Business: Managing Electronic Payments in the 21st Century." He noted that this meeting is the fourth collaboration between the Bank's Payment Cards Center and the Electronic Funds Transfer Association (EFTA) and stressed the success of combining resources to facilitate a public-/private-sector dialogue on critical topics in electronic payments.

Kurt Helwig echoed Burns's comments about the strength of the Payment Cards Center/EFTA relationship and thanked him, and the entire Payment Cards Center staff, for their hospitality and contributions to the joint meetings. Helwig noted that the topic

for this conference arose during a roundtable at an EFTA board of directors meeting earlier in the year at which "payments risk" was unanimously identified as the top concern for the industry and for the businesses the directors represent. Consistent with EFTA's mission to contribute to the advancement of electronic payments, the directors endorsed a cross-industry conference to explore risk holistically, focusing on the need to break down "silos" of operation and to address risk on an enterprise level.

Burns introduced Anthony Santomero, who thanked participants for their diligent efforts in maintaining the security of electronic payments. Santomero noted the appropriateness of holding this discussion on electronic payments at a Federal Reserve Bank because payments were a primary reason for the establishment of the Federal Reserve System. He indicated that the United States is in the midst of an evolution to a new payment system in which paper processing is being displaced by electronic processing. While acknowledging the many benefits of electronic payments, he also noted that periods of transition can be difficult: Time is needed to identify and address the changes in the risk paradigm, and vigilance is necessary to ensure that unintended risk is not a consequence of electronification.

Santomero emphasized that the payment system is built on and sustained by trust among the parties involved. He noted that addressing electronic payment risk is extremely topical—there are multiple articles in newspapers these days—and that there is a tremendous interest in many quarters about the subjects to be addressed during the meeting, particularly identity theft and data security.

"It's important to recognize that risk is the heart of the matter, and it's a topic that is important to both the public and private sectors," he said. "We have a joint mission to work together to address risk and preserve trust in the payments system. That's why we are pleased to serve as the host for this meeting, which explores a timely and important topic."

Fraud Prevention and Mitigation: The Importance of a United Front

Frank D'Angelo, Chairman, EFTA, and President and COO, Payment Solutions Group, Metavante Corporation

Summary: *As chairman of EFTA, Frank D'Angelo set the stage for the presentations that followed and highlighted the need for all participants in the electronic payments industry to work as a team to make a difference in the fight against fraud. He presented statistics from a variety of sources to emphasize the pervasiveness of electronic-based financial fraud and used a video developed by the United States Postal Inspection Service (www.usps.com/postalinspectors) to drive home the point that electronic payments fraud is not just about numbers; it has the potential to cause great harm in the lives of individuals.*

D'Angelo began by stating that fraud is not a product issue, a financial institution issue, or a processor issue, but an issue that must be approached holistically and examined from all angles. He suggested that everyone involved in payments has a responsibility to do his or her part to deter fraud "because—in the end—our customers, families, friends, and each of us in this room could ultimately be a victim of identity theft or other fraudulent activities fueled by activities such as hacking, phishing, and skimming."

The Ever-Changing Face of Fraud

D'Angelo asserted that numbers tell the story of how fraud is manifested in today's electronic payments environment:

- **Hacking**
  - A month after DSW Shoe Warehouse announced a database hacking, investigators determined that transaction information from 1.4 million credit cards was stolen, a much larger figure than originally estimated.
  - A security breach at LexisNexis, a data collection company, affected nearly 10 times the number of consumers first reported: The number grew to 310,000 from the original estimate of 32,000.
- **Phishing**
  - According to TowerGroup, 31,000 distinct phishing attacks were launched in 2004; the number of attacks is predicted to grow to 86,000 during 2005.
  - Gartner Group and the Anti-Phishing Working Group suggest that the response rate to phishing attempts is 5 to 20 percent. Gartner

Group says that phishing is responsible for an estimated $1.2 billion in direct losses to banks and credit card companies worldwide.

- Forrester Research says that phishing has prompted 14 percent of survey respondents to stop using online banking and bill payment and another 20 percent to steer clear of these types of services. (TowerGroup estimates online banking is used in 33 million households.)

He also asserted that fraud is not limited to computer-based schemes:

- **Insider Data Theft**
  - In a Michigan State University study of 1,000 instances of identity theft, 70 percent were traced to insider data theft.

  - Gartner Group estimates that 70 percent of offenders who gain unauthorized access to information systems are employees and that 95 percent of these employee-engineered intrusions result in significant financial losses.

Consumer Confidence Is on the Line

D'Angelo indicated that one of the keys to the success of electronic payments, as with all forms of payments, is consumer confidence. Without it, there is no growth, no innovation, and no benefit to providers, processors, or users. Consumers are increasingly being made aware of the risks associated with electronic payments and expect their financial service providers to create a safe environment in which to conduct their financial activities online:

- According to Financial Insights, 60 percent of consumers surveyed were concerned about identity theft. The concern prompted 6 percent to switch financial institutions.

- Gartner Group predicts that 60 to 75 percent of U.S. banks will use an authentication method stronger than a password by 2007 (token, smart card, biometrics, or personal information).

Team Work

D'Angelo concluded his remarks by encouraging payment industry participants to present a united front in working together to mitigate risk and protect the integrity of the payments system. "It is incumbent on us to work cooperatively to maintain consumer confidence in the system," he stated. "This is a huge and never-ending challenge, but through forums, such as this one sponsored by the Payment Cards Center and the EFTA, we have the opportunity to bring together representatives from all segments of the industry to explore how we can work together to create an environment in which electronic payments can reach their full potential."

Government Affairs: Pending Legislation, Regulation, and Other Issues

Moderator: ***Lynne Barr,*** Partner, Goodwin Procter, and Counsel to EFTA
Panelists: ***Nessa Feddis,*** Senior Federal Counsel, American Bankers Association
Stuart Pratt, President, Consumer Data Industry Association

Summary: *The timing of "Risky Business"—beginning on the first business day following the public announcement of the security breach that involved 40 million accounts at Arizona-based CardSystems Solutions, Inc.—significantly influenced the focus of this session on government affairs. Attendees were specifically interested in exploring compliance issues related to the information security provisions of the Gramm-Leach-Bliley Act (GLBA) and understanding the issues that may be percolating in federal and state legislatures as a result of the recent series of high-profile security breaches.*

FACTA Addresses Identity Theft

Nessa Feddis

Feddis focused her comments on the Fair and Accurate Credit Transactions Act (FACTA or FACT Act), which, she indicated, is an example of Washington's serious stance on halting the misuse of electronic data to facilitate crimes, such as identity theft, against consumers.

Identity theft occurs when a criminal uses another individual's personal information—such as name, Social Security number, or credit card number—to take on that individual's identity to commit fraud. The criminal, for example, may use personal

information to open a new credit card account in the individual's name and establish a new address for statement mailings. When the individual doesn't pay the bills (which he or she doesn't know exist), the delinquent account is reported to a consumer reporting agency (CRA). The information recorded by the CRA has the potential to affect the individual's ability to get credit, insurance, and even a job.

FACTA amends the Fair Credit Reporting Act, which regulates who is entitled to have access to consumers' credit report information and how that information may be used. In separate provisions related to identity theft, FACTA aims to protect consumers by requiring the three major consumer reporting agencies (Experian, TransUnion, and Equifax) to send consumers, upon request, one free copy of their credit history during each 12-month period. In the best case scenario, consumers verify the information on their credit reports for accuracy and promptly report any inaccuracies, thereby minimizing potential damage.

As Feddis explained, FACTA also attempts to protect consumers by requiring that CRAs block any information that occurs as a result of the theft and that they alert lenders. The CRA that receives the fraud alert coordinates with the other two and with lenders, relieving consumers of the responsibility to notify multiple entities. The first fraud alert allows for an initial block of 90 days. Once the victim confirms that identity theft has occurred and obtains a police report (within 90 days), an extended alert may be placed on all files.

FACTA is being implemented in stages. Sections of FACTA for which rules were not necessary became effective December 1, 2004. Sections that require rulemaking are being rolled out. Rules for the prescreening opt-out notice went into effect August 2005, and those concerning medical information are planned for March 2006. Additional proposed rules are anticipated.

According to Feddis, unlike most statutes, in which regulations provide fine-tuning, FACTA is an enormous statute with much of the detail in the rulemaking. "Regulators face an extremely difficult task in the rulemaking process for a number of reasons, including the dynamic nature of fraud, the diversity in the way financial institutions operate, and the challenge of providing enough detail to make rules useful without drawing a roadmap for fraudsters," she said.

"Interagency Guidance for Banks": Responding to Security Breaches

Lynne Barr

Barr noted that the banking regulators' "Interagency Guidance for Banks," finalized in March 2005, is intended to assist financial institutions and others involved in delivering financial services to protect customer financial information—as required in Section 501 of the Gramm-Leach-Bliley Act (GLBA). The guidelines cover implementing an information security program; specifying objectives; assessing risk; managing and controlling risk; testing, training, encrypting, and monitoring; and overseeing service providers. In light of the recent high-profile security breaches, the key issue for many in the industry is how financial institutions should respond if their data are compromised.

Should a data security breach occur, Barr recommended that financial institutions take the following actions:

Preliminary Steps

- Consult counsel and notify legal department.
- Investigate and repair breach, securing systems and determining the scope of information compromised.
- Notify primary regulator and law enforcement, as appropriate.

Consumer Notification

- Determine if the data security breach involved "personally identifiable" or "sensitive customer information" and whether unauthorized use of such information is "reasonably possible."
- Determine if you are affected by state consumer notification requirements, which may vary from—and be more stringent than—federal requirements.[1]
- Prepare a consumer notification, ensuring that your statement is consistent with your stated privacy policies and that your message is reassuring and helpful. You also should tell consumers what to do if they notice unusual activity on their accounts.

[1] See also California guidance on best practices: www.privacyprotection.ca.gov/recommendations/secbreach.pdf.

External Communications

She also recommended that financial institutions take the following steps:

- Notify:
  - MasterCard and/or Visa and bank sponsor, if card data are compromised.
  - Insurers.
  - Audit committee and auditors.
- Review contracts with service providers.
- Make public disclosure (8-K filing and press release).
- File suspicious activity report (SAR).

Duties of Consumer Report Users

In addition to complying with the guidelines covered above, financial institutions must comply with Section 216 of the Fair and Accurate Credit Transactions Act (FACTA), effective July 1, 2005, requiring implementation of measures for proper disposal of consumer information, defined as rendering the information useless to anyone who might find it. The fine for noncompliance is $2,500 for each instance of neglect.

Congressional Outlook

Stuart Pratt

Pratt stated that both Congress and the states are deeply concerned about the security of electronic financial transactions and the industry should expect a variety of actions as a result.

String of Breaches Generates Publicity with Shelf Life

"The factors driving legislative concern include the recent string of security breaches and the ensuing media coverage, as well as the tremendous publicity being given to phishing scams," he said. "There is particular concern about the role of 'data brokers' and the security of the data they handle."

Acknowledging that security breaches have existed for some time, Pratt asked and answered the question, "Why is this year different?" He contended that the relatively new California law, which requires public acknowledgment of security breaches and reporting to the California office of privacy, highlights the public element of security breaches. The ChoicePoint security breach, the first major occurrence after the California law became effective, heightened the awareness of all state legislators of the potential effect of such events on their citizens. In addition, the steady stream of subsequent security breaches—whether or not customer data were at risk—has given the stories "incredible shelf life as reporters weave together old breaches and new." Collectively, these events and coverage of them have created significant public unease about online security and safety, which is translating into legislative concern.

State Activity: Expect More in 2006

Pratt predicted that there is likely to be even greater intensity on the state level in 2006, as legislators move forward with laws and bills addressing information security and notification about security breaches. Groups such as USPIRG, Consumers Union, AARP, and the Privacy Rights Clearing House are producing model bills and lobbying states to take action.

A key concern for Pratt's constituency of credit bureaus, processors, and mortgage lenders is potential laws governing data brokers, which are not regulated at the federal level. He warned that such laws "move through quickly," requiring vigilance on the part of interested parties.

What's Next in Congress?

Congress's first reaction to the publicity about breaches, according to Pratt, was to hold informational hearings related to jurisdictional issues. The hearings were held before a variety of congressional committees: House Energy and Commerce, House Financial Services, Senate Judiciary, Senate Banking, and Senate Commerce. Now that these hearings have concluded, bipartisan bills are likely to be introduced, and they will likely focus on regulating data brokers and Social Security numbers, providing notices about security breaches, and expanding GLBA-like information security requirements beyond the original circle of financial institutions. Legislative hearings will follow, and the complex jurisdictional topography will affect the timing of legislation.

Discussion

Layers of Requirements Could Impair the Smooth Operation of the Payments System

Most conference participants agreed that some form of federal legislation will be forthcoming, but they

expressed concern about the compliance challenges that may result from additional layers of state requirements. Adding layer upon layer of legal and regulatory requirements to make electronic payments more secure may do little to actually improve the security of the system but would surely create operational inefficiencies. Some participants argued that the key to maintaining the integrity of the electronic payments system is accurately ascertaining, at the time an account is first opened, the identity of the party with whom the financial institution or other organization is doing business.

Over-Notification

The possibility of over-notification relating to security breaches was another concern participants generally agreed on. When is notification really necessary, and how many times will a person be notified of the same breach? In this sense, participants argued, it is imperative for legislators and the industry to clearly define security breaches in the context of their potential effect on customers. Depending on the type of information involved, some breaches are highly unlikely to put consumers at risk. Notification in these cases is not only a cost burden, but more important, it can confuse consumers as to what actions to take and it can create unfounded anxieties.

Law Enforcement: The Intersection of Electronic Payments, Fraudsters, and Terrorists

Moderator: ***Judith Rinearson,*** Partner, Bryan Cave
Panelists: ***Christopher Bik,*** Special Agent, DEA
James Candelmo, Assistant U.S. Attorney, Eastern District of North Carolina
Robert A. Goldfinger, Commander of Criminal Investigations for the Rochester, NY Police Department (retired), Certified Anti-Money Laundering Specialist
Brian D. Lamkin, Chief, Financial Crimes Section, Federal Bureau of Investigation

Summary: *Representatives of three different law enforcement groups, joined by a retired police investigator, were unanimous in drawing a direct line between the terrorist events of September 11, 2001, drug trafficking, and other types of criminal activity and electronic commerce. They also were unanimous about the cultural shifts in law enforcement brought about by September 11, specifically the willingness of the various branches of law enforcement to work cooperatively with each other and with the industry to create the extensive network required to gather and deploy intelligence associated with financial crime in an increasingly electronic environment. All encouraged the financial services sector to be proactive in searching for exploitable flaws in the system and collaborating with law enforcement agencies.*

Department of Justice

James Candelmo

According to Candelmo, terrorist warfare renders traditional military responses relatively useless, since terrorists target entire populations, not just military resources. The financial services sector is a key target for terrorists. Although military targets are highly fortified, the financial backbone of the country is open and, therefore, vulnerable.

"The role of technology in aiding law enforcement to identify terrorist targets—ultimately leading to the terrorists themselves—cannot be underrated; nor can the role of finances in putting together a trail leading to terrorists," he stated. "Banks and their regulators are in a unique and valuable position to identify unusual financial activity, making their service and support in fighting terrorism essential. The banks are there on the front line; the FBI isn't, which is why the contributions of banks are important in combating a nontraditional adversary. Law enforcement now collects more intelligence than ever; the challenge is to put together the pieces of the puzzle," Candelmo concluded. A critical piece of this puzzle is often a network of underlying fraudulent financial transactions, and he urged financial service providers to continue in their efforts to combat these crimes.

Drug Enforcement Administration

Christopher Bik

Bik reported that the Drug Enforcement Administration (DEA) has moved beyond "just taking drugs off the street" to focusing on drug financing. Its key priority is stopping the flow of money from the street-level dealer in order to interrupt the financial flows that feed the enterprise.

He indicated that there are three primary ways drug money leaves the United States:

- Driving money across the border, where it can be transported to its final destination.

- Exchanging currency on the black market (e.g., a foreign drug dealer converts pesos into dollars and dollars into pesos).

- Using money services businesses that cash checks, sell traveler's checks, and execute wire transfers.

According to Bik, one of the major problems the DEA faces is distinguishing between funds being transmitted abroad for legitimate reasons (e.g., support of family members) and funds being transmitted as part of drug trafficking schemes. To help differentiate between legitimate and illegitimate transfers, the DEA conducts undercover activities as part of its financial operations, including initiating its own money-laundering schemes to identify how criminals do what they do and the organizations involved. This technique has enabled the DEA to successfully track funds up the money chain. Ultimately, the money goes through banks, which is why he said that the cooperation of the financial services industry is essential.

Federal Bureau of Investigation

Brian Lamkin

Security breaches are not the specific concern of the FBI, but "data that is sitting out there free and open" is, Lamkin told the audience. Similar to the DEA, the goal of the FBI's Financial Crimes Section is to "take down the apparatus [of the organizations that commit financial crimes], focusing on the enterprise rather than the individual violator."

Furthermore, Lamkin noted, "Scams flow to wherever activity is being funded. For example, fraudulent health-care-related activity spiked when the Medicare drug benefit program was announced 18 months ago. Although some fraudsters have gone high tech, there are still many frauds being perpetrated using low-tech techniques."

From the FBI's perspective, the most important step a financial institution can take to prevent crime is to know with whom it is doing business, especially if the financial institution has subsidiaries or operations that are national or international in scope. Financial institutions' involvement with shell corporations also concerns the FBI because a significant amount of fraud is being imported into the U.S. from Eastern Europe.

Bridging the Gap

Robert Goldfinger

According to Goldfinger, terrorist financing, money laundering, and fraud have changed the financial world. Advances in technology have resulted in a corresponding increase in risk: the increasing use of technology has enabled more access, and more access equates to more risk.

Criminals have served as a unifying force to motivate the private sector and government officials to work together. Terrorism and other anti-American criminal activities have resulted in new laws and regulations, setting the stage for positive cultural shifts that encourage coordination of efforts.

Goldfinger posed the question, "What can the financial service sector do to encourage the cultural shift?" and provided the following answers:

- **Cooperation.** Ensure that suspicious activity reports (SARs) are completed and submitted promptly. Conduct preliminary internal investigations, with input from legal advisors, and contact law enforcement with salient and/or time-sensitive information.

- **Coordination.** Seek advice and guidance from within the financial industry and externally from law enforcement. Network to create an informal team that will "get the bad guys" and protect the financial institution and its customers.

- **Communication.** Provide professional training to law enforcement task forces and associations. Contribute material to newsletters and publications.

- **Relationships.** This is a two-way street. Bankers have the in-depth knowledge that law enforcement needs in its investigations. Law enforcement wants to know about the new products that financial institutions are launching; they want to know what's next. Law enforcement is receptive to being asked to participate in the industry's professional training seminars to help build a bridge of understanding about the issues the industry faces.

He also warned that financial institutions can be vulnerable to a variety of money laundering schemes, including:

- **Placement.** Introducing the illegal proceeds into the financial system (i.e., money structuring in accounts).

- **Layering.** Converting the proceeds into a cash equivalent (e.g., smart card, wire transfer, or prepaid card).

- **Integration.** Placing the funds back into the economy (i.e., mixing laundered funds in with legally obtained funds or other assets).

Discussion
Foreign-Based Financial Crimes

In response to questions about criminals based in foreign countries, the panelists noted that ongoing activity encourages the support and cooperation of other countries, but it is a difficult undertaking. The DEA works closely with a number of countries to interrupt the cross-border flow of funds that supports the drug trade. The FBI has legal attachés in most foreign embassies and is placing more. The role of the attaché is to work with host law enforcement. In locales where those mechanisms are set up, there is significantly more cooperation among foreign counterparts.

Suspicious Activity Reports (SARs)

Although some financial service providers complain that there are too many SARs, the panelists agreed that SARs are an important tool for law enforcement. The number of connections being made between SARs and ongoing terror investigations is significant. The dollar figure listed on SARs is not particularly relevant to the FBI because the FBI understands that terrorists will attempt to stay below thresholds to avoid detection or to make money movements appear to be an insignificant credit card scam. The FBI runs parallel investigations. If there is an indication of true terrorism—rather than a purely financial fraud—teams are consolidated to work on the terrorist activities.

Keynote Address – Risk: Another Word for Payments

Suzette Massie, President, Global Payments Consulting, Carreker Corporation

Summary: *The second day's session began with a broad overview by Suzette Massie. Risk management organized around payment silos is not appropriate or effective in today's highly electronified and extremely complex payments environment. Financial institutions must strive to move risk management to the enterprise level, migrating payments and risk management in tandem to achieve this goal.*

According to Massie, managing payments risk was once a sideline of the payments business. Today, that has changed:

- **Fraud occurrences and types are exploding.** Examples include phishing, spoofing, keystroke logging, account takeover, identity theft, money laundering, and customer data breaches.

- **Regulation has mushroomed.** New payment-based regulation has come from a variety of legislation, including the Bank Secrecy Act, the Patriot Act, and Sarbanes-Oxley, section 404.

- **Spending is up.** Financial institutions plan to spend $1.8 billion on security this year, a 12 percent increase over last year.

- **Competition is fierce.** Competition for customers, new products, and evolving services never ends.

Massie argued that, in this environment, financial institutions can scarcely make decisions about the direction their payments system will take without considering enterprise risk each step of the way.

Enterprise Payments and Enterprise Risk

She emphasized that payments are now a critical part of the industry, representing a $200 billion business in the United States and $600 billion globally, and contributing 38 percent of operating income to the top 50 U.S. banks.

Traditionally, payments have operated within a highly fragmented structure within the banking environment, but that is changing. "Many financial institutions are now in the early stages of reorganizing to focus on payments, investing in image applications and bringing together disciplines to create a more robust operating environment," she said. "Looking ahead, financial institutions will create payment services tailored to unique requirements of communities of inter-

est; conducting straight through processing of multiple payment types; automating and strategic sourcing to increase value, quality, and cost; embedding payment risk management and authorization at the point of presentment; and expanding products and services to leverage customer-valued information as an extension of transactions."

She acknowledged that while all financial institutions believe it is important to break down payment silos, only half have embedded or are attempting to fully embed enterprise risk in their risk initiatives. Citing a study conducted by the Aite Group of 10 of the top 50 banks, she noted that 80 percent of anti-fraud units report to a single manager and 90 percent do not centralize fraud detection on a single platform. Yet, 90 percent believe that centralized processing is necessary.

Driving Factors

Massie suggested that both legislation and regulation are the key drivers that necessitate the move to an enterprise approach to fighting fraud. On the national level, provisions of the Patriot Act, Gramm-Leach-Bliley Act, and the OCC Banking Circular 35 (disaster recovery) require financial institutions to have a full view of their payments from an enterprise level. On the global level, financial institutions are affected by the Basel II Accord (risk-based capital backing) and Sarbanes-Oxley 404 (disclosure and certification). In past eras, financial institutions addressed fraud and risk on their own terms. In today's highly charged environment, much of the choice that financial institutions enjoyed has been taken away; timelines for compliance are no longer exclusively under the control of financial institutions.

Another driver highlighted was the growing risk of financial loss. Attempts to defraud and losses from fraud are increasing, as are the types of fraud being perpetrated. She warned that as the massive transformation of payments continues (with financial institutions on the leading edge), larger risk gaps are exposed, creating opportunities for fraudsters to fill those gaps. Every loss or compromise deepens customer distrust of the system, damages reputations, and risks crippling fines. In addition, the publicity galvanizes legislators and regulators, a situation that compounds the loss of control and creates greater uncertainty.

Critical Imperatives and Possibilities

Massie recommended that banks consider multiple agendas with almost every initiative they undertake. She suggested that the critical items on each agenda will frequently merge:

- **Agenda one.** How does this initiative affect our ultimate goal of merging our separate payment silos into a single, integrated payment business?

- **Agenda two.** What risk control points does this initiative affect, open up, or cross paths with? How does it create new risk that we need to manage?

To illustrate her point, she posed a series of questions:

- What are the imperatives and possibilities for financial institutions as they seek to manage their migration to enterprise payments and risk while improving customer service and profitability? How do financial institutions challenge the growing perception that payments are synonymous with risk?

- How does a financial institution protect revenue as it manages the two agendas? If revenue can't be protected, how will it be replaced? Will financial institutions need to reinvent a product to sustain the revenue stream?

- How does a financial institution match the pace of change between the two agendas when they overlap? What happens, for example, with an image archive when you add a new partner and start exchanging image files? Or if a financial institution converts its checks to ACH, does it create a new risk management control point that checks ACH files for stop payments?

In general she noted that "financial institutions that undertake this new way of looking at payments and risk will raise many new questions, the answers to which will be different depending on the customer segments they're dealing with, the particular strategy involved, the payments infrastructure, and the risk management approach and technology."

Tandem Migration

Massie asserted that the key is to balance the tandem migration of payments and fraud/risk consider-

ations to achieve the goal of a fully integrated payment system. She suggested the following tangible actions to achieve this goal:

- **Lay a scalable, sustainable enterprise foundation.** Leveraging existing infrastructure, focus on a modular customer-centric approach that supports consistent access to all payment channels.

- **Lift business knowledge.** Where is the knowledge base within the financial institution? What are the dynamics of processing transactions? Financial institutions should integrate what they know and do best into the new process.

- **Identify quick wins.** Where will changes have the greatest impact? Financial institutions should set priorities and target quick wins to deliver maximum value.

- **Make sure it works for both risk and payments.** Again, using the example of converting checks to ACH: What are the fraud-related processes and checkpoints that normally occur in check payments that now need to be seamlessly wound into ACH payments? However, as Massie explained, it can be more complicated. For example, what if a customer requests a wire transfer but does so over the website? It's critical that financial institutions manage the wire risk as effectively as the online risk (or vice versa) and that they maintain consistency across both channels. Otherwise, they may be leaving a door open for an enterprising crook, trained to spot just such inconsistencies. Or what if a financial institution's client elects to do corporate capture at its own site? The financial institution/client contract probably still calls for the financial institution to verify signatures and large-item transactions, but now the information isn't on the financial institution's system; it's on the client's. What new risk control points have been opened? How will the financial institution ensure that overall risk protection is not diminished?

Conclusion

Massie concluded her remarks by advising that "in the process of balancing the migration of enterprise payments and enterprise risk, only the fittest will survive. And to be the fittest requires careful, planned management of the payments and risk marathons as in-step partners in the race. The process is challenging, but it is an unprecedented opportunity to reinvent and rebuild."

Identity Fraud and the Internet: The Best Defense and the Best Offense

Moderator: ***James Van Dyke,*** Founder and Principal, Javelin Strategy & Research
Panelists: ***Ravi Aurora,*** Vice President, Security and Risk Services, MasterCard International
Katherine Claypool, Senior Vice President, eCommerce, Bank of America
Lisa Robinson, Vice President/Manager, Risk Management and Compliance, Wells Fargo

Summary: *This session drew on one of the nation's most comprehensive studies of identity fraud and addressed strategies for prevention, detection, and resolution. It also explored the Internet as a tool that can promote account security and how banks can use this tool to generate greater customer satisfaction, service, and loyalty.*

James Van Dyke opened the session using a sports analogy. If the Philadelphia Eagles play only defense, they have no chance of winning; the *best* the team can do is achieve a tie. In the world of identity fraud, if financial institutions only play defense with the goal of protecting assets, they forgo both increased safety *and* growth available through the Internet. To win, the industry must take a fresh look at the Internet—with a clear sense of how to integrate customer relations, marketing, and risk management.

According to research conducted by Javelin Strategy & Research, the primary method of identity theft (among known-cause cases) is a lost or stolen checkbook or credit card (28.8 percent). The next most common methods are friends, family, and acquaintances with access to personal information (11.4 percent); corrupt employees (8.7 percent); non-Internet purchases (8.7 percent); and mail fraud (8 percent). Computer spyware, Internet transactions, computer viruses/hackers, and phishing *collectively* account for 11.6 percent of identity theft.

The same study showed that using electronic means to monitor account activity results in signifi-

cantly lower losses when fraud occurs: $551 for accounts monitored via ATMs, the Internet, or other electronic means *versus* $4,543 for accounts monitored using paper statements.

Van Dyke cautioned that in a world with growing threats, the Internet can offer tremendous advantages, but those advantages don't happen by themselves. As is the case with any delivery channel, the financial institution must be aware of the Internet's inherent safety advantages (such as the ability to eliminate access to paper delivered through the U.S. mail and faster detection of fraud).

Challenges to Combating Fraud and Identity Theft on the Internet

Ravi Aurora

In his formal remarks, Aurora emphasized that identity fraud places an organization's reputation and brand at stake and erodes consumer confidence in e-commerce and online banking. He suggested that fraudsters challenge the abilities of legitimate organizations to combat Internet-based fraud and identity theft by using a combination of:

- Social engineering and technical complexities to exploit browser weaknesses, resulting in fraud schemes such as phishing.

- Legitimate technologies hijacked for the purpose of gaining access to personal data on poorly protected computers to gain access to personal data.

- Varying degrees of tolerance for e-crimes among law enforcement agencies and prosecutors.

He suggested that dealing effectively with Internet fraud and identity theft requires a "judicious blend of 'coopetition' [cooperation + competition] to go after fraudsters." It also requires industrywide implementation of stronger, uniform security protocols, using two- or three-layer authentication methods. The protocol must include authentication of who you are, something you have, and something you know.

In addition, he advised the industry to take collective action in the following areas:

- **E-mail toolbars.** Enhanced e-mail tools can alert consumers when they are receiving a suspicious message.

- **ISP content monitoring.** If ISPs were more vigilant in monitoring all aspects of the application process at enrollment, more risk could be averted before damage is done.

- **Consumer education.** Many organizations have done a good job of educating consumers on the risks involved in Internet use, but more can be done to produce clear, up-to-date, and complete communications.

- **Internet browser enhancements.** Enhancements are needed to warn customers of risks and prevent specific crimes (such as pharming or phraming).

He described MasterCard's three key initiatives to combat Internet fraud and identity theft:

- **SecureCode.** A secret code that helps consumers protect against unauthorized use of their cards when shopping online at participating merchants.

- **Site Data Protection.** Minimizes criminal access to consumer payment data at merchants, processors, and elsewhere.

- **Operation StopIT.** An effort to close down websites that sell or share stolen credit card information for phishing or spoofing sites that trick consumers into divulging confidential information. (In the last year MasterCard has shut down 1,700 phishing sites.)

Customer Responsibility

Lisa Robinson

Robinson asserted that a partnership between businesses and customers is needed to make online banking and purchasing safe. Also needed is education that uses "clear and concise communications," to help customers recognize and adopt safe behaviors and to reinforce messages from financial institutions that, as confirmed in the Javelin research, online banking is safe. To give customers total assurance in this area, Wells Fargo offers an "online guarantee," so that customers "don't need to worry that their money is at risk."

According to Robinson, online financial tools can help customers protect themselves from various types of fraud. Wells Fargo offers such tools, including:

- **Online banking.** Allow customers to monitor transactions for unusual activity.

- **Bill pay.** Use e-bills to lower risk of mail fraud.

- **Online statements.** Eliminate paper statements and reduce risk of mail fraud and proactively monitor transactional activity.

Keystroke Logging Is the Greatest Online Threat

Katherine Claypool

Claypool reported that the biggest fraud threats, according to Bank of America's loss history, continue to be "new customers" and "family and friends."

The "most odious online threat" to security is keystroke logging, not the more obvious phishing and spoofing, she noted. Focus groups conducted by Bank of America show that consumers have become increasingly savvy about phishing and spoofing scams, recognizing that communications are a little "off the mark," and not falling for them. On the other hand, customers are not "practicing good computer hygiene" to protect themselves from keystroke logging, resulting in a significant growth in scams that rely on data stolen through illicit monitoring.

She noted that in focus groups, consumers *say* they update their protection every week; in reality, most have allowed 60 days or more to elapse since their last update. Some consumers believe that it's the bank's job to protect their computers from infiltration. A large part of consumer education must be directed at fighting this perception and encouraging consumers to take ownership.

Various reports have indicated that some 40 percent of customers who do not use online banking service have serious concerns about security. What will it take to move them online? Bank of America believes that it will take guarantees and assurances that the bank is protecting them. To address these issues, Bank of America recently rolled out SiteKey, a PassMark Security product, which will be mandatory for online customers by year-end. This security feature uses a customer-selected image that appears when customers log in. If they don't see that image, they're not dealing with Bank of America. If they log on from a computer that the bank normally doesn't associate with them, the bank asks a challenge question to verify their identity. Claypool added that while many customers don't necessarily understand how this technology works, they understand that it enhances security and view it positively.

According to Claypool, the reality is that customers have spoken and they want to use the web. As proof, she noted that Bank of America processes more transactions through its websites than its banking centers. "The channel is here and there are security issues that the industry must deal with," she concluded.

Discussion

Building Relationships with ISPs Is Key

In an online relationship, the customer, the financial institution, and the Internet service provider (ISP) are all points of vulnerability. Customers cannot be compelled to take actions to protect against fraud, and while financial institutions are aggressively working to do what they can do, a key area in which defenses can be shored up is the ISPs. But there is a growing sense of optimism on this front: Conference participants noted increased cooperation among the ISPs, which have begun to realize that they must make certain their networks are safe.

Need for Cross-Industry Partnerships

If any organization is compromised, everyone in the payments chain suffers. There is a compelling need for consortia to share information. For example, Microsoft sponsors a financial services industry group that includes 11 major banks and Internet providers. The members of that group coordinate their approach to fraud detection, thus helping to ensure that Microsoft and financial service providers are synchronized in terms of combating online fraud.

Leading financial institutions are supporting significant initiatives to thwart phishing. Now, however, fraudsters are "moving downstream" to attack smaller financial institutions, which may be less able to respond appropriately. Much of the work to combat phishing so far has been done individually; the next step must be to work collectively to protect smaller industry participants. As one participant emphasized, "If one financial institution is hurt, all are hurt."

Difficulty of Legislative/Regulatory Solutions

One difficulty with relying on U.S. legal or regulatory solutions to force institutions to act responsibly is that the problem is not restricted to the United

States. One participant claimed that the majority of attacks now originate offshore, particularly in Eastern Europe and Asia. Attacks that originate in the United States can usually be shut down quickly. There is little or nothing that U.S. legislation or regulation can do to get to the root of the problem globally.

There has been a dramatic shift in where ISPs are located. One participant asserted that last year 80 percent were in North America; now the fraction in North America is 40 percent, and 60 percent operate overseas. Much of this is likely due to the global spread of Internet usage, but many of the new providers are in jurisdictions with limited law enforcement agencies, suggesting increased criminal intent. Adding to the even greater complexity of global enforcement in the future will be the fact that in a world of about 6.4 billion people, 13 percent have Internet access. As computers get less expensive and Internet access becomes more widely available, fraud will likely worsen, creating even more challenges for law enforcement worldwide.

Self-Policing

Other comments indicated that the financial services industry must get tougher with companies that broker information. Some are very reputable, but others are guilty of misrepresentation. GLBA is clear about financial institutions' responsibilities, and some participants asserted that there is a need to extend these responsibilities to others in the information business with access to sensitive data.

What Can (and Cannot) Be Done?

Suggestions for the industry included:

- Communicate the benefits of real-time information to customers and help customers become accustomed to working through the Internet.
- Figure out a way to share accountability with customers, who have been spoiled by legal protections that shield the consumer from damages. Consumers want financial institutions to take away all the risk, but people must be willing and motivated to protect themselves.
- Begin educating youth through school programs that focus on banking.
- Work with ISPs and Microsoft.
- Recognize that there is no silver bullet that will fix the problems associated with electronic payments. The only option is to work together to send consistent messages, such as: If you don't know who is sending an e-mail, don't download it!

Checks: How to Manage the Risk When the Paper Disappears

Moderator: ***Blake Prichard,*** Executive Vice President, Federal Reserve Bank of Philadelphia

Panelists: ***Susan Robertson,*** Assistant Vice President, Retail Payments Office, Federal Reserve Bank of Atlanta
Louise L. Roseman, Director, Division of Reserve Bank Operations and Payment Systems, Federal Reserve Board of Governors
Sydney Smith Hicks, President, VECTORsgi

Summary: *Checks are being replaced by electronic payments. While almost everyone acknowledges the many benefits of moving from a paper-based payment system to a faster, more efficient electronic one, the shift significantly alters the risk environment for financial institutions. Laws and risk management techniques hammered out over decades to provide security in a paper-based environment do not necessarily translate into the electronic world. As check replacement products continue to grow in usage and popularity, how will they affect risk?*

Check 21

Louise Roseman

Roseman set the stage for her remarks by suggesting that it's important to consider three key points when examining the evolution of Check 21:

- **Trends in electronic payment usage.** For noncash retail payments, electronic payments now exceed check payments.
- **What Check 21 does and does not do.** Check 21 authorizes substitute checks, in effect substituting paper for paper. Although Check 21 *does not authorize* electronic payment, which is still accomplished only by agreement among the parties, it *facilitates*

electronic payments by allowing banks to truncate original checks.

- **Early Check 21 experiences.** Check 21 took effect on October 28, 2004, with the strong support of Congress and the financial industry. (The legislation received no negative votes.) No banks are required to use the authority granted under Check 21, but banks are free to do so according to their business interests.

In June 2005, the Reserve Banks processed approximately 600,000 checks daily under Check 21, about 1 percent of checks collected and 10 percent of dollars.[2] To date, the demand to deposit checks electronically has been stronger than the demand to receive image presentments. Why aren't more banks using Check 21? In some cases, the business case is not yet there; technology investments, including systems and software, must be made to leverage the authority. Software is a challenge: bugs are still being worked out. Roseman noted that the slow and steady start has allowed all parties to work through new processes and make appropriate adjustments that might not have been possible with a full cutover on day one.

Check 21 Risks

Roseman then turned her attention to the risks posed by Check 21:

- **Duplicate checks.** There is only one original check, but once the original check is truncated, multiple images or multiple substitute checks could exist. Banks must ensure that they have internal controls to prevent the transfer of duplicate items.

- **Physical security features.** Many original checks have built-in security features, such as watermarks or micro-printing, that don't survive the transition to substitute checks. Roseman expects that better, image-survivable security features will likely be created in the future. Examples include seal encoding and 2D bar encoding.

- **Nonbank truncation.** A bank may give customers the right to truncate checks, but the risk must be evaluated. For example, if a bank permits its nonbank customer to create substitute checks, it must provide the associated Check 21 warranties on behalf of the customer.

Under Check 21, the bank that creates the substitute check generally bears the liability. The idea is that since the bank is realizing the benefit, it should be responsible for internalizing the risk. If a bank incurs a loss from a substitute check that it wouldn't have incurred with a paper check, it may pass through the loss to the bank that created the substitute check.

Expectations

In terms of what the industry could expect as a result of Check 21, Roseman indicated that the declining number of checks has already caused a reduction in the number of Reserve Bank check processing locations. In 2002, there were 45 locations. By the end of 2006, there will be fewer than half that number. The "tipping point" for Check 21 will occur between 2007 and 2010, she suggested. By that time, a substantial number of banks will have made the investment in in-house technology or formed arrangements through service providers to deposit and accept checks electronically. She expects that this will lead to a substantial restructuring of physical transportation networks. Unpaid checks that are handled electronically will be returned to the depository bank faster, but others that continue to be handled in paper form may take longer to return.

Roseman noted that projections with a longer timeline are more speculative and "a topic of spirited debate within the Fed." She offered her own personal prediction, which she emphasized is not an official Fed position: A decade from now, Reserve Banks will only handle checks electronically, and any checks that continue to be cleared in paper form will be cleared outside the Federal Reserve.

She also offered the following potential implications of this scenario:

- One Federal Reserve check processing region.

- All checks nationwide will be deemed local checks, subject to a two-day maximum hold period.

- Unpaid checks will be returned to depository

[2] The numbers cited by Roseman were accurate at the time of presentation. Check 21 volume has increased since June 2005.

banks faster, but not fast enough to protect depository banks from fraud risk.

Conclusion

"Over time Check 21 should lead to a much more electronic and efficient check collection system," Roseman concluded. "This change will be evolutionary, not revolutionary, with the transition being market driven. The transition will reduce some risks, while increasing others. And, at the end of the day, check collection will be similar to ACH—with pictures."

Assessing ACH Risk and Solutions

Susan Robertson

Robertson indicated that the Federal Reserve will soon launch a new service to assist originating depository financial institutions (ODFIs) to mitigate their fraud exposure by monitoring and controlling third-party and originator access to the ACH network.

Background

Addressing the origin of the new service, she noted that a series of meetings with bankers, followed by nationwide focus groups and consultations with advisory groups, identified ACH-related risk as a potential "hidden iceberg" for financial institutions. There was strong consensus among meeting and focus group participants that it is appropriate and desirable for the Fed to play a role in mitigating ACH risk. On the basis of these findings, the Fed, which provides operator services to more than 21,000 ACH participants and processes two-thirds of forward commercial ACH volume, determined that it could and should address risk mitigation, consistent with its role as an ACH operator.

According to Robertson, the relatively new ACH WEB (Internet-initiated) and TEL (telephone-initiated) services are key areas of risk for ODFIs, since they are the ones responsible for warranting the validity of ACH transactions.

FedACH Risk Origination Monitoring Service

Robertson reported that in response to these key risk areas, the Fed created and tested the FedACH Risk Origination Monitoring Service. The service enables ODFIs to determine:

- Which originators it wants to monitor (e.g., originators operating in high-risk businesses, with a high percentage of returns or high activity/dollar volumes, and with poor audit results)

- The monitoring criteria (e.g., daily caps, batch caps, or number of debits) it wants to employ

ODFIs enter the monitoring criteria to the FedACH Information Services via FedLine Web or FedLine Advantage™ and send files to FedACH Services to conduct risk monitoring at the batch level or within the FedACH application. The Fed responds with near real-time e-mail notices of pended batches to the ODFI. The ODFI takes action on the pended batches, either rejecting or releasing via FedACH. The batches remaining at the end of the day are processed or rejected according to the end-of-day default. Service features include:

- ODFIs administer their own risk management criteria and may select from a variety of service options.

- Pre-set criteria include debit and/or credit caps for one or more originators across ODFI RTM, end-of-day default to either reject or process batches, and monitoring over process day or exposure days.

- ODFIs determine in near real time whether to process or reject pended batches.

- E-mail notification of pended batches may be accessed by multiple recipients.

"The risk service, which is expected to be in full production in the first quarter of 2006, is available to any bank that originates ACH payments processed by FedACH Services," Robinson noted. "Participating in the service is independent of the bank's ACH operator relationship. It is a value-added, priced service, and its use is not mandatory."

A Changing Risk Environment

Sydney Smith Hicks

Hicks characterized Check 21 as "the biggest operational change in payment processing since the introduction of the MICR line" and suggested that Check 21 will change the payments risk model in significant ways:

- **New process risk.** Distributed capture, the biggest

operational change enabled by Check 21, will enable lower cost geographic expansion but will alter check fraud dynamics, initially increasing risks (new operators, new physical locations, new backup plans, new customers), but ultimately decreasing risk as reengineered processes are introduced. Day 2 processes will move into Day 1.

- **New product risk.** Hicks anticipated that image replacement documents (IRDs) will be used more often in the early stages of Check 21 adoption, since some banks will not be able to accept electronic presentment. The creation of IRDs, or substitute checks, means that the creating bank provides warranties and indemnification, unless responsibilities are shifted by agreements among the parties. Faced with this risk, banks creating IRDs/substitute checks, Hicks argued, should consider strengthening account agreements and installing systems to detect duplicate items.

Changing Risk

During the last decade, she noted, financial institutions have invested millions of dollars each year to address check fraud; yet, fraud losses have remained stable during the past several years and are still a significant problem. Losses for large banks have trended downward as they have deployed technology. Fraud losses are not trending downward at smaller banks.

Hicks identified the major types of check fraud (kiting, counterfeit checks, alterations, forged endorsements, forged signatures, NSF/uncollected funds, closed accounts, and stop payments) and suggested that Check 21 will alter the dynamics of four of these types: counterfeit checks, alterations, forged endorsements, and forged signatures. While some analysts suggest that kiting will go away, she suggested the reality is that the existing paper process will work more slowly as banks cut back on the frequency of courier pickups. As a result of the uneven implementation of Check 21 and the slower movement of the paper, losses from kiting—in the short term—may increase, as kiters move to banks that adopt Check 21 more slowly.

Hicks predicted that the adoption of Check 21 will have a variety of consequences in terms of preventing check fraud. In some situations, Check 21 offers a positive advantage on existing techniques; in others it is neutral; and in some situations it makes check fraud prevention more difficult:

- **Positive effect.** The following techniques become more effective with the use of images. In the case of positive pay, the payee's name can be verified from the image and compared to the issue file. Images processed at the teller line can be verified immediately before cash leaves the teller station. Reverse positive pay (where the customer monitors the items before they are paid) is possible due to the ease of making images available online. Immediate scanning of images combined with new processing algorithms will make fraud detection quicker and more effective for a larger number of items:
  - Rules-based system for on-us items
  - Rules-based system for deposited items
  - Signature verification
  - Positive pay
  - Reverse positive pay
  - Image-based fraud detection

- **Neutral effect:**
  - MICR detection
  - Shared account information databases
  - New account opening/tracking

- **Negative effect.** Physical security properties of paper checks do not carry over to an IRD or imaged environment. These features include thermochromatic ink, copy void pantographs, watermarks, laid line, microprinting, and chemical reactive papers.

Other Risk Mitigation Enhancements

Hicks also indicated that Check 21 offers additional risk mitigation benefits not available in traditional paper check-based processing:

- **Anti-money laundering.** The technology that makes it possible to recognize handwriting on a check makes it possible to compare the payee information on a check to the OFAC list to enable identification, tracking, research, and documentation.

- **Immediately available images.** Because images are available immediately, research into check kiting activities can take place on a more timely basis.

The Biggest Change in 30 Years

Hicks concluded her remarks by summarizing her views on the long-term effects of Check 21:

- Traditional process clearing times may increase as dedicated plane transportation arrangements are cancelled, increasing the risks to old processes and products.
- Distributed processing is the new reality, with the ability to move into new markets.
- Movement into new markets means more classic "know your customer" challenges.
- There are significant new processes to manage.
- The increased availability of images gives bankers new powers to reengineer and mitigate fraud risks.

Data and Information Security: It's More Than Money

Moderator: ***Rahul Gupta,*** Senior Vice President, Risk Management, EFT Delivery Services, eFunds

Panelists: ***Tom Kellermann,*** Senior Data Risk Management Specialist, World Bank
Mark MacCarthy, Senior Vice President, Visa USA
Stuart Pratt, President, Consumer Data Industry Association

Summary: *Data and information are never more secure than the weakest link in the access chain. In the highly interconnected and competitive world of payments processing, that access chain is large and growing. Not all players stand ready to accept their responsibility to adequately safeguard the data and information they use and collect. Real industry-initiated solutions are needed to provide security and protect the reputation of the industry and its individual members.*

As a launching point for a discussion on data and information security, moderator Rahul Gupta framed the topic and the issues by asserting that data today are the equivalent of gold and currency in old economies. Much is protected, but much isn't—especially data that are accessible because of the Internet and the interconnectedness of financial institutions, processors, and other service providers. The central issues of data and information security are access control and where the internal and external gaps are.

Gupta identified the types of data relevant to this discussion as:

Sensitive Personal Information

- Customer's name
- Address
- Telephone number
- Social Security number
- Taxpayer ID number
- Driver's license number

Sensitive Account Information

- Consumer's credit card number
- Debit card number
- Other financial account numbers

Sensitive data are maintained—and lost—by a variety of organizations, including government, service entities (such as universities and hospitals), financial services organizations, payments networks, and third-party service providers (such as data brokers and credit reporting agencies).

Gupta said that data may be lost in a host of ways through a variety of channels:

- **ATM.** Skimming, employee theft, trapping.
- **Internet/PC.** Phishing, spamming, hacking.
- **Physical.** Dumpster diving, employee theft, mail theft, contractor theft.
- **POS.** Skimming, employee theft.
- **Wireless.** Spamming, employee theft, trapping.

Although data loss does not necessarily translate into fraudulent events, it sets the stage for illicit activities, including fraudulent account openings, counterfeiting, accessing consumer data, and altering data. Although the direct correlation between data loss and fraud is never known, it is known that data loss has been on the increase and so has fraud. To emphasize the point, he noted that:

- Identity theft is the number one growth crime, according to the FBI.

- Computer crime has increased 3,600 percent since 1997.

- 19.3 million people in the United States have been the victims of identity theft during the past two years.

- 57 percent of hack attacks target banks.

- 83 percent of financial institutions experienced a compromise last year.

- Reported computer intrusions at U.S. banks increased five-fold during 2003.

According to Gupta, one of the many serious implications of the increase in data loss and fraudulent activities is the loss of consumer trust in online systems. Companies pay a price for security breaches. The *Wall Street Journal* studied 14 companies in which a breach occurred. In 10 out of 14, the stock price declined an average of 3.3 percent the day after the breach became public and was down an average of 5.0 percent in the weeks and months following—a real loss to stockholders. As noted in an earlier panel, there are known relationships between identity theft, drug running, and organized crime—leading to further reputational loss for organizations and increased consumer mistrust of the financial system.

What is the industry's response to the challenge of securing data?

Gupta offered the eFunds board of directors as an example of the industry's concern for data security, indicating that it "wants direct reports on data security—not just around physical and logical access control, but also organizational control, ownership, best practices for employees, and vetting customers and vendors.

"Businesses are just beginning to deal with these issues, particularly focusing on *who* within the organization is accountable," he continued. "Solutions will emerge as businesses create the right incentive structures and as the right legislation is put in place. On a scale of one to 10, the industry is only at a one or two in terms of doing what needs to be done to protect data."

At the conclusion of his remarks, Gupta directed questions to the panelists:

- **What is the government doing with respect to data security?**

  Mark MacCarthy noted that many organizations that save sensitive consumer data are not covered by the requirements of the Gramm-Leach-Bliley Act (GLBA), as financial institutions and others in financial services are. A key legislative goal is to make security and safekeeping requirements uniform across the board, because the reality is that some merchants and processors do not live up to the rules in place.

  He also noted that nonsecure businesses are an obvious target for criminal organizations, "The companies have already aggregated the data they're after."

  Stuart Pratt reiterated MacCarthy's concern about the "unevenness" of the regulatory environment; some data aggregators are covered by GLBA and the Fair Credit Reporting Act, and some are not. He noted that a name, address, and Social Security number are "different from what they used to be." They're now accessible on the web and are not commonly used on their own to verify identity.

- **What are the key gaps in data security?**

  Tom Kellermann identified key gaps in securing data:

  - **Identity management.** In e-finance, financial institutions face the challenge of knowing the parties with whom they're doing business.

  - **Factor identity not in place.** Too often senior management is not aware of what the CIO is doing, and the company's activities are creating opportunities for data loss and putting the company's reputation on the line.

  - **Dynamic information security policies.** Again, too often they are not in place.

  - **Wireless.** Wireless and the use of wireless in e-brokerage are highly problematical, creating an increase in online e-brokerage fraud.

- **Can you comment on internal risk and employee theft?**

  MacCarthy indicated that Visa shares its security rules, including employee requirements and controls, with other entities to promote a secure environment, but employees always present a point of vulnerability. In addition, one of the key sources of internal risk is saving data. Some merchants save data, including security data, without knowing they're doing it; they do it because the software they purchased was designed that way. Vendors know how to fix this vulnerability and are now developing software that does not save inappropriate data, but legacy systems remain—creating a large, ongoing problem. Visa mandates that security codes not be saved; going forward, it will require merchants and processors to use point-of-sale software applications that do not save security codes. It's essential to gain the cooperation of merchants and processors to combat internal risk and employee theft.

  Kellermann noted that 70 percent of computer fraud is internal, but one out of every three computers is compromised. The real problem is not the employee, but the digital outsider. According to an OECD study, one out of every three computers is hijacked. These zombie PCs allow hackers to infiltrate secure enclaves and siphon out personal data and access controls. The way to address this situation is to mandate two-factor authentication, as defined by the FDIC and the OCC; to continually conduct penetration and vulnerability assessments; and to be proactive in addressing software vulnerabilities. He also noted that PCs that have been compromised present an ongoing problem because old worms create backdoor tunnels. Most of today's worms reverse-engineer backdoors created in systems by yesterday's malicious code. This phenomenon is possible because most organizations do not hunt for the backdoors placed in systems as a result of electronic intrusion.

  Pratt elaborated on the threat presented by digital insiders, expressing his concern for background screening standards and practices, as well as the private sector's inability to access criminal records to use in the evaluation of potential employees.

- **Are there national security issues involved?**

  Pratt responded that identity validation is a homeland security issue. The Real ID Act of 2005—which proposes standardized, electronically readable driver's licenses—is supposed to solve all identity-related issues in the United States. But, he noted, it also raises fears about ushering in what amounts to a national ID card and creating a false sense of security because it eliminates other forms of identification.

  MacCarthy noted that the FDIC is pushing for federal guidance on two-factor identification (such as including an image for online validation), focusing on preventing phishing. Is the person who is coming back to your financial institution the person you enrolled? He added that while it may seem to be unattractive to be subject to agency mandates, the industry appears to be moving in that direction.

Discussion

The follow-up discussion focused on whether security issues had become so overwhelming that the industry should move away from the magnetic stripe as the standard for card-based transactions. A variety of viewpoints related to this and other issues were offered by panelists and the audience:

- **Mark MacCarthy:** Neural networks complement magnetic stripe cards to significantly enhance security. Does a cost-benefit analysis indicate that there is enough of an advantage to put in new devices at the point of sale?

- **Richard Parry:** The issue is more fundamental. In the UK, the vast majority of financial institutions are issuers and acquirers, enabling them to see the payments business holistically. Ever since issuers and acquirers have been fragmented in the United States, the acquirer wags the dog. A change in interchange is needed to drive positive change.

- **Ron Congemi:** The only way to accomplish what needs to be done is to provide incentives.

- **Paul Tomasofsky:** The issue is what the industry as a whole will pay for the transaction—issuers, acquirers, consumers, and merchants. If the level of risk reaches an unacceptably high level, business

margins will come down. In an environment with falling margins, costs associated with increased losses caused by inadequate risk mitigation eat into the dwindling profit margins. The lower margin players will exit the business, while the well-run ones will thrive. Effective, efficient risk mitigation by the survivors will become a sustainable competitive advantage.

Best Practices: Industry Sector Recommendations for a Secure Electronic Payment Environment

Moderator: ***Jean Bruesewitz,*** Senior Vice President, Visa USA

Panelists: ***Ron Congemi,*** Senior Vice President, Strategic Industry Relations, FDC
Robb Evans, Managing Director, Account and Risk Solutions, eFunds
Richard Parry, Senior Vice President, JPMorganChase
Rodman K. Reef, Chairman & CEO, Citishare Corp., a Citigroup subsidiary

Summary: *In this culminating session, five industry experts—representing different parts of the electronic payments industry—offered best practices to secure the system. Although segments were addressed individually, all agreed on the need for enterprise-based risk management to create overall payments security.*

Signature-Based Debit Products

Jean Bruesewitz

Bruesewitz noted that electronic payments offer consumers incredible convenience and financial institutions the opportunity to generate incremental income. They also present significant new challenges to the industry in the form of new types of fraud. Effective risk management has always been an important part of the banking equation, and today it is even more critical to preserve consumer confidence in the system. While, as an industry, we have made many advances in risk management, there continues to be room for improvement.

Then and Now

"How has the proliferation of electronic payments changed the risk environment?" Bruesewitz asked. In the past, risk management was relatively straightforward. There was a single demand deposit account (DDA) and a single access device—the check. Multi-day processing provided a cushion of time in which to detect and deter fraud. Today's environment is exceedingly more complex. There is still one DDA, but it may be accessed in many ways: paper checks, checks converted at the point of sale, check cards, ATMs, ACH debits, and online banking and bill payment. Electronic processing reduces or eliminates the processing time cushion and the virtual world presents its own set of risks.

She noted that in the 21st century, consumers are taking advantage of the convenience of all the ways they can access their accounts. Debit continues to grow in all of its manifestations, as do card-not-present and e-commerce transactions. Check use continues to decline, and fraudsters continue to attempt to exploit the payments system. Electronic payments are a natural target for several reasons. First, improved fraud detection in older channels encourages fraudsters to pursue opportunities in new channels. Second, technology provides fraudsters with tools to attack the payments system in new ways, such as hacking and phishing.

Evolving Fraud Detection Needs

Bruesewitz contended that to remain effective, fraud detection must evolve to address today's challenges. This requires moving beyond identifying fraud simply at the transaction and account levels (as neural networks do quite effectively) and creating capabilities to detect fraud horizontally—across the payment system—*at the event level*. For example, if fraud detection focuses *only* on the account level, a $1 fraud might go unnoticed—even if that fraud is perpetrated against 40 million accounts. If fraud detection expands at the event level, it is possible to identify a $1 fraud perpetrated 40 millions times based on a change in activity among a large number of accounts.

Visa is building a new risk management infrastructure that addresses both payments system risk and account risk. A significant part of the new infrastructure is identifying the "first instance of fraud," the initial fraud transaction (prior to the pattern of fraud developing), and "single ping fraud," a single instance of fraud within an account. Visa has introduced significant new capabilities that allow decisions to be made in real time and that add risk intelligence to all of the authorizations processed through VisaNet.

Debit Best Practices

Bruesewitz highlighted debit best practices for issuers, including:

- Using application risk tools to support new account processes.
- Maintaining an effective card distribution and activation process.
- Providing an online authentication program such as Verified by Visa.
- Actively managing cardholder authorizations:
  - Continuously updating balance files.
  - Using expiration date/CVV/CVV2 in decisions about authorization.
  - Using fraud detection tools.
  - Managing stand-in parameters.
- Implementing effective fraud case management and loss recovery practices.
- Tracking fraud and report fraud internally, to your processor, and to your card organizations.

Pin-Based Products

Ron Congemi

"Fraud has not gone away, but it's moved—to the second, third, and fourth tier financial institutions," asserted Congemi. "Large organizations—such as eFunds, FDC, and Visa—have moved as fast as they can and have taken on as much as they can to address fraud, but it's not a fair fight. All we can do is try to keep up the best we can." The worm in the apple analogy is a good one, he noted. "You can get rid of the worm, but you can't patch up the damage that was done—particularly when that damage involves reputational loss.

"If the industry doesn't think that fraud is a problem, the consumer certainly does—with the press sensationalizing every event," he contended. "The industry can't be satisfied with fraud at five basis points, because that's five basis points of a huge pie. The absolute dollar figure we're talking about is large enough to justify an investment in change."

Identity Theft

According to Congemi, identify theft and identity-related fraud continue to grow: Approximately 14 million adults reported instances of identity theft in 2004, up from 12 million in 2003. When consumers were asked when identity theft occurred, their responses have been consistent over several years' time, suggesting that identity theft continues despite efforts to combat it.

He identified frauds that contribute to identity theft:

- **Phishing.** Approximately 43 percent of adults (about 91 million) have received a phishing e-mail or phone call. An estimated 5 percent of consumers contacted by phishing fraudsters provided the requested personal information. Forty-five percent of victimized adults (approximately 2 million) report that the personal information provided was used to make an unauthorized transaction, open an account, or commit another type of identity theft. In the first quarter of 2005, the instances of phishing far exceeded the total for all of 2004.
- **Skimming.** Skimming—when cards are compromised by devices that read and record magnetic stripe and, possibly, PIN information—also continues to threaten consumers' identities and accounts. Skimming devices include PC-based systems, which are readily available for sale, that can be connected to POS terminals and counterfeit or compromised ATMs.

Best Practices

Congemi offered suggestions for what financial institutions can do to protect themselves and customers from PIN-based fraud:

- Operate cameras at all ATMs.
- Monitor ATM activity:
  - Card reader and dispenser errors.
  - PIN entry timeouts.
  - Changes in transaction patterns.
  - No transaction activity periods.
- Perform daily physical inspections of branch ATMs.
- Tell consumers to contact their financial institution if they suspect phishing or ATM tampering.

- Perform due diligence on nonbank-owned ATMs.
- Use card-based PIN offsets and validate offsets in the authorization process.
- Check CVV/CVC during authorization of PIN transactions and monitor CVV mismatch activity.
- Use neural network fraud detection systems.
- Report fraud.
- Conduct velocity checks on bad PIN transactions.
- Implement a card activation process.
- Confirm address changes.
- Separate card and PIN mailers.
- Don't use PIN for VRU or online banking.

Educate Customers to Reduce Victimization

"Most important," Congemi concluded, "provide education to help consumers identify fraudulent schemes *before* they're victimized."

ACH Transactions

Robb Evans

As check use is declining, payment transactions are being moved into a variety of alternative vehicles, such as debit cards, electronic bill presentment and payment (EBPP), and check conversion (not substitution) at the point of sale, stated Evans. The latter two are examples of new payment vehicles that have necessitated development of new types of ACH payments, creating a hybrid situation from a risk management point of view. He argued that it is incumbent on all members of the industry to work together to manage these new payment types and their associated risk.

Organizational Silos Deter Effective Risk Management

Evans contended that although financial institutions have done a good job at combating fraud, they've done it within organizational silos, creating an inefficient process that increases costs, fails to leverage fraud-related lessons, and encourages fraudsters to focus attention on the weakest part of the system. Banks have a unique opportunity to use this transition period from paper to electronic processing to begin managing fraud on an enterprise level by:

- Integrating siloed payments processing and fraud management infrastructure.
- Managing data across the entire account and transaction life cycle.
- Integrating internal and external sources of data and analytics for making decisions in real time.
- Investing in real-time solutions and flexible infrastructure.
- Automating back-office manual processes to integrate more effectively with front office.
- Migrating operations gradually to mitigate costs, balancing the risks and rewards of technology change.

Framework for Success

Evans noted that many parties are involved in any ACH payment transaction: the originator, banks (ODFI and RDFI), receiver, and possibly other processing intermediaries. Each plays an integral role in handling the payment; each has an opportunity and the responsibility to manage the risk associated with that payment; and each has certain obligations under NACHA rules. Effective measures for meeting these obligations and using industry best practices lead to a solid and secure payments framework. New payment types have created a need for each entity to go a step beyond what was required for handling traditional ACH payments, such as direct deposit of payroll, and recurring debit transactions, such as insurance premiums. As payment usage grows in both breadth and depth, increased diligence is required to address increased payment risk.

ACH Best Practices: New Payment Types

Evans identified ACH best practices for new payment types:

- **WEB/TEL (Internet- and Telephone-Initiated Entries).** Consumer-initiated transactions via the phone and the Internet continue to grow. Often

these payments are single-usage payments (e.g., to make a purchase). The nonrecurring nature of the transaction and the relative anonymity of the initiator create additional potential risk.

  - **Obligations of Originators.** Agreement with ODFIs; authorization requirements; risk management, including implementing a fraudulent-transaction detection system, verifying routing numbers, providing security to Internet session, auditing website security.

  - **Responsibilities of ODFIs.** Agreements with originators, provision of warranties and liabilities, and formatting requirements.

- **ARC (Accounts Receivable Check Conversion).** The conversion of consumer-to-biller remittance payments in lockbox operations has created tremendous new volume of ACH payments. The volume and hybrid nature of these transactions (originated as paper checks written by consumers, converted into electronic ACH items by the billers) create additional potential risk:

  - Provide biller/bank with additional risk mitigation by reducing exposure created by re-opening credit lines based on fraudulent payments (bust-out fraud).

- **BOC (Back-Office Check Conversion).** NACHA is exploring/piloting a way for merchants to convert checks received at the point-of-sale into electronic ACH items. Like ARC, this form of check conversion would generate new volume of a hybrid nature into the ACH network, thereby creating potential new risk.

  - Place holds on funds pending presentment.

  - Hold the resubmission of a returned item until the merchant has verified that the funds are in the consumer's account.

  - Conduct risk-weighted transaction scoring to identify the relative risk of an item and to use as parameters in determining how to clear the item.

  - Consider offering a service to merchants to address the "unknown" MICR lines, i.e., those not found in databases currently used to verify checks.

In summary, Evans argued that these new payment types may actually reduce the total risk in the financial system because, in many cases, ACH payments—by nature of their speed of collection—create less risk than checks and other payment alternatives. Nonetheless, the convergence of payment media and the growth of the ACH network as a primary medium require all entities handling ACH transactions (as an originator, receiver, or payment intermediary) to enhance their ACH risk mitigation processes.

Exercise the Model

Rodman Reef

According to Reef, one of the most critical—and often overlooked—elements of safeguarding the integrity of electronic payments is for all participants to know the rules and to follow through by complying with or enforcing the rules, as appropriate. The governance structure is important to fraud prevention.

"The electronic payments business is interesting because sometimes organizations that make the rules don't operate the system," he stated. "In the recent CardSystems security breach, for example, banks were not named in the press releases— Visa and MasterCard were. But Visa and MasterCard didn't hire that processor; they had agreements with the banks that hired CardSystems and did not have a direct way to enforce the rules, which was the responsibility of the banks."

He argued that it is the responsibility of payment system operators to hold participants accountable: Ensure that all direct members actively pursue their roles and provide direction about "what is expected" and "how it is measured." If a bank is participating directly in a payment system, it must know its responsibilities and those of the other participants. In addition, users of a payment system must understand each participant's role.

"As the financial services industry explores every opportunity to reduce fraud," he concluded, "it must understand that problems can be avoided if all participants know the rules, exercise the model, and perform the roles that they have accepted for their organizations."

Financial Institutions

Richard Parry

Parry indicated that it is necessary for financial services firms to think about risk systematically and to think about risk as a process that can be made better at every juncture.

"How you define fraud—the cause, the effect, and the remedy—is also important, because your definition of fraud determines how you will fix it. Bad definitions can lead you to attempt to solve the wrong problem," he continued. "When the industry addresses payment risk, there are hundreds of problems to be solved: Some need to be fixed in granular ways, some tactically, some through policy oversight, and some through systems. There must be a whole framework of control; there is no silver bullet from any vendor."

Parry reiterated the frequently heard complaint, "Your data is out there," and advised the industry "to get over it," because it is irresponsible to manage risk under any other assumption. "In this business, there is always another risk coming along," he suggested. "Getting hypertension over it doesn't accomplish anything. Defect analysis is critical to developing focused solutions to well-understood problems. To conduct defect analysis properly requires experienced professionals with comprehensive skills in risk management, process, operations, audit, and computer security. Fraud must be managed and measured. The prevailing standard of security will always be breached in time, as the technology to build it becomes cheaper and more accessible to those who seek to breach it. Thus, it's a process of constant and relentless improvement."

The "Gold Standard" Lock on the Door

Parry asked the audience to assume that the "gold standard" lock is on the door to financial data. Then, he asked two questions and elaborated on the significance of the questions:

- "How do we know to whom we are giving the keys if there is no way of uniquely identifying the parties?" It's not just a question of being entitled to access, but how do we know that the person with the key is the person to whom it was issued.

- "How do we know if that person is who he claims to be?" Identity (the person our mothers know us to be) is too readily confused with identification (a credential that identifies us for society's purposes, including payments, billing, and settlements) and authentication (a means by which we can prove that we are entitled to have access to something or to be somewhere).

Parry contended that the industry has an authentication problem in need of a solution. "And it's more than a technology challenge; the industry must balance the individual consumer's rights and need for privacy against society's, and our institutions need to differentiate themselves from each other."

To date, no two-factor identification solution is ready for prime time, according to Parry. Most solutions only address one product or channel, not the multiple channel/multiple product relationships that are identity critical.

Means, Motive, and Opportunity

Parry suggested that the "means, motive, opportunity" mantra of criminal attorneys is instructive in looking at alternative approaches to mitigating losses and protecting customers:

- Means. Using people's identity characteristics (impersonation).

- Motive. Get money!

- Opportunity. No foolproof method of tying "identity" to the real person.

"Motive" provides insight into opportunities for remedies, he posited. Thieves steal because they can and because there's a gain to be had. Making it more difficult to steal money—even if thieves get in the door or gain access to data—reduces risk and protects customers. Also, when banks close one door, criminals seek to enter through another by changing their product/channel target, method, location, or targeted financial institution. Therefore, he argued, focusing risk management techniques, such as aberrant behavior monitoring, at the customer level rather than the product or channel level offers many advantages.

According to Parry, in the absence of a more robust infrastructure to control identity, the objective must be to stop money from leaving the bank. "The mouse click does not mean that the money is out of the bank," he stated. The money usually moves only

after the transaction has been loaded in a batch file for subsequent processing, much as it has for over 40 years. Parry believes that this provides an opportunity for monitoring behavior at the customer level to potentially stop fraud before a loss is realized.

However, as more banks adopt more robust controls, banks with weaker controls will be attacked—driven by the age-old doctrine of the path of least resistance. But what happens to smaller banks that can't afford robust controls? "The industry can ill afford banks that may not have the expertise or resources to manage risk adequately declaring that the sky is falling," he stated. Phishing, he noted, is a good example. It's an important risk, but it's only social engineering with a neat delivery channel. And it's only one of the many risks we're contending with at any given time. Many banks address phishing with a combination of controls: a robust process for responding to fraud or attempted fraud, internal transaction controls, collaboration with one another and with law enforcement, and customer awareness training, thus ensuring that the impact is modest.

Monitoring Aberrant Transactions

Financial institutions want robust, long-term remedies to identity, enrollment, and authentication challenges, Parry contended, but they must recognize that all solutions are fallible and have limited effectiveness over time. The behavior models currently in use, primarily to stop credit card fraud, offer many "backstop opportunities while some promising emerging vendor solutions mature. Let's quit straightening the deck chairs on the Titanic and look out for the iceberg," he concluded.

Conclusion

The conference's timely discussion of electronic payment risk in the 21st century especially benefited from the wide-ranging experiences and perspectives of the participants—panelists, moderators, and attendees.

Two key points were evident throughout the day-and-a-half of discourse:

The industry is engaged in managing electronic payments risk. Stakeholders in electronic payments are keenly aware of the risks associated with electronic payments and have taken significant actions to mitigate these risks, including working with third parties, such as merchants and processors, to reinforce security requirements and best practices at every level of exposure.

The industry has taken a proactive approach to electronic payments risk, recognizing that:

- The system is no more secure than its weakest link.

- Effective risk management is a cornerstone to maintaining trust in the payments system.

Many at the conference argued that the industry must also discard its traditional "silo" approach to payments risk in favor of a more holistic management process. Holistic management includes addressing risk both on an enterprise level and across business relationships. Although some organizations have taken initial steps toward holistic risk management of electronic payments, most believe that the transition is in a nascent state.

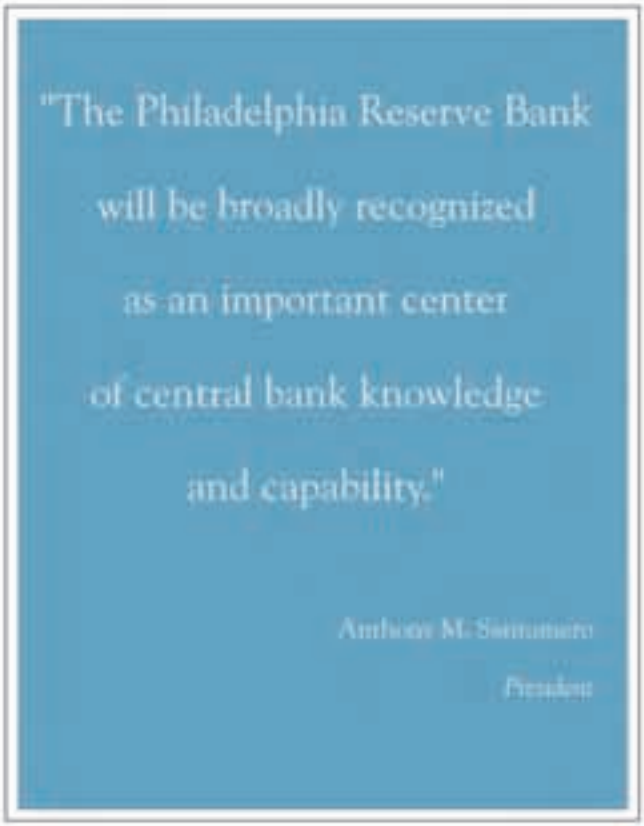
More must be done. At the same time many participants emphasized the dynamic nature of security management. Managing electronic payments risk is a job without an end because it continually evolves. Just as faster, cheaper, more powerful technology supports the ability of the financial services industry to expand products and electronify processes, it also provides fraudsters with more potent tools to attack systems. All fraud-fighting solutions must be regarded as temporary.

Participants generally argued that authentication processes must become more robust. They debated—but did not resolve—the issue of whether more robust infrastructure involves modifying existing magnetic stripe and PIN-based technologies or a significant re-engineering of the infrastructure to support other technologies, such as smart cards.

A further challenge cited by a number of participants is the increasing globalization of payment fraud. Because electronic payments are borderless, traditional protections provided by government are less meaningful. A significant amount of fraud in the U.S. electronic payments system originates from outside the country. Attention is needed to eliminate safe havens for electronic fraudsters anywhere in the world. This need is particularly compelling in light of the potential for electronic payment fraud, including money laundering, to contribute to drug trafficking and international terrorism.

Electronic payments have proven their value to all payment stakeholders, including the financial services industry, businesses, government, and consumers. In reality, 21st century commerce could not survive

without the highly efficient electronified systems that have evolved during the last decades. As many people at the conference emphasized, consumers have confidence in electronic payments and have embraced the convenience and flexibility afforded by the many innovations. As such, it is incumbent on all industry participants to recognize the risks of losing consumer confidence if we fail to better manage the security risks that have emerged.



PAYMENT CARDS *Center*

FEDERAL RESERVE BANK OF PHILADELPHIA

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 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.