

Chicago Fed Letter

Assessing the landscape of payments fraud

by Katy Jacob, research specialist, and Bruce J. Summers, former director, Federal Reserve Information Technology, and independent consultant on payments systems and technology management

The Federal Reserve Bank of Chicago will host its eighth payments conference on June 5–6, 2008. The conference will highlight threats to the security of the payments system and explore solutions to those challenges. This article previews issues that will be covered at the conference.

For more information on the conference, see www.chicagofed.org/paymentsystems or contact Katy Jacob at (312) 322-2915 or kjacob@frbchi.org.

One of the key roles of the Federal Reserve is to promote the integrity and efficiency of the U.S. payments system.¹ This mission takes on many forms, and encompasses financial services, supervisory activities, the Fed's public policy function, and economic research. The Federal Reserve System provides retail payments services on behalf of the U.S. Department of the Treasury and clearing and settlement services to depositories; helps set payments policy; provides consumer protections; and regulates the payments activities of banks around the country.²

A key component of maintaining the integrity of the payments system includes risk mitigation and fraud management. Since the very first incidents of counterfeit currency, the payments industry has faced a variety of security-related challenges. Concerns related to payments security have escalated in recent years. As payments shift away from paper-based forms toward electronic instruments, consumers face an increasing array of payments options that entail different fraud risks. The Fed plays an active role in identifying new trends in payments fraud and developing effective ways of implementing responses to those trends.

Payments fraud: Past, present, and future

Fraud is a very real threat to the payments system's efficiency, which is measured

by the quality of its operational performance and cost.³ According to one recent survey, 71% of financial institutions reported instances of payments fraud in 2007, and 37% of those firms reported financial losses stemming from the fraudulent activity.⁴ Fraud degrades operational performance and increases cost—not only for the parties to the transaction(s) whose payments are disrupted but also for the payments system as a whole.

While older payment forms, such as checks, have always been vulnerable to fraud, newer electronic forms have opened up a more complex array of opportunities for fraud and data theft; these are related to the more open nature of twenty-first-century electronic information and recordkeeping. Moreover, the number and type of players in the payments industry is growing, as nonbank companies, such as Wal-Mart, compete directly with financial institutions by offering payments services. All of these changes have led to an increasingly complex security environment for payments providers, merchants, consumers, and the public sector. Various players must discern whether new payment types carry excessive fraud risk; who is liable when payments fraud occurs; how losses are allocated; what consumer protections should be in place; and how standards should be defined to lessen the incidence of fraud. While everyone might agree

on the fundamental importance of reducing fraud in the payments system, there are differing philosophies about how to achieve this goal.

The role of the market

Payments practitioners have an immediate incentive to reduce fraud in order to remain profitable and to avoid reputational and regulatory risks associated with fraud losses. Industry participants

constantly adapt to keep pace with criminal activity, technology-driven change, and innovation in the payments system.

Roundtable representatives concluded that it would be impossible to eliminate fraud completely. They noted that fraud prevention initiatives must balance costs and benefits and that payments practitioners have different incentives motivating their fraud resolution measures. While the roundtable representatives

While some economists and practitioners consider the current state of fraud containment in the retail payments marketplace to be sufficient, others question this assessment.

recognize that security is hard to achieve and ensure. Security is expensive to produce; therefore, it can result in indirect but nonetheless real costs to consumers. For this reason, cooperation across the supply chain is not only desirable but also necessary to achieve efficient outcomes for consumers. Institutions that are trying to manage payments fraud levels face constant change as they attempt to keep abreast of new technology and security needs. Regardless of the fast pace of change, participants in the payments system recognize the importance of effective fraud reduction strategies, since the banking and payments industries depend on reputation and trust for their success.

Many payments practitioners and some economists argue that the payments system performs quite well in responding to fraud risks; therefore, they favor a private market approach to fraud containment. This view of retail payments system fraud was represented by the diverse cross section of participants in a 2007 roundtable on the subject sponsored by the Federal Reserve Board's Payments System Policy Advisory Committee.⁵ The roundtable, which included representatives of banks, nonbank payments providers, payment card companies, and technologists, offered a variety of views but also reached a broad consensus on some important points. There was consensus that the current level of payments fraud is being effectively managed; however, organizations must

indicated that the dollar value of fraud relative to business revenue is declining, their business costs for fraud mitigation are both substantial and trending upward. An especially interesting consensus emerged: The instrument that is the principal source of fraud losses on a comparative basis is the traditional paper check, as opposed to more recent electronic payment innovations.⁶

Roundtable participants also spoke about the impact of e-commerce. The Internet allows fraud directed at the U.S. payments system to originate anywhere in the world. This technological innovation has turned payments security issues on their head: In a classic bank robbery, the crooks tunnel into the bank from a location next door, while on the Internet, everyone is virtually next door.

Overall, participants agreed that, while protecting consumer information is clearly a responsibility of payments providers, it is also important to encourage and help consumers to follow good security practices. The roundtable concluded that fraud detection and prevention would improve through more industry-wide information sharing and collaboration, greater use of enhanced authentication technologies, and more widespread adoption of the Payment Card Industry Data Security Standard, also known as PCI.⁷

The consensus reached by the roundtable is supported by the results of an earlier survey of approximately 100 large nonfinancial firms that actively use a

variety of payments services.⁸ In the survey, each firm identified its most important payments processing requirements. While participating firms generally responded that controlling fraud is critically important, a relatively low percentage responded that they are dissatisfied with the ability of current payment methods to control fraud. Consequently, other payment improvements, such as the ability to track transactions, emerged as needing higher-priority attention than fraud containment. Thus, many payments participants noted that, while payments fraud is an inherent concern, it is one that can be effectively managed if the private sector makes the necessary financial and time commitments.

Is more intervention needed?

Some would argue that a more active public sector approach may be required to ensure the most effective and efficient operation of the payments system. Payments systems and markets are thought of as special because they entail network effects. As network industries, payments systems operate most effectively when many large and small players are included. Payments networks also exhibit externalities, meaning that the costs and/or benefits associated with payments services are not always recognized by the parties to commercial transactions. In addition, the markets may suffer from asymmetric information—i.e., the sellers and buyers of payments services may not be equally well informed about the risks associated with a particular payments service. Authentication is one such asymmetry in the payments market.

While some economists and practitioners consider the current state of fraud containment in the retail payments marketplace to be sufficient, others question this assessment. It is important to note that smaller payment firms, merchants, and other participants often look to the government to ensure equity in the payments system and to help control payments fraud. This might be accomplished by issuing regulations that specify disclosures required for payments service security, by enforcing those and other regulations, and possibly by facilitating industry-wide practices that lead to

desired effectiveness and efficiency outcomes for the payments system.

Some recent economic analyses suggest that current market incentives and mechanisms are not up to the task of containing fraud to a degree that optimizes overall payments system effectiveness and efficiency. One recent research paper shows that nonbanks currently play an important role in retail payments systems worldwide, especially in the U.S., and that this role is likely to continue to grow.⁹ It argues that the growing prominence of nonbanks has increased operational risk, including data security risk and, by extension, fraud risk. The paper also raises concerns about systemic operational disruptions as a consequence of concentrating operations among fewer key nonbank payments services providers. Finally, the paper speaks to the banks' role as "payments system gatekeeper" and to the inherent difficulties that banks have in fulfilling their role because the operational locus is shifting to nonbanks.

While it is certainly true that the role of nonbanks in the retail payments system is increasing, it is not clear that this trend in itself results in greater operational risk. Electronic payments are among the most technology-intensive financial services. The pace of change in the technology environment, and in fraud prevention in particular, requires providers to try to stay a step ahead of the fraudsters. Partnerships among banks and nonbank entities, if managed well, tend to strengthen, not weaken, the payments system. Also, it is not necessarily true that concentrating the supply of sophisticated operational services increases operational risk. Fragmented operations that perform poorly, or perform below a recognized standard, can be riskier than consolidated operations that perform at a higher standard—one that sufficiently accounts for security, business continuity, and operational contingency arrangements. Of course, operational cost is also a factor, in that electronic processing exhibits increased economies of scale.

Another research paper, written by a Federal Reserve Bank of Kansas City economist, questions the notion that market solutions to payments fraud are

adequate in today's marketplace.¹⁰ This economist argues that the fraud control measures that were in effect during the paper payments era have not changed substantially in the electronic payments era, even though the threat now is inherently much bigger. Her paper focuses on "transactional identity" and "information-dependent transactions" involving non-cash retail payments. It concludes that because of the problems with externalities and asymmetric information, the private marketplace will not contain identity theft to an efficient degree and, as a result, the integrity and efficiency of the payments system are at risk.

This paper goes on to prescribe an active role for public authorities to ensure the integrity of transactions within the payments system. Some examples of public policy prescriptions to deal with market failure include disclosure rules to address the asymmetric information problem and laws to clearly and comprehensively assign liability to address the problem with externalities. However, one could also argue that the payments industry itself has a powerful incentive to develop effective and efficient fraud control strategies to keep up with new electronic payment platforms.

Conclusion

It is clear that some participants and observers of the payments system believe that the problem of payments fraud is significant but well within the power of the private sector to address. However, others challenge this position. They believe there is a need to evaluate the role of the public sector in protecting the integrity of the payments system as a whole, not just the integrity of individual service offerings. Others argue that there is merit on both sides of the debate. This view recognizes that payments security is best provided by the private sector, but that the public sector should play a vital role. The public sector should coordinate various parties and help foster confidence in the overall payments system while discouraging counterproductive practices that enhance opportunities for fraud.¹¹

We need to keep these different views in mind when attempting to size up the problem of payments fraud, propose ways

to contain it, and provide implications for public policy. We must consider whether the private sector alone is able to do enough to contain fraud in a manner that protects the payments system as a whole. We must also consider whether government intervention in fraud management might make matters worse, for instance, by reducing the efficiency of the payments system—the perennial problem of unintended consequences.

The integrity of the payments system becomes more important each day, as electronic real-time payments supplant conventional paper instruments, dependencies on sophisticated technologies increase, and nonbanks play a greater role as providers of payments services. In this environment, it is conceivable that public policy institutions, including the Federal Reserve, might come to play a greater role in the payments system. In the meantime, the Federal Reserve can help to uncover the nature of the payments fraud problem by convening public forums on the issue.

While the issue of payments fraud is widely discussed in the media and the industry, few forums have explored the roles and responsibilities of players in the payments industry in an analytical setting involving the economics of the

Charles L. Evans, *President*; Daniel G. Sullivan, *Senior Vice President and Director of Research*; Douglas Evanoff, *Vice President, financial studies*; Jonas Fisher, *Economic Advisor and Team Leader, macroeconomic policy research*; Richard Porter, *Vice President, payment studies*; Daniel Aaronson, *Economic Advisor and Team Leader, microeconomic policy research*; William Testa, *Vice President, regional programs, and Economics Editor*; Helen O'D. Koshy, Kathryn Moran, and Han Y. Choi, *Editors*; Rita Molloy and Julia Baker, *Production Editors*.

Chicago Fed Letter is published monthly by the Research Department of the Federal Reserve Bank of Chicago. The views expressed are the authors' and are not necessarily those of the Federal Reserve Bank of Chicago or the Federal Reserve System.

© 2008 Federal Reserve Bank of Chicago
Chicago Fed Letter articles may be reproduced in whole or in part, provided the articles are not reproduced or distributed for commercial gain and provided the source is appropriately credited. Prior written permission must be obtained for any other reproduction, distribution, republication, or creation of derivative works of *Chicago Fed Letter* articles. To request permission, please contact Helen Koshy, senior editor, at 312-322-5830 or email Helen.Koshy@chi.frb.org. *Chicago Fed Letter* and other Bank publications are available on the Bank's website at www.chicagofed.org.

ISSN 0895-0164

industry as a whole. To explore the complex problem of payments fraud and methods for combating it, the Chicago Fed is pleased to host its eighth annual payments conference, Payments Fraud: Perception Versus Reality, on June 5–6, 2008. The conference will

highlight threats to the security of the U.S. payments system and outline solutions. The conference discussions will focus on the following five themes: identifying security issues in the retail payments system; preventing and containing payments fraud; allocating losses when

payments fraud occurs; exploring fraud in emerging payment channels; and evaluating public and private responses to payments fraud. We look forward to lively discussions on the topics covered in this article.

¹ See www.federalreserve.gov/PaymentSystems/pricing/frpaysys.htm.

² Consumer protection regulations related to payments include Regulation Z, which addresses credit card disclosure, and Regulation E, which outlines protections related to electronic funds transfers.

³ Bruce J. Summers, 1994, "The payment system in a market economy," in *The Payment System: Design, Management, and Supervision*, Bruce J. Summers (ed.), Washington, DC: International Monetary Fund.

⁴ 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.

⁵ The roundtable discussion was held on March 27, 2007, at the Federal Reserve Bank of Minneapolis; see Board of

Governors of the Federal Reserve System, 2007, "A summary of the roundtable discussion on retail payments fraud," report, Washington, DC, July. The Fed's Payments System Policy Advisory Committee evaluates risk-management issues, primarily in wholesale payment and settlement systems.

⁶ A recent study by the Federal Reserve Board shows that financial institutions incur annual check fraud losses of nearly \$1 billion; see Board of Governors of the Federal Reserve System, 2007, "Report to the Congress on the Check Clearing for the 21st Century Act of 2003," report, Washington, DC, April.

⁷ This standard defines guidelines for merchants' handling and processing of payment card data in order to prevent card fraud and data breaches.

⁸ Sandy Krieger and Michele Braun, 2004, "Opportunities to improve payments

services: Results from a survey of large corporations," Federal Reserve Bank of New York, report, July.

⁹ Members of the European Central Bank, Oversight Division, and Members of Federal Reserve Bank of Kansas City, Payments System Research Function, 2007, "Nonbanks in the payment system: European and U.S. perspectives," Federal Reserve Bank of Kansas City, Payments System Research, working paper, No. 07-01.

¹⁰ Stacey L. Schreft, 2007, "Risks of identity theft: Can the market protect the payment system?," *Economic Review*, Federal Reserve Bank of Kansas City, Fourth Quarter, pp. 5–40.

¹¹ 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, forthcoming.