Economic Perspectives special issue on payments fraud: An introduction

Gene Amromin and Richard D. Porter

In this special issue of *Economic Perspectives*, we present selected papers based on our recent conference, Payments Fraud: Perception Versus Reality, hosted by the Federal Reserve Bank of Chicago on June 5–6, 2008. The conference brought together decision-makers from the banking, payments, legal, regulatory, and merchant communities for a wide-ranging discussion of the threats to the security of the payments system and how those threats might best be addressed.

The volume starts with an extensive summary of conference presentations, keynote addresses, and open floor discussions, written by Tiffany Gates and Katy Jacob. In order to give a sense of the intense back-and-forth exchanges that took place during this day-and-a-half-long event, the authors structure their summary around the broad themes of the discussion rather than simply presenting a chronological account. The themes are as follows: organizational structures for management of fraud risks; technological innovation; alignment of incentives for fraud prevention among consumers, merchants, and payments providers; and regulatory policies.

Gates and Jacob's article highlights the challenges involved in bringing the various constituencies together to forge common ways to address fraud in payments systems. Gates and Jacob find that payments fraud cannot be eliminated without decreasing the openness and efficiency of the payments system. In the current environment, technological innovations have enabled system participants to enhance payments security, at the same time that technology has made it easier for criminals to perpetrate payments fraud remotely. Practitioners are constantly weighing the costs and benefits of payments fraud mitigation and are looking to the public sector to offer guidance and support. As the industry combats payments fraud, companies are banding together to find common solutions. For instance, throughout the conference, financial industry participants emphasized the concept of enterprise-wide fraud management, while many also acknowledged the difficulties faced by small merchants and many financial institutions in fashioning such holistic strategies. A number of legal professionals stressed the detrimental effects of legacy laws and regulations that evolved independently around individual payment product lines. Together, these viewpoints contributed to a budding consensus on the importance of dedicated high-level executive involvement in payments fraud management and of outsourcing development of fraud prevention tools to specialized entities.

The rest of this volume is devoted to articles that address in greater detail some of the key topics discussed at the conference. The contributors of these papers span the spectrum of thought leaders in combating payments fraud—industry experts in fraud detection systems, legal professionals, academic researchers in economics and technology, and senior officials of the Federal Reserve System.

The first article is written by Bruce J. Summers. His paper provides a synthesis of the approaches of practitioners and economists to thinking about the problems in containing *retail* payments fraud. As Summers makes clear, these approaches differ somewhat for reasons that have to do with both perspective and analytical framework. Yet, both parties are integral in formulating a coherent public policy response to the problem of payments fraud.

In particular, payments industry practitioners tend to regard fraud as a persistent but manageable problem that requires both unrelenting attention and significant expenditures. These expenditures on fraud mitigation

Gene Amromin is a senior financial economist and Richard D. Porter is a vice president, senior policy advisor, and the director of the payments team in the Financial Markets Group at the Federal Reserve Bank of Chicago.

have resulted in declining rates of fraud losses. Still, there is concern that maintaining such results in the future will require ever-expanding expenditures. Part of this argument rests on the view that fraud threats to electronic payments networks arise globally, are increasingly sophisticated, and propagate quickly. The bottom line is that for the practitioners, payments fraud is part of the cost of doing business, which can be ameliorated by pooling fraud prevention efforts. To underscore this view, Summers reports consensus recommendations from a recent industry roundtable (which is a focus of the article by Malphrus later in this volume). Those recommendations call for information sharing, better authentication technologies, and adoption of standards—ideas that take into account the economies of scale and scope in fraud prevention, though not necessarily the conflicting incentives among the many participants in payments networks.

Economists tend to think of the payments system as a vast network of participants whose divergent incentives generate considerable spillovers from their own actions. The effects of these spillovers are frequently not fully appreciated by the participants because market prices fail to convey the extent of the spillovers to them. An example of such an "externality" is when a consumer (or merchant) fails to be appropriately vigilant about data security because limited liability rules (or existing penalties for breaching network security protocols) do not signal the extent to which such actions affect other participants in the payments system. Moreover, because fraud prevention by one party usually improves the experience of everyone else, there is ample incentive for other participants to "freeload." As a result, there may be drastic underprovision of fraud prevention in the *aggregate*. This framework forces economists to take a systemic view of payments networks, focusing on ways in which policy can better align the incentives of all participants. One important implication of this view is that incentives (or regulation) must be appropriately allocated across the payments network because the entire system is only as strong as its "weakest link."

The juxtaposition of the views of practitioners and academic economists gives rise to an interesting and provocative observation that industry practitioners' relatively sanguine view of risk is partly attributed to their focus on practices of their own firms. Thought leaders in the industry are keenly aware that the interconnectedness between the many players in the payments space poses risks that are not directly observable by any individual participant. Yet, their primary responsibility for managing fraud at their enterprises may instill a somewhat false sense of security. This comparison also points to a potentially key role of the Federal Reserve in bridging the gap, since it is both a research center and a major payments provider.

The next three articles in this volume are, in some sense, elaborations on Summers' conclusion. The first of these, by William Roberds and Stacey L. Schreft, lays out an economic framework for thinking about fraud in payments networks. The second, by Steve Malphrus, gives the industry view on the current state of efforts in retail fraud management. The third, by Mark N. Greene, addresses the nature of payments fraud and the need for coordinated efforts in fighting it.

Roberds and Schreft start out by noting the inevitable trade-off between more efficient payments markets and loss of privacy. On the one hand, as an economy grows, paying for transactions in cash becomes prohibitively expensive and inefficient. On the other hand, credit- and debit-based transactions between parties that typically do not know each other are impossible without exchanging some information that verifies both the identity and the creditworthiness of the parties. The resulting transfer of information back and forth presents opportunities for fraud. Still, without such transmission of private information modern payments systems would be infeasible, thereby forcing payments activity onto the slower rails of cash-facilitated exchanges of yesteryear.

What is the proper balance then? As Roberds and Schreft argue, it is useful to think of this balance as "confidentiality" of payments transactions. "Confidentiality" thus consists of "data informativeness" (how much identifying information is exchanged between parties) and "data integrity" (how well this information is protected). If you tilt the balance too much toward safeguarding privacy (that is, lessen data informativeness), then the wheels of credit-based and remote transactions grind to a halt. But if you tilt it too much toward being absolutely certain about the identity and creditworthiness of the consumer, then you may transmit so much data that you increase the incidence of and losses from fraud.

To get closer to the answer, the authors lean on economic theory. They note that neither information nor integrity diminishes with repeated use. For example, say Wal-Mart knows Mr. A is not a fraudulent actor and, therefore, processes payments it receives from him. The fact that Wal-Mart has this information does not diminish the value of the information to Home Depot. These seemingly abstract concepts matter because they help us think about the way in which "confidentiality" can be provided efficiently. In particular, the fact that the two attributes of "confidentiality" do not wear down with consequent use implies that, at some point, the marginal cost of providing it is close to zero.

This insight implies that optimally there will be only a few large producers of "confidentiality" that are able to leverage vast economies of scale in building networks for collecting and transmitting necessary information securely (for example, credit bureaus, card networks, and so on). However, since information must be exchanged among many different parties (for example, merchants, issuers, and consumers) in order to have value, the potential for conflicts of interest is large. Some parties may have weaker incentives to safeguard information and thus become the "weak link" that compromises the entire system. Some parties may choose to freeload on data integrity efforts of others because the cost of fraud or loss of "confidentiality" is not proportionately allocated.

The authors' analysis of "confidentiality" further points to the proper role for policymakers in fostering efficient (but not fraud-free) payments systems. Public policy should aim to resolve the potential for conflicts of interest through coordination, judicious imposition of standards, and proper allocation of legal incentives (as discussed in greater detail in Douglass's article later in this volume). The public sector should not focus on duplicating the job done by the private sector in collecting, verifying, and processing payments-related information. As Roberds and Schreft underscore, the ultimate goal of regulators should be to strike the proper balance between privacy and efficiency.

Malphrus's article summarizes the results from a special roundtable discussion on retail payments fraud, which was held at the Federal Reserve Bank of Minneapolis in March 2007. The participants reported that, despite the declining use of checks, check payments still generated the largest number of fraud attempts. They emphasized that criminals are continually searching for weaknesses in fraud detection and prevention practices. Many thought that banks and businesses needed to adopt a holistic approach to detecting and preventing retail payments fraud, being ever mindful of the overall fraud landscape across all of their operations. The roundtable participants shared a number of suggestions for improving the industry's ability to detect and prevent retail payments fraud, including better protection of customers' personal and financial data. They recommended more effective sharing of best practices with respect to fraud detection and prevention within the industry. Industry leaders specifically discussed the effectiveness of PIN (personal identification number) and chip technology. Some stated that fraud rates on PIN debit cards are significantly lower than those for other payment types, and advocated a more widespread application of PIN security to card payments.

Malphrus also shares some thoughts on new account fraud that has featured prominently in recent discussions on retail payments systems' vulnerabilities. Allowing customers to open accounts electronically, as opposed to in person at a bank, clearly offers the potential for fraud. However, this risk can be mitigated by making use of various technologies; for example, software can identify the geographical location of the user's computer, and device identification tests can be subjected to further fraud screening. All of these technologies are currently operational, and their widespread adoption is likely to make a considerable difference in mitigating a particular aspect of retail payments fraud.

Malphrus also highlights an increasingly important aspect of policymaking—the need to protect privacy while countering terrorist financing and money laundering. As different agencies (for example, the Central Intelligence Agency and the Federal Reserve) cooperate to combat these threats, they must be vigilant about how they exchange information about U.S. citizens. Moreover, as those perpetrating illicit activities increasingly attempt to leverage existing payments networks, the need for cooperation between the private sector and government agencies becomes all the more important.

The next contributor, Greene, represents Fair Isaac Corporation—a leading provider of automated identification procedures for prospective fraud on electronic payments networks. Greene's role gives him a clear perspective on the nature of the current threats to the payments system. As Greene argues in his article, greater cooperation among the various payments system participants is necessary to combat fraud. Increasingly, modern day fraudsters operate globally, often outside the jurisdiction of the U.S., and they are well organized and well financed.

In particular, Greene warns that adopting piecemeal solutions that focus on individual payments segments or regions would be inadequate to beat the scams. While payments providers may have an incentive to differentiate their products and seek competitive advantage, they need to find ways to cooperate with each other in sharing information or developing standards that would help lessen the problem. He suggests that piecemeal solutions are like pushing on a balloon—they may impede fraud in the particular targeted segment or region but quite often at the expense of increasing fraud elsewhere.

Instead, Greene advocates a fraud protection system that works like a burglar alarm, covering *all* the openings—"doors and windows"—since fraudsters will always make the most of the weakest link. He argues it is possible to build better models of fraud

containment that profile not only individuals but also devices and merchants. With this platform, one could successfully identify uncharacteristic and possibly fraudulent payment behavior. Such modeling exercises would be more effective if they could be "trained" (that is, estimated on large amounts of current real-world data); this might require the cooperation of various payments system participants. Some public sector cooperation might be desirable to remove the concern that such industry data-sharing exercises constituted collusive practices.

In the question-and-answer session that followed Greene's keynote address at the conference, Greene raised the possibility of a *mass compromise* to the payments system by fraudsters. In a typical card compromise where the information could be stolen for, say, 25,000 cards, Greene acknowledged there is often only a limited amount of resulting damage—perhaps on the order of 400 fraudulent transactions. He suggested that the outcome could be considerably larger, with perhaps as many as 4 million fraudulent transactions generated on the same (25,000) card base. In this circumstance, Greene argued the systemic risk to payments could be huge. Moreover, he stressed that the industry is not prepared to deal with such a contingency. This might require a joint public–private initiative to scope out the problem and propose solutions.

The next article in this volume, by Duncan B. Douglass, takes us back to the central role that proper allocation of incentives plays in the efficient functioning of payments systems. Douglass focuses on ways in which the current framework of public laws and private network rules distributes fraud liability among the three principal sets of participants—consumers, merchants, and card issuers. Although the discussion centers on signature-based credit and debit cards, its implications are readily extended to other payments instruments.

The public law framework that governs the legal liability for fraud losses is based on the Truth in Lending Act (TILA) and the Electronic Fund Transfer Act (EFTA), as well as the associated Federal Reserve Board Regulations Z and E. As Douglass points out, the primary goal of these laws and rules is to effectively absolve the consumer from liability for losses related to fraud, regardless of whether a consumer's own behavior contributed to fraud in the first place. Although a lack of care on the part of consumers often contributes to fraud, Douglass argues that making consumers bear more of the consequences for their actions is not realistic. This owes both to the political environment and, more importantly, to the desire to instill confidence in the security of card transactions among consumers.

The private card networks' rules take over from where public laws stop—by setting cardholder liability to zero—and proceed to further allocate fraud loss liability between merchants and card issuers. In brief, the rules effectively assign liability for losses in card-present transactions to issuers and in card-not-present transactions to merchants. Douglass emphasizes that this joint framework of public laws and private rules leads to several predictable outcomes that make system-wide fraud prevention efforts somewhat inefficient. To paraphrase, consumers never care too much about safeguarding their transactions, merchants try to exercise due diligence primarily in card-not-present environments, and card issuers are concerned mostly with point-of-sale transactions. Each party thus has ample incentives to undermine the efforts of the other—for example, merchants not verifying signatures at the point of sale.

Douglass illustrates this dynamic with the example of the failed adoption of networks' payer authentication programs. Although these programs are effective in reducing online fraud, consumers, who bear no responsibility for fraud, have balked at merchants' efforts to adopt these measures. For their part, card issuers, which bear less of a burden for fraud in card-not-present transactions, were content to sit on the sidelines and not force their customers to enroll in such programs.

The final article in the volume, by Kevin Fu, Thomas S. Heydt-Benjamin, Daniel V. Bailey, Ari Juels, and Tom O'Hare, focuses on technological vulnerabilities in a newly popular set of payments instruments—devices that use RFID (radio frequency identification), such as credit cards. Such cards offer the promise of speedier contactless transactions at the checkout or gas station and, unlike traditional magnetic stripe cards, require only physical proximity between the card and the associated reader.

Fu and his co-authors demonstrate that the more convenient retail experience provided by RFID devices over magnetic stripe cards may come at the price of several vulnerabilities in RFID's first-generation incarnations. Using their toolkit as electrical engineers, the authors find that *all* of the 20 million RFID-enabled cards currently in circulation are subject to privacy invasion. The cards can be scanned and private information can be removed by the fraudsters without the awareness or consent of the cardholders.

These vulnerabilities should not necessarily be viewed as a fatal indictment of the technology; rather, they represent what might be expected for a work in progress. If successful, RFID technology will overcome these vulnerabilities along its developmental path.

New (and ultimately successful) payments innovations do not necessarily provide full fraud protection capabilities at launch but often gain them over time as they scale up efficiently. The history of PayPal illustrates this point quite nicely.[1] We hope that the message delivered by Fu and his co-authors will rouse the card manufacturers to address these challenges quickly.

Each of the articles collected in this volume offers a specific insight into the current state of efforts in combating retail payments fraud. The articles also outline a number of ways in which these efforts can be made more successful at a systemwide level and offer a methodological framework for thinking about the problem. We hope this work will provide a valuable basis for ongoing discussions on how we can develop and coordinate public and private responses to the pressing need to manage payments fraud risk.

NOTES

[1]Sujit Chakravorti and Carrie Jankowski, 2005, "Forces shaping the payments environment: A summary of the Chicago Fed's 2005 Payments Conference," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 219a, October, p. 2.