Fraud containment

Bruce J. Summers

Fraud is an unfortunate aspect of the technical efficiency of the payment system, which is measured by the quality of its operational performance and cost.[1] Fraud degrades operational performance and increases cost—not only for the parties to the transaction(s) whose payments are disrupted, but for the payment system as a whole. Indeed, any serious consideration of payments fraud must account not only for the readily measurable business and consumer impacts of such fraud, but also for impacts on the performance and cost efficiency of the payment system.

Today's panel[2] on fraud containment has been asked to identify the most common forms of retail payments fraud; the most effective fraud reduction tools, especially those pertaining to real-time payments; and approaches that payment providers and merchants take to balance fraud risk and consumer convenience. In taking up the last issue in particular we will attempt to provide a broad perspective that addresses the consequences of fraud not only for individual businesses and consumers, but for the integrity of the payment system as a whole.

While the focus of the conference is, naturally, on the U.S. payment system, it should be noted at the outset that the fraud problem is global, affecting many national payment systems and cross-border payment arrangements. For example, payment system fraud poses a threat to the internal market for payments in the European Union and is therefore receiving prominent attention in Europe.[3] My sense is that the main payment system fraud concerns and issues in the U.S. and Europe are very similar and that we have a lot to learn from each other's experiences and responses. Accordingly, we should consider today's discussion part of a global dialogue about payment system fraud, and we should be open to opportunities to be informed by the international debate. This is especially so with regard to the public policy responses to the fraud problem.

The members of the panel bring an ideal combination of informed perspective and practical experience to bear on the problem of fraud. We have an information security technologist, a banking security practitioner, and a seasoned retail industry lawyer who has been concerned with customer data privacy and protection. Each of the panelists, whom I will introduce in a few minutes, will take 15 minutes to present his perspectives, and then we look forward to taking your questions and engaging in dialogue with you.

I would like to begin with some introductory remarks intended to set the stage for the panel discussion. In particular, I want to crystallize the business and public policy issues that involve containment of retail payments fraud. I will do so by summarizing the thinking of practitioners (by which I mean the providers and corporate users of payment services) and economists about fraud and efforts to contain it. The views of these two groups vary somewhat and are important because they influence public policy. You will understand that my background as a central bank economist, and also as a payments product manager and technology manager, has a strong bearing on how I cast the issues.

Economists' view of payments fraud

Payment system economists are principally interested in the most effective and efficient possible operation of the payment system. Of course, economists also respect the role of markets in delivering efficient

Bruce J. Summers is an independent consultant on payment systems and technology management. He is the former director of Federal Reserve Information Technology. *The author thanks Katy Jacob and Tara Rice for their assistance in the preparation of this article.*

outcomes, and the payment system market is no exception. From the perspective of economic analysis, however, payment systems and markets are thought of as special because they entail something called "network effects" and "two-sided" services, which are characteristic of public goods.[4]

Payment markets, moreover, may not always function like perfect markets because of the presence of "externalities," meaning that the costs and/or benefits associated with payment services are not always recognized by the parties to commercial transactions. As an example, my decision to use a risky means of payment may be a relatively easy one if it imposes costs on others and on the payment system, but not so much on myself. In addition, the markets may suffer from "asymmetrical information," meaning that the sellers and buyers of payment services are not equally well informed about the riskiness of a particular payment service. For example, as a buyer I may not know as much as I would want or need to know about how well my personal payment information is secured in the service provider's systems.

For these reasons, as I will describe later, some economists see a natural role for the public authorities in helping control payment system fraud. They might do so by issuing regulations that specify the amount and type of disclosure required for payment 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 payment system.

The views of economists are often informed by observed experience, and accordingly, I would like to share with you some lessons learned by practitioners who have met the business challenge of delivering effective, efficient, secure, and well-controlled payment services, especially as it pertains to security. They have found, first, that security is hard to achieve and ensure, and it requires relentless attention. Second, security is very expensive to produce and can impose indirect but nonetheless very real costs on consumers through the "user experience." Third, cooperation across the supply chain is not only desirable but also necessary to achieve meaningful outcomes for customers because security is "only as strong as the weakest link," as the adage goes. Fourth, certain aspects of technology, and security in particular, are moving outside the banks' sphere of core competency, leading to outsourcing as a means of staying ahead of the curve; this leads to new types of risk that must be managed. Finally, the reputational risk associated with providing payment services is of greatest consequence to boards of directors of banking institutions because the success of the banking franchise depends on reputation and trust. Any business consideration of fraud containment must start with the board of directors and the corporate culture surrounding the private market approach to fraud containment.

The Federal Reserve's role

A word or two about the Federal Reserve's operational responsibilities in the payments marketplace will help illustrate that the Fed is in close touch with business and operational realities faced by practitioners. The Federal Reserve Banks directly provide retail payment services, primarily check, electronic check, and automated clearinghouse (ACH), for which they charge fees that are designed to recover the full costs of operation. They also produce retail payment services on behalf of the U.S. Department of the Treasury in their role as fiscal agents. This includes electronic payment services in support of the Treasury's public debt and, if I can put it in these terms, accounts receivable and payable operations. The Fed thereby indirectly interacts with a large proportion of the retail public. Moreover, and perhaps especially important in the context of today's discussion, the Federal Reserve Banks' electronic payment operations are Internet-intensive, meaning that the public Internet figures prominently in the delivery of their services.

This brings the reality of public networking and protection of customer information very close to home for the Federal Reserve Banks. Speaking of close to home, this is an opportunity to recognize the leading role played by the host of this conference, the Federal Reserve Bank of Chicago, as the Reserve Bank responsible for the content, quality, security, and bottom line financial viability of the Federal Reserve's electronic payments. The Chicago Fed deserves to be recognized as the U.S. central bank's Internet payments pioneer.

An industry perspective of payments fraud

The current state of thinking by industry practitioners about retail payment system fraud is well 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 payment providers, card companies, and technologists, produced a variety of views but also a broad consensus on some important points. There was consensus that the current level of payments fraud is being effectively managed and that organizations must constantly adapt to keep pace with criminal activity, technology-driven change, and innovation in the payment system. At the same time, the industry representatives concluded that it

will never be possible to eradicate fraud completely and that the never-ending challenge of fraud prevention must balance costs and benefits.

While the roundtable participants indicated that the dollar value of fraud relative to business revenue is declining, their business costs of fraud mitigation are both substantial and trending upward. An especially interesting consensus emerged: The payment instrument that is the principal source of fraud losses on a comparative basis is the traditional paper check. We should try to validate this observation today and, depending on the outcome, reflect on the implications for future fraud containment as reliance on electronic payments continues to increase.

The roundtable participants spoke to the challenges posed by the Internet as a source of fraud, since it allows fraud that is directed to the domestic payment system to originate anywhere in the world. Some took a broad view of payments fraud by saying—rightly so in my view—that protecting customer information is part of the responsibility shouldered by payment providers. In the end, it was noted that detecting and preventing retail payments fraud requires a holistic approach that includes not only designing and producing well-secured payment services, but also encouraging and helping customers to practice good security behaviors. The roundtable made three suggestions for improving fraud detection and prevention. These are to increase 1) industry-wide information sharing and collaboration, 2) use of enhanced authentication technologies, and 3) adoption of the standards set by the PCI (Payment Card Industry) Security Standards Council LLC.[6]

The consensus reached by the roundtable is supported by the results of a somewhat earlier survey of approximately 100 large nonfinancial firms that actively use a variety of payment services.[7] In the survey, each firm identified its most important payment processing needs and those needs that are least well met. While the firms participating in the survey generally responded that controlling fraud is very or 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.

Public versus private responses to payments fraud

The evidence suggests that practitioners are comfortable with the current state of fraud control in the retail payments marketplace. Their views can be contrasted with those of economists who take a public policy interest in the payment system. Economists' current thinking about retail payment system fraud is somewhat more difficult to discern than that of practitioners because it has a work-in-process quality to it. Nonetheless, some recent economic analysis suggests that the view of economists is likely to be a bit less sanguine than that of the practitioners in the retail payment industry.

There seems to be the sense that market incentives and mechanisms per se are not up to the task of containing fraud and possibly other operational risks to a degree that optimizes overall payment system effectiveness and efficiency, and indeed they might not even maintain the integrity of the payment system as it continues to evolve. Two recent economic analyses undertaken within the central banking community suggest that the growing role of third-party, or nonbank, providers of payment services is a cause for concern and, moreover, that the public-good aspects of payment systems call for a more active governmental role. Let me elaborate briefly on some of the main conclusions from these analyses for they are important.

The role of nonbanks

A paper presented at the recent conference on nonbanks and risk in retail payments, sponsored jointly by the European Central Bank and the Bank of England, shows that nonbanks currently play an important role, especially in the United States, and will play an increasingly important role in a variety of retail payment systems worldwide.[8] It argues that the growing nonbank presence 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 payment services providers. Finally, the paper speaks to the "payment system gatekeeper" role of banks and to the inherent difficulties that banks have in fulfilling their role while the operational locus shifts to nonbanks.

I think that it is very useful to measure and highlight the significant and increasing role of nonbanks in the retail payment system. At the same time, however, I question the conclusion that a more prominent operational role for nonbanks automatically increases operational risk. Electronic payments are among the most technology-intensive financial services. My practical experience with electronic payments is that the pace of change in the technology environment, including the technical capabilities that support fraud schemes, requires providers to operate on or near the technology frontier, especially if they want to stay a step ahead of the bad actors who perpetrate fraud.

Staying a step ahead of payments fraud in this environment is simply not possible for banks to accomplish without forming business alliances and partnerships that mobilize the needed technology skills. These business partnerships more often than not take the form of outsourcing to nonbank specialists, which, if managed well, act to strengthen the payment system. Also, I question whether concentrating the supply of sophisticated operational services, at least up to a point, necessarily increases operational risk. I think, again based on practical experience, that fragmented operations poorly performed, or performed below a recognized high standard, can be riskier than consolidated operations performed at the highest standard if due attention is given to security, business continuity, and operational contingency arrangements. Of course, operational cost is also a factor in that electronic processing exhibits natural economies of scale.

Information-dependent transactions

An additional paper relevant to the topic of fraud containment is that by a Federal Reserve Bank of Kansas City economist regarding the ability of the private sector alone to protect against the risk of identity theft and to protect the retail payment system.[9] This paper focuses on "transactional identity" and "information-dependent transactions" involving noncash retail payments. It concludes that because of the problems with externalities and asymmetric information, the marketplace will not contain identity theft to an efficient degree; and as a result, the integrity and efficiency of the payment system, which we are to think of as a public good, are threatened. The concept of market failure is evoked and an active role for public authorities is envisioned to ensure the integrity of the payment system. Some examples of public policy prescriptions to deal with market failure—such as disclosure rules to address the asymmetric information problem and laws to clearly and comprehensively assign liability to address the problem with externalities—are very familiar to us. The paper holds out the more intriguing prospect of other payment system interventions by public authorities along the lines of the Federal Reserve's lender of last resort role in the credit markets or the federal deposit insurance.

This economic analysis seems to be at odds with the views of industry practitioners who think that the payments fraud challenge, while significant, is within the power of the private sector to address. The challenge, I think, is to evaluate seriously what remains to be done in the realm of private sector initiatives to protect the integrity of the payment system, not just the integrity of individual service offerings.

Conclusion

As we head into the panel discussion, it will be important to keep in mind the apparent differences in how practitioners and payment system economists size up the problem of fraud, the ways in which it is contained, and the implications for public policy. In taking up the issues assigned to us—the most common types of payments fraud, the most effective tools to deal with these types of fraud, and the costs of containing fraud—the panelists will provide their business perspectives and also help us understand whether the private sector is able to do enough alone to contain fraud in a manner that protects the payment system as a whole. The issue of the integrity of the payment system becomes more important each day, as electronic real-time payments supplant conventional paper instruments, dependence on sophisticated technologies increases, and nonbanks come to play an increasingly important role as providers of payment services. Depending on the outcome of the debate, public policy institutions such as the Federal Reserve could come to play a more active and interventionist role in the payment system as regulators and supervisors, and nonbanks could come more directly under the regulatory and supervisory purview of the authorities.

NOTES

[1]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.

[2]This panel, which I moderated, comprised Jeff Schmidt, an independent consultant; Bob West, chief executive officer, Echelon One; and Mallory Duncan, senior vice president and general counsel, National Retail Federation.

[3]Commission of the European Communities, 2008, "Report on fraud regarding noncash means of payments in the EU: The implementation of the 2004–07 EU Action Plan," commission staff working document, Brussels, Belgium, April 22.

[4]A network effect occurs when the value to existing users of a product or service increases as the number of additional users increases. Rochet and Tirole define a two-sided market as a market in which end-users are unable to negotiate prices based on costs to participate on a platform and the price structure affects the total volume of transactions; see Jean-Charles Rochet and Jean Tirole, 2006, "Two-sided markets: A progress report," *RAND Journal of Economics*, Vol. 37, No. 3, Autumn, pp. 645–667. For further discussion on network effects and two-sided markets, see Wilko Bolt and Sujit Chakravorti, 2008, "Economics of payment cards: A status report," *Economic Perspectives*, Federal Reserve Bank of Chicago, Vol. 32, No. 4, Fourth Quarter, pp. 15–27.

[5]See Board of Governors of the Federal Reserve System, 2007, "A summary of the roundtable discussion on retail payments fraud," report, Washington, DC, July. This article summarizes the roundtable discussion on payments fraud held on March 27, 2007, at the Federal Reserve Bank of Minneapolis. For details on the Fed's Payments System Policy Advisory Committee, see www.federalreserve.gov/paymentsystems/comm/default.htm.

[6]Experience shows that continuous and timely strengthening of recommended standards deserves as much emphasis as does their adoption. For example, it has been reported recently that the standards set by the PCI Security Standards Council provide incomplete protection of "data in transit" through telecommunications channels. See Associated Press, 2008, "Credit card breach raises broad concerns," *New York Times*, March 23, and Joseph Pereira, 2008, "Credit card security falters," *Wall Street Journal*, April 29.

[7]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.

[8]Simonetta Rosati, Terri Bradford, Fumiko Hayashi, Christian Hung, Richard J. Sullivan, Zhu Wang, and Stuart E. Weiner, 2007, "Nonbanks and risk in retail payments," Federal Reserve Bank of Kansas City, Payments System Research, working paper, No. 07-02. This paper was presented at the joint European Central Bank–Bank of England conference on payment systems and financial stability, which was held on November 12–13, 2007, in Frankfurt, Germany.

[9]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.