Collaboration to address payments risks and fraud

August 10, 2009

In the world of payments, all players share an interest in seeing that risks are detected and mitigated quickly and effectively. However, when threats emerge, is it everyone for themselves? How does the variety of interests and goals among all the players converge? In a private marketplace mixed with government actors, how can we work better together?

Participants at a 2008 conference hosted by the Retail Payments Risk Forum discussed these issues and described the challenges and potential solutions. A year later, the findings of this forum are worth revisiting.

Information sharing
Real or perceived information-sharing limitations among financial institutions, regulators, law enforcement, and others can substantially impede addressing retail payments risks on a timely and effective basis. Examples include inconsistent or incomplete payments data, varying success levels of intra- and interagency collaborations, varied and overlapping jurisdictions, an incomplete network of memoranda of understanding (MOUs), privacy restrictions, perceived barriers beyond legal restrictions, competitive interests, costs, and trust. Suggestions for improvement in this area focused on:

- collection, consistency, and commonality of payments data, better understanding of its utility, and analysis tools. While data needs vary, a first step would be to focus on data elements of shared interest. A working group could facilitate ongoing payments data compilation and analysis efforts;
- formal and informal dialogue among various agencies and others, including simple measures such as shared contact lists;
- development of a “matrix” of various roles/responsibilities/information sources for shared use to facilitate more timely location of information and expertise available; and
- a more systematic, organized mechanism for information sharing, perhaps by establishing “brokers” for relevant information such as payments data.

Policing bad actors
Many noted that communication about bad actors is often ad hoc and that information is too widely dispersed to be useful and timely. Individual agency efforts, published enforcement actions, SAR filings, interbank collaborations, and industry self-regulatory efforts, while all worthwhile, have not fully promoted effective information gathering and sharing among all the parties who can have an impact. Suggestions for improvement in this area included:

- better understanding of risks across payment channels, both for front-end access point(s) and back-end processing, to mitigate fraudster arbitrage of vulnerabilities;
- publishing enforcement actions and related settlements more effectively as a deterrent;
- establishing a central “negative list” or “watch list” of bad actors;
- extending registration requirements for third parties participating in payments networks beyond existing targeted voluntary efforts;
- strengthening and clarifying regulatory guidance, such as that for counterfeit checks and consumer account statements;
- better educating consumers and banks regarding common issues;
- a more direct means of compensating victims;
• mining specific activity reports and other existing agency databases such as consumer complaints data; and
• potential new SEC codes within ACH to better track risks.

**Collaboration**
Participants identified collaborative efforts to help detect and/or mitigate retail payments risk issues and identified benefits and gaps. Examples included bank regulatory groups (intra- and interagency), national and regional law enforcement partnerships, interstate collaboration, federal-state working collaborations, joint investigative task forces, examination- or case-driven *ad hoc* efforts, and industry data-sharing efforts. Potential avenues for improved collaborative action included:

• a law enforcement/regulatory payments fraud working group;
• a virtual collaborative forum via Web sites, e-mail lists, or regular phone calls;
• greater attention paid to requests for comments on proposed NACHA rules;
• examiner and law enforcement training opportunities;
• participation in and/or support for industry database sharing efforts;
• engagement with industry groups to improve best practices;
• a Web-based resource for consumers supported by all (“fraud.gov”);
• implementation of further MOUs among agencies; and
• efforts to identify fraud patterns across agencies, such as the federal government’s Eliminating Improper Payments Initiative.

**Substantive areas of concern**
Participants were asked to describe substantive retail payments risk issues that keep them up at night. Some common themes emerged, including:

• strengthening the oversight of third-party payments processors and others not covered by the Bank Service Company Act;
• quantifying and better managing the misuse of remotely created checks;
• understanding and mitigating risks associated with “cross-channel” fraud;
• “Know Your Customers’ Customer” due diligence, compliance, and associated risks and potential liabilities for fraud detection/mitigation purposes;
• establishing a common means of redress for consumers regardless of the payment channel; and
• improving the clarity of consumer account statements by instituting standards and reducing jargon.

Progress has been made on a number of these ideas in the past year, including the formation of new working groups and other collaborations. The Retail Payments Risk Forum continues to explore opportunities and implement solutions to help foster collaborative action to address these and other industry concerns. Your input in the form of comments to Portals and Rails on these or other topics is welcomed!

*By Clifford S. Stanford*, assistant vice president and director of the Retail Payments Risk Forum at the Atlanta Fed.