Payments Fraud: Perception Versus Reality—A conference summary

Tiffany Gates and Katy Jacob

An overview of payments fraud

Payments fraud can be broadly defined as any activity that uses information from any type of payments transaction for unlawful gain. Such fraud can be perpetrated on any type of payments device, including credit and debit cards, cash, checks, online or mobile payments, and automated clearinghouse (ACH) transactions. Payments fraud can be committed knowingly by a consumer (first-party fraud), or consumers can be victimized by fraudsters operating within financial institutions or as part of criminal enterprises (third-party fraud). Payments fraud has received extensive attention in the popular press and in public policy venues recently, and the payments industry is fighting the perception that fraud is now occurring at unmanageable levels. While there has been increasing emphasis on all types of payments fraud, fraud perpetrated by criminals has received special attention of late.[1]

Fraud is a very real threat to the payments system's efficiency. According to one recent report, 71 percent of surveyed organizations experienced payments fraud in 2007, and over one-third of those firms reported financial losses stemming from the fraudulent activity.[2] As another example of the size of the payments fraud problem, in a 2007 data breach involving TJX Companies Inc. (the holding company of retailers T. J. Maxx, Marshalls, Winners, HomeGoods, TK Maxx, A. J. Wright, and HomeSense), 45,700,000 credit card and debit card account numbers were stolen, along with 455,000 merchandise return records containing customer names and driver's license numbers. Latest reports allege that an additional 48 million people have been affected for a total of over 30 percent of the entire U.S. population. The situation has cost TJX Companies Inc. more than $130 million in settlement claims. The breach was a worldwide effort perpetrated by criminals from the United States, Eastern Europe, and China. The U.S. Department of Justice has arrested 11 people in this case, which is the largest hacking and identity theft case ever prosecuted by the department.[3]

As more payments become electronic, the size and scope of payments fraud has grown, in part because the relevant parties in a payments transaction do not know one another. Information about those parties is vital to prevent fraud and enable legitimate transactions. However, as innovations in payments technology have made authentication of information more reliable, other technological innovations have made that information more widely available and subject to abuse. Fraud such as counterfeiting or check forgery has always had a global reach. However, payments fraud used to be much more reliant on physical connections between parties, such as the theft of an individual checkbook or credit card.

Today, modern databases, online information sharing, and increased access points have opened up opportunities for sophisticated criminal gangs to perpetrate fraud from remote corners of the globe. Further, the growing presence of nonbanks and third-party service providers means that regulated financial institutions must consider the security of those providers. At the same time, new laws and standards are being developed for payment activities and instruments. While the continual refining of systems and rules arguably makes payments easier and more efficient, the fast pace of change can compound fraud potential as fraudsters hunt to exploit the weakest link in the emerging systems.

In this complex environment, market participants and governments must determine whether new payment

Tiffany Gates is a supervision analyst in the Banking Supervision and Regulation Department at the Federal Reserve Bank of Chicago. Katy Jacob is a research specialist in the Financial Markets Group at the Federal Reserve Bank of Chicago. *The authors thank the Chicago Fed's payments team for their help in producing this article.*

types carry excessive fraud risk; who is liable when payments fraud occurs; how losses are allocated; what consumer protections should be in place; how notification of fraud should be handled; and how standards should be defined to minimize the incidence of fraud. It is a tall order, but payments providers must also identify consumers whom they have never met and authorize electronic transactions from which they might be far removed. And, increasingly, they must do this in real time.

To explore the problem of payments fraud, the Federal Reserve Bank of Chicago organized its eighth annual Payments Conference around the topic. The conference, Payments Fraud: Perception Versus Reality, took place on June 5–6, 2008.[4] In this article, we summarize the conference and focus on the following themes: why the industry is worried about payments fraud; managing fraud risks; the impact of technology and innovation on fraud; responsibilities and incentives for fraud prevention; and public sector involvement in mitigating payments fraud. We note that market participants agree that payments fraud cannot be eliminated without risking the viability of certain payment channels, but also find that close industry collaboration, properly aligned incentives, technological innovations, and active risk management can lessen fraud's ill effects.

Why worry about payments fraud?

Fraud degrades operational performance and increases cost—not only for the parties to the transactions whose payments are disrupted, but also for the payments system as a whole. Indeed, payments networks are vulnerable to fraud at any point in a payments chain, and fraudsters often attempt to exploit the weakest link in that chain. One of the foremost concerns is the potential for a single data breach or compromise to disrupt an entire payments system. According to conference panelist Jeff Schmidt, an independent consultant, it is possible for a single data breach to affect multiple layers in the payments system and disrupt the efficient operation of the entire system if confidence in the system is lost.

Further, Mark Greene, Fair Isaac Corporation, raised the possibility of a mass compromise of significant components of the U.S. payments industry. Greene said that the industry is not prepared for a mass attack wherein fraudsters target multiple companies simultaneously through hacking and sophisticated phishing techniques.[5] These threats have the potential not only to harm a financial institution but also to degrade the payments system globally. Bruce Summers, a payments system and technology management consultant, questioned whether the marketplace alone could contain fraud and protect the payments system as a whole if such a mass compromise were to occur. Indeed, Allison Edwards, Fiserv EFT, commented that the payments industry was completely caught off guard by the aforementioned 2007 TJX Companies data breach because of its size and scope.

It is important to note that there is a distinction in the payments industry between actual fraud that has been perpetrated and potential fraud from compromised information that might not necessarily result in criminal activity. Ellen Richey, Visa Inc., claimed that the number of compromise incidents in the United States is rising, while other analysts contend that only the reporting of these incidents is increasing. Regardless of the magnitude of growth, industry leaders are concerned about both stopping compromises from occurring and ensuring that significant fraud does not take place when compromises do occur. Conference panelists maintained that when such fraud happens, consumer confidence can only be restored by a fast and thorough industry response.

Managing fraud risks

As it stands, many in the industry find it difficult to gauge the full impact of fraud on the payments system. Richey applauded the payments industry for doing a good job in stemming the tide of increasing fraud attacks, stating that global fraud rates in the card industry have remained largely constant since 2002. Others at the conference argued that, while the total amount of fraud has gone down, the impact of the fraud that does occur has become more costly to society. Summers commented that many in the payments industry argue that today's level of fraud protection is sufficient, and noted that few market participants seem dissatisfied with the overall state of payments fraud. Some players view fraud as just another cost of doing business, though according to several conference participants, that view is being overshadowed by an urgent need to keep fraud under control.[6]

According to David Poe, of Edgar, Dunn, and Company, many payments participants often make suboptimal risk-management business decisions because the true cost of fraud is misunderstood. Most analysts only take account of fraud losses to issuers (banks that issue payment cards to consumers or businesses) when tallying fraud costs. Poe noted that the monthly benchmarks for issuers' fraud losses are approximately 0.07–0.08 percent of transaction volumes. Fraud losses to acquirers (banks that process card payments for merchants) from chargebacks are also of about the same magnitude. Poe echoed Greene by noting that statistics on issuers' credit card losses from first-party fraud showed that fraud could account for as much as 10 percent of their credit losses if correctly categorized.

Moreover, opportunity cost—where consumers pass up one payment option or company in favor of another because of perceived security concerns—is arguably the biggest cost of fraud and the most difficult to quantify. It is the largest potential risk in that customers might not use a payment product at all, or might not use the product in the appropriate way, because they do not trust that the payment instrument is secure.

When determining the true cost of payments fraud, analysts sometimes also fail to count the cost borne by issuers, acquirers, and merchants to *manage* fraud risks. Bob Ledig, of Fried, Frank, Harris, Shriver, and Jacobson LLP, stated that the costs of fraud cannot be limited to direct costs borne by any one party in the payments system. Rather, resource, compliance, enforcement, reputation, and litigation costs must also be taken into consideration. He noted that data security should be an inherent part of the payments vehicle, rather than a separate line of business. These comments about the true price of payments fraud raise the possibility that there may be some type of market failure in the payments system, wherein the nature of fraud is so complex that firms are unable to price it correctly.

To keep costs down and to better manage the risk associated with payment channels and instruments, financial institutions are looking to incorporate an enterprise-wide approach to fraud management. Challenges arise because lines of business have historically been developed as independent silos. Judith Rinearson, of Bryan Cave LLP, stressed that payments laws and regulations have largely emerged around individual product lines, making it difficult to implement enterprise-wide solutions. Many audience members commented that small merchants also struggle to implement enterprise-wide solutions, as they lack the resources to obtain high-end fraud prevention tools. The transition to an enterprise-wide approach to fraud mitigation is driven by governance and culture. Conference participants felt that the comparative handful of organizations that have appointed "payment czars" have been more effective in looking at payments fraud across the institution as a whole. Yet, if an institution has a deeply siloed governance and organizational structure, it is difficult to develop consistent, cost-efficient business processes across different product lines.

Greene urged the industry to take note of the "balloon effect" in payments fraud. Namely, once fraud begins to decrease in one payment method, criminals often shift focus to another part of the payments system, where fraud rates begin to rise. Audience members commented that fraud might also shift among regions or nations. Some speculated that the increasing use of chip and PIN (personal identification number) technology in Europe and Canada might lead criminals in those countries to focus on countries that rely more heavily on older magnetic stripe technology, such as the United States. These different types of fraud shifts could lead to misperceptions about what is truly occurring in the system as a whole, and they are especially important to consider when new payments technologies enter the market.

Payments technology and innovation

On the one hand, technological innovations have enabled market participants to authenticate payments information more accurately in real time, greatly enhancing the security of electronic payments transactions. On the other hand, the speed of payments innovation can accelerate fraud risks. Traditionally, the payments industry has been slow to manage technology, while fraudsters have quickly adapted to the new channels available. Poe reinforced the idea that technology has made fraud easier to commit on a wide scale, citing the increases in phishing, pharming, skimming, and other fraud tactics that often rely on remote or card-not-present transactions.[7]

According to Kevin Fu, University of Massachusetts Amherst, phishing is one of the biggest security problems on the Internet. It is certainly the easiest way a spammer (one who uses electronic messaging systems to indiscriminately send unsolicited bulk messages) can infiltrate thousands or millions of compromised machines around the world. If just a tiny fraction of the people spammed respond, the spammer can obtain quite a bit of sensitive information that can be used to perpetrate fraud. Richey went further by saying that the top vulnerabilities in the payments system are the storing of prohibited data; out-of-date security systems; perimeter security; weak wireless security systems; and structured query language (SQL) injection attacks.[8] These vulnerabilities can only be addressed if every participant in the payments system is accountable and vigilant about protecting data, upgrading systems, and monitoring its own staff and its partner firms. However, upgrading software and infrastructure can be quite costly. In some cases, technology enhancements happen so quickly that companies, especially small merchants and processors, have little time to react.

Consumer perceptions of fraud risks can also directly impact the success of a new payment method. Greene noted that consumers' perception that mobile and contactless payments are more prone to fraud has apparently stunted the growth of those payment channels in the United States. Mobile payments are payments that are initiated by a mobile device, such as a mobile phone.[9] A contactless payment device, such

as a card or fob, uses radio frequency identification (RFID) or near field communication (NFC) technology to make secure payments. The embedded chip and antenna enable consumers to wave their payment device over a reader at the point of sale. Both RFID and NFC payment methods are relatively new in the U.S. market, and it should be noted that it often takes time for consumers to adopt any new instrument or market. Bruce Cundiff, Javelin Strategy and Research, echoed the sentiment that risk adversely affects consumer adoption of these new payment instruments. Because repairing the damage done by payments fraud is becoming more complex for consumers, many are reluctant to switch to a new payment method. For example, in a recent Javelin survey, 65 percent of those who said they did not want to use contactless cards named security fears as the number one reason, and 33 percent of those surveyed viewed mobile banking as too risky.[10]

Cundiff pointed out a marked change in the way that consumers perceive the security efforts of their financial institutions. Consumers now want to be more engaged in security measures and view companies that allow them to be engaged through account alerts or verification calls as being more reliable. Rinearson agreed, arguing that many consumers are confused about fraud prevention features of different payment cards, such as prepaid cards[11] versus debit or credit cards. For example, consumers might find out about fraudulent transactions from billing statements for their debit cards or credit cards, but would not have such information for a number of prepaid cards.

Payments fraud can affect the availability of new products as well. Payments providers might be hesitant to innovate in an area where unknown fraud risks exist. Paul Tomasofsky, Two Sparrows Consulting LLC, said that the newly emerging decoupled debit field faces challenges as issuers work out several potential risks. A decoupled debit card is a debit card issued by a nonbank or bank that is linked to a demand deposit account that the issuer does not own. The payments are processed on the automated clearinghouse network, are typically co-branded with a particular merchant, and may include other options such as a credit feature or reward program.[12] Tomasofsky pointed out that issuers need to thoroughly authenticate both the user of the card and the user's checking account to verify that they are in fact linked. Issuers, moreover, run the risk of the account holder having nonsufficient funds because they aren't able to check deposit account balances directly. It is also unclear who will be responsible for handling dispute resolution for decoupled debit cards. While relatively low merchant fees may make these cards attractive to the merchant community, their slow start suggests that some of these perceived risks might be impeding their adoption.

Online payments also face numerous threats from payments fraud. Steve Malphrus, Board of Governors of the Federal Reserve System, noted that fraud is more prevalent in online transactions than in person-to-person transactions. According to Bob West, Echelon One, there is $2.3 billion–$3.2 billion in online credit card fraud per year, much of which is orchestrated by very sophisticated crime syndicates.[13]

Moreover, even traditional payment forms that are undergoing modernization face new potential fraud risks. For example, David Walker, Electronic Check Clearing House Organization (ECCHO), explained that in check imaging, technology moved much faster than the laws related to handling check fraud issues. While imaging reduces fraud potential over paper checks, industry players are unsure how to interpret their new roles related to risk management. Walker explained how new forms of check fraud have arisen following the introduction of check imaging. These forms of fraud include a greater volume of duplicate checks and images that do not conform to standards set in the Check Clearing for the 21st Century Act.[14] Walker said that many institutions struggle to decide whether imaged checks are authorized and who should receive returned checks.

The increased fraud risk from some technological innovations has even begun to change the way that institutions view new customer relationships for deposit accounts. Malphrus commented on how the increase in remote account opening has created a new set of fraud risks, which can hopefully be managed by increasingly sophisticated authentication technologies. West expanded on this theme by discussing the overall disconnection between the physical and online worlds in payments, stating that this basic problem is with us to stay.

Fraud perpetrators regularly exploit new technologies to their benefit, but payments providers are working to find ways to exploit technology for fraud resolution as well. These firms are incorporating technology into the broader design of their fraud detection mechanisms. Edwards noted that "neural" networks[15] are helping companies to manage their risk profiles more conservatively by adding the elements of time control and customer targeting. Fu discussed the ways that RFID technology in contactless cards and mobile payment devices can allow for sophisticated tracking in order to reduce fraudulent transactions. The RFID tags, which mimic minicomputers and store enormous amounts of data, can mitigate the security risk of handing over your card to someone who may want to compromise the information contained on it.

Greene mentioned the rise of profiling mechanisms that compile fraud patterns for specific merchants as well as in geographically dispersed payment devices and terminals. These mechanisms can be used in adaptive models that keep up with changes in fraud patterns; they allow users to dynamically change model weights to suit their needs. He argued that fraud prevention should not be viewed as providing a competitive advantage for any firm. Otherwise, fraud becomes too great of a collective problem. Fu also supported the use of open source RFID technology rather than the proprietary systems that companies are now pursuing. This idea furthers the notion that collaboration is required to combat fraud in the payments system.

Responsibilities and incentives for fraud prevention

Conference participants noted that, as consumers, merchants, and payments providers struggle with the issue of payments fraud, the goal is not to eliminate fraud but rather to generate better risk-management practices that strike a balance between allowing for risks in the payments system and dictating payments choices. Speakers at the conference were unanimous in the view that collaboration within and among companies is a necessary aspect of successful payments fraud mitigation. Security is expensive to achieve and maintain. Therefore, it can result in indirect but nonetheless real costs to consumers if those costs are transferred. Cooperation is thus not only desirable but also necessary.

According to the conference speakers, in order to be effective, payments fraud mitigation efforts must recognize the need to include all members of the system. To do this, incentives must be properly aligned. Market participants must have sufficient reasons to care about fraud mitigation. For instance, Mallory Duncan, National Retail Federation, argued that we currently have pricing and protection scenarios that encourage customers to use signature-based payment cards rather than PIN-based cards, leading to perverse incentives to use a payment vehicle that is perceived to be less secure. Moreover, banks and merchants often base their preference for different payments mechanisms on narrow cost reasons, thereby overlooking the hidden costs embedded on the security side.

Duncan also noted that if merchants do not feel that they are directly benefiting from increased data security, they will not be willing to pay for new security infrastructure. He said that it is very difficult for merchants to keep up with constantly changing payments rules, as merchants are being asked to handle payments technologies that are outside of their core competencies. Schmidt countered that today all industries face security issues and that compliance is not specific to payments.

Several conference participants suggested that one solution to the problem of data storage standards is to be parsimonious with payments data and store only as little as the law requires. Mark Michelon, Orbitz Worldwide, explained that fraud detection needs to be automated in order for merchants to do it in a cost-effective manner. Richey elaborated by stating that effective authentication can make stolen data useless. Schmidt agreed, noting that there is so much payments data available that fraud solutions should not focus on limiting data but rather on making the data less meaningful. Public disclosure of sensitive data devalues the data for fraudsters and essentially halts the fraud. In other words, if data such as Social Security numbers are not deemed to be highly confidential, the impact of having such data stolen will not be as great. Alternative types of data include addresses or zip codes; according to Richey, these are quite effective authentication tools in many instances.

Schmidt suggested that incentives for fraud prevention should be aligned with responsibility and that potential victims should be given good reasons to care about protecting their own payments data. Several presenters commented on consumers' relative lack of incentives in preventing payments fraud, especially in the credit card market where zero liability policies protect consumers from virtually all losses. Duncan Douglass, of Alston and Bird LLP, argued that there needs to be a realistic price tag placed on risk. Currently, he said, attorneys work with payments system participants to help them decide if paying to eliminate risk is worth the cost. Payment channels rely on customer confidence for survival, but there is a moral hazard problem when customers have little incentive to be careful with data. Michelon stated that one solution to this problem is consumer education about payments fraud and data protection. While these efforts can be useful, in order for them to have meaningful effects, all actors in the payments system must have similar incentives to avoid payments fraud.

Indeed, if fraudsters are to stay in business, it would seem to be in their best interest to avoid creating a situation where a mass compromise would disrupt the payments system as a whole or destroy a specific payment channel that had previously proven lucrative for them. Marsha McClellan, United States Attorney's Office for the Northern District of Illinois, remarked that there should be real consequences for committing payments fraud that are significant enough to make criminals think twice. She stated that it is difficult to prosecute a payments fraud case because

of the electronic nature of the crime, which usually means there is not much physical evidence. Moreover, many consumers have a hard time pinpointing compromised information. McClellan suggested that monetary incentives were the most likely way to deter fraud. United States Attorneys have the authority to seize the proceeds of criminal activity even before prosecutions occur. If funds are seized, criminals lose the ability to continue their operations. However, Sujit Chakravorti, Federal Reserve Bank of Chicago, agreed with Schmidt's point that this type of monetary incentive does not work for irrational actors, such as pedophiles, terrorists, and other perpetrators of payments fraud who are not motivated primarily by financial goals. Clearly, these types of actors present a problem to society that goes far beyond payments. Some argue that the existence of such issues with broad implications for our society leads to the need for public sector intervention in the problem of payments fraud.

The role of the public sector

Payments markets contain strong public-good components. Gene Amromin, Federal Reserve Bank of Chicago,[16] argued that payments services are neither purely public goods nor purely private goods; thus, they are best provided by the private sector but with government oversight. Because of the inherent conflicts of interest, as noted in the previous discussion concerning misaligned incentives, the public sector can help counter information asymmetries by designing proper mechanisms to deter fraud, helping to align incentives to prevent fraud, and providing information to all levels of the payments system about the issue of payments fraud. While government involvement might therefore be seen as a crucial component in combating payments fraud, no clear consensus emerged at the conference on the best specific strategies for doing this.[17]

Charles Docherty, MBNA Canada Bank, offered a perspective on how other nations deal with the role of government in payments fraud. In Canada, where there are fewer financial institutions and the central bank is not an active participant in the payments market, payments issues are largely governed by the private Canadian Payments Association, which consists of credit unions and banks. Docherty argued that in Canada, consumers and payments providers are considered the first line of defense for fighting payments fraud, followed by the government.

In contrast to the payments environment in Canada, in the United States regulatory and legal incentives have always been a central aspect of payments. Christian Johnson, University of Utah S. J. Quinney College of Law,[18] noted that there are four types of laws that directly affect how payments fraud issues are handled (most of them involving the public sector): contracts between payments parties; state laws and regulations; federal laws and regulations; and international laws and treaties. All participants in the payments system must recognize these legal constraints.

Greene highlighted the importance of the government in the extremely crowded and competitive U.S. payments market. He said that the payments industry is concerned that sharing data and strategies related to payments fraud prevention might be viewed as collusive, possibly leading to a need for objective government intervention. Richey noted that by setting uniform rules, the public sector would be in a unique position to get at the root of payments fraud. However, Richey cautioned that too much intervention would stifle innovation. Some audience members argued that a uniform set of standards for all payment channels, governed by one body, would greatly deter payments fraud.

Ledig commented that the recent proposal by U.S. Treasury Secretary Henry M. Paulson, Jr., to give the Federal Reserve more power over all payment forms would be a step toward centralizing payments policy.[19] Charles Evans, president and chief executive officer, Federal Reserve Bank of Chicago, reiterated that one of the key responsibilities of the Federal Reserve is to maintain the integrity of the U.S. payments system. Malphrus suggested that even in the current framework, which does not give the Federal Reserve governance over the entire payments system, the Fed should take up both advisory and participatory roles for that system. Such a role would still let the private market thrive. Some in the audience suggested that the Federal Reserve is in a unique position to advise on payments fraud issues, since it is both a direct participant and an overseer of the payments marketplace. Others, however, argued that these roles could prove conflicting for the Fed. Overall, conference participants seemed to favor a balanced approach of government and central bank intervention with support that would still allow the private market to police itself.

Conclusion

Participants in the conference felt that some level of fraud will always remain: Fraud could be eliminated entirely from the market only by shutting down active payment channels. However, a consensus was reached that the effects of data breaches and information compromises can be minimized through a holistic approach to data security. Such an approach would recognize the importance of cooperation within and across companies and among various actors in the private market. This cooperation would also be advanced by

government actions that are able to bring more uniformity to fraud mitigation without stifling innovation.

Fraud is an ongoing issue in the payments market, and the fast pace of technological change is likely to bring new opportunities for fraud to occur at the same time that it will spur more efficient fraud mitigation solutions. Policy leaders around the globe are struggling to define new rules and expectations of market participants, and industry leaders have different perspectives on the state of payments fraud and its future. The articles included in this volume represent various views on payments fraud from academic and industry speakers at the Federal Reserve Bank of Chicago's 2008 Payments Conference.

NOTES

[1]Identity theft is another aspect of payments fraud. However, when payments information is used to help criminals obtain information about consumers in order to commit identity theft, the crime goes beyond payments. We do not focus on identity theft in this article.

[2]Association for Financial Professionals, 2008, "*2008 AFP Payments Fraud and Control Survey*: Report of survey results," Bethesda, MD, March, available at www.afponline.org/pub/pdf/2008PaymentsFraudandContolSurvey.pdf. The survey includes a variety of types of organizations from merchants and manufacturers to financial institutions to government agencies.

[3]Conspirators obtained the credit card and debit card numbers by hacking into TJX Companies' wireless computer networks. At the time, TJX Companies was in the process of becoming compliant with the Payment Card Industry Data Security Standard (PCI DSS), which defines guidelines for merchants' handling and processing of payment card data in order to prevent card fraud and data breaches. See Brad Stone, 2008, "Global trail of an online crime ring," *New York Times,* August 11, available at www.nytimes.com/2008/08/12/technology/12theft.html. Also see www.privacyrights.org.

[4]For more information, see Katy Jacob and Bruce J. Summers, 2008, "Assessing the landscape of payments fraud," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 252, July.

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

[6]In March 2007, the Federal Reserve Bank of Minneapolis held a roundtable discussion on payments fraud. A variety of market participants and regulators participated in the discussion. At this roundtable, participants revealed varying levels of comfort with the current state of payments fraud. See Board of Governors of the Federal Reserve System, 2007, "A summary of the roundtable discussion on retail payments fraud," report, Washington, DC, July.

[7]Phishing is explained in note 5. During a pharming attack, a hacker tampers with the domain name resolution process so that users might go to the website of a legitimate financial institution and be unknowingly routed to a compromised site, where they reveal their personal information. A skimming device is one that is mounted to an automated teller machine or point-of-sale machine to copy encoded data from the magnetic stripe on the back of a payment card. For more information, see www.spamlaws.com/online-credit-card-fraud.html.

[8]Perimeter security refers to security systems that are developed to stop criminals from getting inside a network or database. In a SQL injection attack, a hacker uses knowledge of the SQL programming language to obtain hidden information in a database or network.

[9]For more on mobile payments, see Katy Jacob, 2007, "Are mobile payments the smart cards of the aughts?," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 240, July.

[10]Bruce Cundiff, 2007, "Online payments forecast: Alternative payments to go mainstream as consumers seek security and convenience," Javelin Strategy and Research, report, September.

[11]Prepaid cards allow users to pay merchants with funds transferred in advance to a prepaid account. For a summary on prepaid cards, see Sujit Chakravorti and Victor Lubasi, 2006, "Payment instrument choice: The case of prepaid cards," *Economic Perspectives*, Federal Reserve Bank of Chicago, Vol. 30, No. 2, Second Quarter, pp. 29–43.

[12]Capital One was the first issuer to develop a decoupled debit card in June 2007. HSBC (Hongkong and Shanghai Banking Corporation), along with Tempo Payments, developed a decoupled debit program in July 2007. See M. Bruno-Britz, 2008, "Rethinking the card business: The evolution of payment cards," *Bank Systems and Technology*, Vol. 45, No. 2, February, pp. 31–35. Also see M. Bruno-Britz, 2007, "Debit cards: Cutting the debit ties," *Bank Systems and Technology*, Vol. 44, No. 11, November, p. 14.

[13]For more information about issues related to online payments fraud, see Thomas P. Brown and Richard A. Epstein, 2008, "Cybersecurity in the payment card industry," *University of Chicago Law Review*, Vol. 75, No. 1, Winter, pp. 203–223.

[14]For some details on the Check Clearing for the 21st Century Act, see www.federalreserve.gov/paymentsystems/truncation/.

[15]A neural network is a system of programs and data structures that mimics the neurons in the human brain. Neural networks "remember" information and data in complex ways. See www.webopedia.com/TERM/N/neural_network.html.

[16]Amromin stood in for William Roberds, Federal Reserve Bank of Atlanta, who was scheduled to moderate the final panel but was unable to attend. For more on Roberds' perspective of payments fraud, see Michele Braun, James McAndrews, William Roberds, and Richard Sullivan, 2008, "Understanding risk management in emerging retail payments," *Economic Policy Review*, Federal Reserve Bank of New York, Vol. 14, No. 2, September, pp. 137–159.

[17]For a more detailed argument for an increased governmental role in payments, see Stacey L. Schreft, 2007, "Risks of identify theft: Can the market protect the payment system?," *Economic Review*, Federal Reserve Bank of Kansas City, Fourth Quarter, pp. 5–40.

[18]Ronald Mann, Columbia Law School, was originally slated to moderate the panel on fraud loss and dispute resolution. Christian Johnson moderated in his absence.

[19]The proposal states: "Treasury recommends the creation of a federal charter for systemically important payment and settlement systems. The Federal Reserve should have primary oversight responsibilities for such systems." See U.S. Department of the Treasury, 2008, *The Department of the Treasury Blueprint for a Modernized Financial Regulatory Structure*, report, Washington, DC, March, available at www.treas.gov/press/releases/reports/Blueprint.pdf.

2008 Payments Conference
Payments Fraud: Perception Versus Reality

Thursday, June 5, 2008

INTRODUCTION AND WELCOME

Gordon Werkema, First Vice President and Chief Operating Officer,
Federal Reserve Bank of Chicago

KEYNOTE SPEECH

Divided We Fall: Fighting Payments Fraud Together
Mark Greene, Chief Executive Officer, Fair Isaac Corporation

IDENTIFYING SECURITY ISSUES IN THE RETAIL PAYMENTS SYSTEM

Moderator: Robert Ledig, Partner, Fried, Frank, Harris, Shriver & Jacobson LLP

Panelists

David Poe, Managing Director, Edgar, Dunn & Company

Ellen Richey, Chief Enterprise Risk Officer, Visa Inc.

Talking Points

What are the main security threats to retail payments?

What are the potential costs of payments fraud and of solutions to guard against it?

What role, if any, should public authorities play to protect payments system participants from these threats?

FRAUD CONTAINMENT

Moderator: Bruce Summers, Payment System and Technology Management Consultant

Panelists

Jeff Schmidt, Consultant

Bob West, Chief Executive Officer, Echelon One

Mallory Duncan, Senior Vice President and General Counsel, National Retail Federation

Talking Points

What are the most common forms of retail payments fraud?

What are the most effective fraud reduction tools, and how have these tools evolved to support "real-time" payments?

How do payment providers and merchants balance fraud risk and consumer convenience?

FRAUD LOSS AND DISPUTE RESOLUTION

Moderator: Christian Johnson, Professor, University of Utah S. J. Quinney College of Law

Panelists

Mark Michelon, Senior Director, E-commerce Risk and Revenue Protection, Orbitz Worldwide

Duncan Douglass, Partner, Alston & Bird LLP

Charles Docherty, Legal Counsel, MBNA Canada Bank

Talking Points

Who is responsible for mitigating fraud in the payments system, and what are the consequences of that responsibility?

How are losses allocated when fraud occurs?

Do current fraud resolution measures distort incentives for payments system participants to adequately secure payment information?

Friday, June 6, 2008

WELCOME AND INTRODUCTION

Daniel G. Sullivan, Senior Vice President and Director of Research, Federal Reserve Bank of Chicago

SECURITY RISKS AND SOLUTIONS IN EMERGING PAYMENT CHANNELS

Moderator: Bruce Cundiff, Director of Payments Research, Javelin Strategy and Research

Panelists

David Walker, President and Chief Executive Officer, Electronic Check Clearing House Organization (ECCHO)

Paul Tomasofsky, President, Two Sparrows Consulting LLC

Kevin Fu, Assistant Professor, University of Massachusetts Amherst

Talking Points

Do new payment channels, such as mobile, electronic images of checks, and decoupled debit, entail different fraud risks?

Are new tools necessary to minimize risks associated with emerging payment platforms?

Do these new channels provide any security features that mitigate risk in the payments system?

KEYNOTE SPEECH

Introduction: Charles L. Evans, President and Chief Executive Officer, Federal Reserve Bank of Chicago

Steve Malphrus, Staff Director for Management, Board of Governors of the Federal Reserve System

PUBLIC AND PRIVATE RESPONSES TO PAYMENTS FRAUD

Moderator: William Roberds, Research Economist and Policy Advisor, Federal Reserve Bank of Atlanta

Panelists

Judith Rinearson, Partner, Bryan Cave LLP

Allison Edwards, Director of Product Development, Fiserv EFT

Marsha McClellan, Chief, Money Laundering and Asset Forfeiture, United States Attorney's Office for the Northern District of Illinois

Talking Points

How can the government define its role in fraud containment without stifling innovation?

Should different payment instruments have similar laws and regulations governing them?

Have standards been an effective tool in combating payments fraud?

CLOSING REMARKS

Sujit Chakravorti, Senior Economist, Federal Reserve Bank of Chicago