A summary of the roundtable discussion on retail payments fraud

The Federal Reserve System's Payments System Policy Advisory Committee (PSPAC) has an ongoing program to discuss payments system developments and barriers to innovation with the payments industry and relevant payments system participants. As part of this program, the committee hosted a roundtable discussion with industry leaders on issues involving fraud in retail payments.[1] The roundtable discussion was held at the Federal Reserve Bank of Minneapolis on March 27, 2007. During the discussion, fourteen industry experts representing depository institutions, corporations, service providers, and law enforcement provided the committee with insights into key areas of concern regarding fraud in retail payments.[2]

Introduction

The roundtable participants agreed that although the current level of payments fraud is being effectively managed and does not represent a crisis, organizations must constantly adapt to keep pace with criminal activity and with changes in technology and the payments landscape. It will never be practical to eradicate fraud completely. Rather, the range of organizations affected by payments fraud need to balance the costs and benefits of fraud prevention. The participants reported that while the dollar amount of fraud relative to business revenues in the U.S. likely is declining, the costs associated with investing in fraud mitigation are substantial and increasing.[3]

---

[1] The Federal Reserve's Payments System Policy Advisory Committee advises the Board on developments in both wholesale and retail payments at a time of significant overall change in the U.S. payments system and helps coordinate Federal Reserve work involving domestic and international payments and settlement systems. The members of the committee are Donald Kohn (chair), Vice Chairman, Board of Governors of the Federal Reserve System; Timothy Geithner, President of the Federal Reserve Bank of New York; Randall Kroszner, Governor, Board of Governors of the Federal Reserve System; Cathy Minehan, President of the Federal Reserve Bank of Boston; Michael Moskow, President of the Federal Reserve Bank of Chicago; Gary Stern, President of the Federal Reserve Bank of Minneapolis; and Kevin Warsh, Governor, Board of Governors of the Federal Reserve System. Patrick Barron, First Vice President of the Federal Reserve Bank of Atlanta, is a liaison member of the committee.

[2] The organizations represented at the roundtable were Bank of America, Comerica, Early Warning Services, Fair Isaac Corporation, First State Bank, Manheim, Mastercard, PayPal, STAR, SuperValu, Two Sparrows Consulting, the U.S. Secret Service, Wal-Mart, and Wells Fargo Bank.

[3] The participants discussed both direct and indirect costs associated with fraud mitigation. Direct costs include resources devoted to purchasing and maintaining fraud-detection and fraud-prevention tools as well as any losses incurred as the result of fraudulent activity. Indirect costs include outlays on customer service in the wake of a fraud event and costs associated with "false positives," which occur when a legitimate payment is erroneously identified as fraudulent.

The participants' discussion of specific issues associated with retail payments fraud covered four overarching topics: (1) the changing landscape of retail payments fraud, (2) current trends, (3) emerging concerns, and (4) areas for improvement in fraud detection and prevention.

The changing landscape of retail payments fraud

The participants reported that, despite waning check use across the country, the largest number of fraud attempts experienced by their organizations remains in check payments.[4] Fraud losses are also highest for checks on a comparative basis with other payment methods. Although the participants did not discuss specific check loss figures, publicly available data confirm this point.[5] A number of participants stated that business losses resulting from check fraud are significantly higher than losses from noncheck payment types because checks are relatively easy to alter or forge using readily available printers, scanners, and computer software.[6]

The participants also discussed how changes in the payments system and in criminal behavior have introduced additional risk into the payments system. One change in the payments system has been the proliferation of commerce conducted over the Internet.[7] The Internet has created new means for criminals to gain access to consumers' personal and financial information and has facilitated the formation of extensive illegal networks through which criminals buy and sell this information without regard to geography. A number of participants noted that substantial Internet fraud operations are now linked to sites located in certain developing countries. The Internet

[4] A 2004 Federal Reserve study on the use of retail payment instruments revealed for the first time that the number of electronic payments in the United States--such as credit card, debit card, and automated clearinghouse (ACH) payments--exceeded check payments. A range of data now indicate that electronic payments have continued to increase and that check payments have continued to decline.

[5] A study conducted in 2006 by the Federal Reserve Board, for example, estimates that the total value of check losses by depository institutions before any recoveries was $1.0 billion in 2005, an increase of approximately $121 million, or 13 percent, from 2004. The Report to the Congress on the Check Clearing for the 21st Century Act of 2003 is available at http://www.federalreserve.gov/boarddocs/RptCongress/check21/check21.pdf.

[6] The participants generally agreed, however, that to date, check losses are at a "manageable" level.

[7] The U.S. Census Bureau estimates that in the fourth quarter of 2006 retail e-commerce sales were $29.3 billion (3.0 percent of total retail sales), an increase of almost 200 percent from $10.0 billion (1.2 percent of total sales) in the fourth quarter of 2001.

has also accelerated information sharing among criminals regarding successful fraudulent schemes; participants noted how quickly new fraud techniques may now move around the country. In addition, the growth in online commerce has lead to an increase in the number of transactions in which merchants are not physically present to authenticate the identity of the purchasers.[8]

Other participants, however, noted that some changes in the payments system have helped reduce risk. Specifically, a number of participants discussed the potentially faster clearing of check payments associated with Check 21 and check-to-ACH conversion.[9] Being able to clear payments more quickly can mean that a fraudulent check may be returned before a collecting bank makes funds available to the depositor. At a minimum, faster returns help provide faster information to banks and their customers that fraud is taking place.[10] These comments were tempered, however, by some views that ACH e-check payments may be more vulnerable to fraud then other ACH standard

[8] To "authenticate" means to verify that purchasers are who they say they are. Authentication is typically a step in a process to determine that the use of a specific payment instrument is authorized. At the physical point of sale, customers using a credit card may authenticate themselves by providing a signature that also authorizes the transaction. Customers using a debit card can authenticate themselves and authorize the transaction by providing a personal identification number (PIN) known only to themselves or by providing a signature.

Some tools used by the industry to respond to this risk include card verification numbers (CVN) and address verification services (AVS). A CVN is the three- or four-digit number found on the back of most major credit cards. This information is not stored on the magnetic stripe of the card or embossed on the front and is therefore not captured through a point-of-sale terminal or imprint machine. The ability of a consumer to provide a valid CVN during an online transaction increases the likelihood that he or she is in possession of the actual card. AVS tools verify that the billing address provided by the consumer matches the address on file with the issuer. AVS protects against an instance when a thief has a credit card number and expiration date but no other identity information about a cardholder.

[9] The Check Clearing for the 21st Century Act (Check 21) became effective in October 2004. Before Check 21, depository institutions had to present the original paper check to a paying bank unless the paying bank had agreed to accept presentment of the check electronically. While Check 21 did not mandate the electronic processing or presentment of checks, it did authorize a new negotiable (paper) instrument, called a substitute check, which is the legal equivalent of the original check. Substitute checks can be presented to a paying bank that requires presentment of paper checks. This enables the electronic processing of checks that previously had to be physically transported from one bank to another.

The term "check-to-ACH conversion" generally refers to transactions that are originated as paper checks but processed over the ACH. These transactions include accounts receivable conversions (ARC), point-of-purchase (POP) transactions, and back-office conversions (BOC). ARC transactions allow billing companies to receive check payments at a "lock box" location, and then use the information from a customer's paper check to create an ACH debit transaction. POP transactions enable businesses to use a paper check as a source document to initiate an ACH transaction at the point of sale. BOC transactions enable businesses to accept checks at the point of sale and convert eligible checks to ACH debits in the businesses' back offices.

[10] See the Report to the Congress on the Check Clearing for the 21st Century Act of 2003 for a review of the effects of Check 21 on the time necessary to present and return checks. The Report is available at http://www.federalreserve.gov/boarddocs/RptCongress/check21/check21.pdf.

entry code categories, notably ACH WEB and ACH TEL. Concerns were also raised by corporate participants that the greater use of check images in the Check 21 environment may reduce the usefulness of some current check security features used by corporations, because those features may not survive when an image is taken of a corporate check.

In addition to changes in the payments system, several participants commented that criminals' ability to adapt to changes in the industry's fraud-detection and fraud-prevention practices is a continuing challenge. Specifically, the participants noted that criminals continue to seek the path of least resistance. As large merchants and banks have developed robust tools to detect and prevent fraud, criminals have increasingly turned to small and medium-sized enterprises because they are less likely to have the resources to dedicate to fraud detection and prevention. Some participants believed that because fraud affects the entire financial industry, it is the duty of larger businesses and banks to reach out to educate and aid these smaller organizations. Some participants also suggested that criminal penalties for fraud should be more significant and prosecution occur more frequently.

Current trends

Several participants highlighted the ongoing importance of protecting consumer information. Citing a number of high-profile breaches recently in the media, a number of participants were concerned about the potential damage to their respective brands' reputations in the event of a data breach.[11] The participants emphasized that this is not a new issue and that the industry has taken steps to protect consumers from fraud that may result from compromised information. Specifically, some participants pointed out that banks and card networks monitor customer accounts that may have been compromised for evidence of fraud and may reissue debit or credit cards when necessary. Others agreed that although the storage of data is a potentially vulnerable point in the

[11] Several data breaches have been discussed in the media recently. For example, on Jan 17, 2007, the T.J. Maxx Company reported that 45.7 million credit and debit card numbers were compromised, along with 455,000 merchandise return records containing customers' driver's license numbers. On March 12, 2007, nearly 9 million pieces of customer information were stolen from Dai Nippon printing company, including names, addresses, and credit card numbers. On February 19, 2007, Stop and Shop Supermarket Company reported the theft of an unknown number of their customers' credit and debit card information, and on January 12, 2007, Moneygram reported that a server containing information on 79,000 bill payment customers was unlawfully accessed using the Internet.

payments system, the extent to which compromised information has actually been used is relatively insignificant. Several participants added that if consumer information is compromised and subsequently used to commit payments fraud, the consumer is frequently not liable for the associated losses.[12] Some participants added that while it is important to protect consumer data, it is equally important to develop tools to prevent the fraudulent use of data or to otherwise render data unusable.

Consumers' personal and financial information can also be divulged through phishing schemes.[13] While several participants cited phishing as a current threat to the security of consumer information, they also believed that the level of actual loss incurred from phishing has been relatively low in aggregate. Some participants noted that the most significant effect of phishing has been damage to their companies' reputations. Others pointed out that when consumers share personal or financial information as the result of phishing schemes, banks often incur costs to prevent fraud on the consumers' accounts even though the bank is not directly responsible for the compromise of the consumer's information. Some participants stated that consumer education has been reasonably effective in preventing consumers from divulging information. Others discussed phishing as an example of the ongoing challenge to security of consumer information, as well as the need to adjust security techniques and educational programs as criminals develop new and increasingly savvy techniques for snaring victims.

In addition, the participants discussed the extent to which the theft and subsequent misuse of consumer information is defined as "payments fraud" or "identity

[12] Regulation E and Regulation Z generally limit a consumer's liability from unauthorized electronic funds transfers or unauthorized credit card transactions to $50 dollars. Consumers are further protected by Visa's and MasterCard's "zero liability" policies, which stipulate that consumers are not liable for losses stemming from the fraudulent use of Visa or MasterCard debit or credit cards. Consumers are also protected from unauthorized check transactions. The Uniform Commercial Code stipulates that consumers are not liable for unauthorized check transactions provided the consumer notifies the bank within a reasonable period.

[13] Phishing involves the fraudulent acquisition and use of an individual's personal or financial information. In a common type of phishing scam individuals receive e-mail messages that appear to have been initiated by their financial institution. These messages may look authentic and often include the institution's logo and marketing slogans. The e-mail messages often describe a situation that requires immediate attention and state that the accounts will be terminated unless the recipients verify their account information immediately by clicking on a provided web link. The web link then takes the e-mail recipients to a screen that asks for personal or financial information including account numbers, Social Security numbers, passwords, place of birth, or other information used to identify the consumers. Those perpetrating the fraud then use this information to access consumers' accounts or assume the consumers' identities.

theft." The participants agreed that both are a crime, but several participants noted that the ramifications of each are substantially different. The Federal Trade Commission (FTC) has defined the term "identity theft" to refer to fraud perpetrated by (1) obtaining access to and illegally using a consumer's existing financial information, such as a credit card number or bank account number, or (2) illicitly obtaining identity information about a consumer to open new financial accounts using the consumer's name.[14] The roundtable participants generally believed that only the second part of the FTC's definition should be considered "identity theft," and that the first part should be considered "payments fraud." Some participants stated that the FTC report used an overly broad definition of identity theft, which has led to an overestimate of the true frequency of this type of fraud and media hype overstating the problem.[15] Other participants emphasized that the consequences of what they consider true identity theft can be very significant for consumers , including having misinformation reported to national credit bureaus.

Emerging concerns

The participants emphasized that criminals are continually searching for weaknesses in fraud-detection fraud-and prevention practices. Several participants said that the potential movement of check-based fraud to the ACH network is an area of growing concern to the industry. A fraudulent payment initiated with a check can move into the ACH system through a point-of-purchase (POP), back-office-conversion (BOC), or accounts-receivable-conversion (ARC) transaction. The ACH was traditionally used for recurring payments from trusted sources. Thus, banks may not yet have in place as many robust tools to detect fraudulent ACH payments as have been built up for check payments.[16] Fraudulent checks that may be detected using existing tools might therefore

[14] The participants referenced the 2003 FTC "Identity Theft Survey Report. The report is available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[15] The 2003 Federal Trade Commission's (FTC's) "Identity Theft Survey Report," stated that there were almost 10 million cases of identity theft in 2003. When considering only the second part of the definition (as provided in the text), identity theft affected about one-third of the 10 million people cited in the report.

[16] Although the participants speculated that the use of POP and BOC could potentially increase retail fraud, a few participants stated that POP transactions have allowed their businesses to detect a fraudulent item more quickly than before. One participant was optimistic that the implementation of BOC may also help mitigate payments fraud through early detection.

go undetected if processed using the ACH network.[17] This possibility is a particular concern to businesses that use check fraud-prevention services, such as positive pay, that are not available for ACH payments.[18] While the participants are concerned about this possibility, they generally agreed that fraud of this nature is, at present, negligible.

The participants also commented that the industry has only recently been monitoring the movement of fraud across payment channels. Some argued that further study is required to understand fully how fraud is moving between paper and electronic instruments or between different electronic instruments. Many participants commented that banks and businesses need to adopt a holistic approach to detecting and preventing retail payments fraud, looking across their different payments systems to gain a complete picture of fraud within their operations. One participant described this as managing fraud at the "relationship" (that is, an individual or a corporate client for a bank; a customer for a merchant) level, rather than the "product" (that is, payment instrument) level.

In addition, the participants discussed how the introduction of new payment instruments could increase fraud in the payments system. Some participants expressed concern over the potential for fraud using open- and closed-loop prepaid or stored-value cards.[19] One participant noted that some of these cards can be easily reloaded with funds and can be used anonymously, making them effective vehicles for money laundering. Another participant posited that open-loop, reloadable prepaid cards could be a primary vehicle for fraud in the future, and other participants concurred that prepaid cards are a growing area of concern. The participants pointed out that businesses

[17] Efforts are underway, however, to develop and implement additional fraud prevention tools and practices for the ACH network. A survey conducted by the Association for Financial Professionals (AFP), for example, reported that in 2006, fourteen percent of the respondents who reported experiencing ACH fraud stated that their banks link their internal check and ACH systems enabling them to detect fraudulent checks converted to ACH.

[18] Many banks offer "positive pay," a fraud-detection service, to their corporate customers. As part of this service, the corporation sends to its bank payment data for checks it has issued. As checks are presented for payment, the corporation's bank validates that the data found on the checks match the information provided by the corporation. If the check data match the data provided, the check is paid. If the data do not match, further investigation is conducted to determine whether the check should be returned unpaid.

[19] "Open-loop" products, such as gift cards, payroll cards, and travel cards, can generally be used at any location that is connected to the particular card network, such as Visa, MasterCard, American Express, or Discover. Although still considered open-system prepaid products, some products restrict where and how the cards may be used. For example, a flexible spending account card can only be used for eligible medical purchases. "Closed-loop" products are limited to a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system.

are beginning to take steps to mitigate these risks. As an example, one participant stated that a large issuer of open-loop prepaid cards has simply exited the market. Another participant added that some businesses now stock their prepaid products behind the customer service desk in order to protect them and others require consumers to register the cards they purchase before the cards can be activated.

The participants discussed the relative safety of two other emerging access devices for initiating payments: handheld devices, such as mobile phones, and contactless cards. A few participants thought that payments made using these devices could be less safe depending on their security features. For example, if a consumer were to lose a typical cell phone, a myriad of personal and financial information could be compromised. Other participants pointed out that the development of security enhancements, such as "dynamic" authorization techniques, for some payment devices can offer significant security enhancements.[20] Some participants posited that the hesitation in trusting emerging payment instruments may stem from the fact that their risks are not yet understood or security features have not yet been widely used. One participant noted that successful payment mechanisms have historically had to put innovative systems into production before a fully mature risk-mitigation strategy has been adopted. Additional security or usability features are often added as the instrument gains widespread adoption and such features become more important.

Areas for improvement in fraud detection and prevention

The roundtable participants shared a number of suggestions for improving the industry's ability to detect and prevent retail payments fraud, including better protecting customers' personal and financial data. Three of the areas discussed were (1) the need for increased industry collaboration and information sharing, (2) the use of enhanced authentication techniques, and (3) the industry's adoption of the Payment Card Initiative (PCI) standards.

Many participants noted that merchants and financial institutions would

[20] A dynamic authorization changes after every transaction. For example, a criminal who obtained information from a contactless card with dynamic authorization functionality but does not physically possess the card, would therefore be able to use the authorization for at most one transaction before it is rendered useless.

benefit from increased collaboration and information sharing. Participants urged payments system participants to share best practices with respect to fraud detection and prevention. Some highlighted the need to increase communication across industries, such as between merchants and banks, while others suggested sharing best practices across payment types. One participant, for example, posited that organizations might observe fraud-mitigation tools that are effective for one payment type such as credit cards, and apply similar cost-appropriate tools to another payment type like the ACH.

Other participants advocated sharing specific data on organizations' experiences with fraud. For example, one participant proposed the creation of a national fraud-notification database containing records of accounts or persons known to have been associated with fraudulent activity. This database would be accessible by both financial institutions and merchants and would enable participating organizations to identify rapidly potential fraudulent transactions. Some participants noted, however, that banks and businesses are reluctant to share proprietary information. Others pointed out that concerns over consumer privacy might prevent banks from sharing this information.[21] Participants also voiced concern that a large repository for consumers' personal and financial information would itself be a likely target for criminals. A few participants encouraged moving beyond the competitive concerns that may dampen interest in sharing information and effective practices.

Some participants emphasized the need not only to detect fraudulent transactions in process, but also to prevent fraud from occurring by improving authentication at the point-of-sale. The participants specifically discussed the effectiveness of two current fraud-prevention tools: PIN and chip technology. Some participants stated that fraud rates on PIN debit cards are significantly lower than those for other payment types and advocated the application of PIN security to card payments in general. Citing widespread adoption of chip technology in other countries, one participant urged the adoption of chip technology as a safer alternative to magnetic stripe

[21] For example, the Gramm-Leach-Bliley Act (GLB), enacted in 1999, addresses the privacy of consumer information held at financial institutions. GLB prohibits financial institutions from sharing nonpublic personal information with nonaffiliated third parties unless financial institutions clearly and conspicuously disclose to their consumers that such information may be disclosed and provide the consumers with ample opportunity to opt out of such disclosure.

technology for card-based transactions.[22] Other participants agreed that chip technology may be effective in mitigating fraud risk, but questioned the cost-effectiveness of the broad-based retrofitting of existing point-of-sale systems with chip readers to accommodate this technology. Emerging payment instruments or access devices such as contactless cards, however, already rely on chip technology and may therefore help facilitate this transition.

The participants also discussed the role of the PCI program, developed jointly by Visa and MasterCard, in protecting consumers' personal and financial information.[23] One participant argued that full compliance with PCI standards will help the industry safeguard consumers' personal and financial information and added that to date there has not been a data breach involving a PCI-compliant organization. Other participants agreed that the PCI program can be helpful in protecting consumers' information but noted difficulties for some organizations to become PCI compliant. Some participants pointed out that completing the steps to become PCI compliant can be complex, costly, and time consuming. The resources required are of particular concern for small and medium-sized organizations with fewer resources to devote to compliance. The participants widely agreed that PCI guidelines are not well understood by small and medium-sized merchants. A few participants suggested simplifying the requirements for small and medium-sized merchants so as to encourage faster adoption of PCI standards. One participant suggested focusing first on a single PCI requirement, noting that preventing merchants from storing consumer information captured at the point of sale would be a significant step towards improving the protection of consumer information.[24] One participant noted that only around 40 percent of merchants are currently PCI compliant.

---

[22] Chip technology enables authentication whereby information unique to the card holder is encrypted in a chip on the card. The information is read from the chip at the point of sale, thereby authenticating the user.

[23] The PCI program prescribes twelve standards for businesses that store or transmit payment card information. These standards were published in 2004 and have been endorsed by several card networks, including American Express and Discover. The PCI Data Security Standards establish four levels of compliance for merchants and three levels of compliance for service providers based primarily on the volume of transactions processed annually.

[24] Another participant explained that some merchants may not be aware that they are storing consumer information at the point of sale. In some instances, the software used to process payments at the point of sale may automatically store this information.

Some participants also noted that the PCI program is a good first step in securing consumer information and discussed additional opportunities to improve data security in general. Some participants observed that protecting consumer information associated with credit and some debit card transactions is important but pointed out that comprehensive programs such as PCI do not exist for other payment mechanisms such as the ACH and certain debit card systems. Other participants stated that existing data privacy regimes generally apply to banks or merchants, but exclude others, such as third-party service providers, with access to significant amount of consumers' personal and financial information. Several participants stated that to improve the security of consumer information, it is desirable to expand data protection regimes with respect to both the types of payments and types of organizations that are included.

Ultimately, participants agreed that criminals will continue to search for the fastest and easiest ways to commit payments fraud. As a result, a majority of participants agreed that fraud-detection and fraud-prevention strategies should be considered holistically so as to not merely shift fraud from one payment channel to another. The participants also emphasized that it is not financially feasible to prevent all payments fraud. Rather, businesses must make prudent, risk-based decisions that will yield appropriate returns relative to the investment required to minimize fraud.

Conclusion

The evolution in the retail payments landscape is continuing to change the way that fraud affects the payments system. Check 21 and check-to-ACH conversion have enabled the faster clearing and settlement of check payments, and the Internet is playing an increasing role in retail commerce. These developments have facilitated more-efficient payment processing and have allowed banks and other businesses to reach a broader customer base. Advances in payments technology, however, also expose the payments system to new avenues for fraud. Specifically, criminals have at their disposal an increasing array of techniques to obtain consumer information and use it fraudulently. Consequently, banks and other businesses continue to invest in tools to combat fraud so that they may benefit from Internet technology and other advances while continuing to safeguard consumers' information and minimize losses from fraudulent transactions. The

participants highlighted the fact that their organizations continue to balance costs and benefits when investing in fraud-mitigation tools.

Several participants suggested ways in which the Federal Reserve might assist the industry's efforts to mitigate fraud. Some encouraged the committee to continue its industry outreach events as a forum for sharing concerns and effective practices, while others emphasized the importance of the Federal Reserve's research on payment and fraud-related issues. As a general matter, however, the participants advocated the continued application of market-driven approaches to keep payments fraud at a manageable level. Payments system participants' ability to adapt to changes in criminal behavior will be critical to maintaining a safe and efficient payments system.