NOTE: The panelists' and other participants' views described herein reflect their personal views presented in the context of a working forum and do not necessarily represent the official views of the agency/organization with which they are associated.

CONFERENCE SUMMARY

Hosted by the Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta on October 6-7, 2008, this conference provided a collaborative forum to facilitate information sharing among experts and to foster improved detection and mitigation of retail payments risks and fraud in check and automated clearinghouse (ACH) payment systems. Experts from banking agencies, state and federal law enforcement, NACHA, the ACH operators, and others explored barriers and discussed opportunities. The meeting leveraged the assembled expertise to identify opportunities for further collaboration.

Three expert panels discussed themes regarding third-party risks in retail payments, enforcement actions, and consumer protection concerns. Participants were then asked to discuss key topics in smaller breakout groups, including information-sharing limitations, policing bad actors, collaborative opportunities, substantive areas of concern, and the role of the Retail Payments Risk Forum.

Introduction of the Federal Reserve Bank of Atlanta's Retail Payments Risk Forum

The session opened with remarks from Rich Oliver**,** Atlanta Fed executive vice president and retail payments product manager for the Federal Reserve System. This diverse gathering fulfilled a commitment to continue the dialogue begun at a meeting in January

2008. With the collective knowledge assembled, participants could now begin to develop actionable plans to improve detection and mitigation of retail payments risks. Oliver offered the assistance of the Atlanta Fed to help facilitate this collaboration, including via the newly created Retail Payments Risk Forum.

Cliff Stanford, director of the Retail Payments Risk Forum at the Atlanta Fed, described the mission of the forum overall—to act as a "catalyst for collaboration" among thought leaders addressing retail payments risks and fraud by convening interested parties, promoting actions to mitigate risk, conducting research and analysis, and providing education. This conference included three moderated panel presentations, followed by an action-oriented brainstorming session. Key themes of each are described below.

Changing Roles and Risk Implications of Third Parties in Payment Systems

Claudia Swendseid, senior vice president at the Minneapolis Fed, kicked off the first panel, discussing changing roles and risk implications of third parties in payment systems, particularly ACH and check systems. Citing research conducted by the Kansas City Fed, she noted two ways in which third parties may add risk to the payments system. First, third parties are more often the source of "disruptive innovations" in payments compared to financial institutions that more typically introduce "incremental innovations." Disruptive innovations often involve more risk than incremental innovation, if only because the vulnerabilities associated with the former are not fully understood and so may not be mitigated adequately. For example, third-party entities have been at the forefront of payments products involving the Internet, which were subject to substantially more fraud when first introduced than they are today. This difference may explain, in part, why third parties are associated with higher risk in payments.

Second, third parties provide another entry point for risk and fraud in the upstream payment process. The transactions introduced by third parties are not necessarily more risky, but the payments system overall may be exposed to more risk if these additional

entry points' risks are not mitigated effectively. In this regard, Swendseid noted that third parties can only introduce payments into the system if enabled by a financial institution that consequently bears the responsibility for safeguarding these transactions. In referencing payments-related bank losses data, Swendseid emphasized that we should focus resources on better controls for those payment types with the most vulnerability based on actual data. This recommendation reinforces the importance of data collection and data sharing so that financial institutions and others know where to apply resources. Otherwise, risk mitigation initiatives may overly tax retail payments systems, with the unintended effect of making these systems uneconomic or driving the same transactions into riskier environments.

Roy DeCicco, managing director at JPMorgan Chase and chairman of NACHA's Risk Management Advisory Group (RMAG), discussed the work of the RMAG and indicated that no single silver bullet exists to address ACH risk issues. Fraudsters follow the path of least resistance, so it behooves the entire payments industry (across all channels) to manage vulnerabilities diligently. Among the RMAG's efforts, DeCicco highlighted a NACHA policy seeking voluntary registration of direct-access relationships for ACH debit originations. NACHA has enhanced network enforcement rules requiring originating depository financial institutions to report action plans when their customers exceed an unauthorized returns threshold, with increased fines for violations. New rules require standard identification requirements for originators and third parties so that account holders can better identify who is debiting their accounts. Other efforts under way include a negative watch list of "problem" ACH originators, a central ACH database and reporting tool combining operator and other data to allow for consistent data mining, and enhanced risk management tools, as well as a potential rule change to align NACHA rules with Regulation E.

Carter Messick, national bank examiner/lead technology expert at the Office of the Comptroller of the Currency (OCC), offered thoughts from a bank supervisory view. During a 2004 midsize bank horizontal review, OCC identified a number of issues related to third-party involvement in ACH, namely weaknesses in banks' risk selection and

customer due diligence. In payments-related supervisory activities that resulted in OCC enforcement action, he noted two driving factors. First, each case had third-party involvement. While banks can increase their ACH business through third-party relationships, they also introduce additional challenges related to compliance, due diligence, and risk management. The second related factor in supervisory concerns is allowing a sales culture to direct the ACH business in banks while insufficient attention and empowerment are given to risk management. Banks should instill a disciplined risk selection process with third parties and originators in the ACH business just as they do for lending and other lines of business.

Some suggested that bank regulators should require stricter risk management standards similar to those required by state enforcement action settlements. Limited rulemaking authority in this regard has led the regulators to rely upon guidance. It was suggested that NACHA issue a rule that addresses originator due diligence standards, either directly or by incorporating bank regulator guidance. Concerns were raised about the applicability of such guidance to banks of various charters and whether it could be made more succinct. Further discussion surrounded costs and benefits of stricter rule-based vetting and registration processes for all originators and third parties who enter the ACH network.

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 adequately promoted effective information gathering and sharing among all the parties who can have an impact.

Implications of Regulatory Enforcement Actions—Level-Setting and Debate

Richard Fraher, assistant general counsel and Retail Payments Office counsel for the Atlanta Fed, introduced some overarching themes regarding regulatory enforcement actions in the payments space. Banks must optimize risk management in payments

systems, which may require new risk metrics applicable to new products and new business relationships. While the 2008 Wachovia settlement with the OCC sent an important signal to banks about the consequences of risky payments relationships, it may have raised more questions than answers for banks trying to calibrate risk management decisions. Under what circumstances will a bank become liable for all financial losses that result from the bad behavior of the bank's customer or the customer's customer? What defines the scope of such exposure? On the other hand, from a consumer's perspective, the key question may be whether the remedies in the Wachovia matter went far enough to make sure that the victims would be compensated.[1] Aside from enforcement actions, Fraher noted that the examination process is placing new emphasis on retail payments, especially emerging payments processes. What is the optimal balance between examiners' judgments and bank judgments regarding risk and risk management in the payments business? Heightened supervision and enforcement activity is likely to improve risk management in bank-to-bank payments mechanisms and enhance the integrity of payments systems. On the other hand, enhanced supervisory attention creates compliance costs. How much additional compliance cost can the inexpensive bank-to-bank payments businesses, such as check and ACH, absorb? How will these costs be absorbed or passed on?

Jonathan Fink, special counsel at the OCC, discussed the OCC's ongoing efforts to address payments risks through supervision, guidance, interagency cooperation, and vigorous enforcement. He linked OCC enforcement activity to specific guidance, noting, for example, activity related to Internet payday lenders. Anecdotally, telemarketers turned to remotely created checks as better ACH risk controls came online. Enforcement remedies have included restitution to customers, funding of consumer education programs, and enhanced bank risk management programs. Sometimes banks have been found to have no contract with a payments intermediary, no audits, and/or no board reporting of such relationships. While banks must balance efficient payments with legal

[1] Note: the OCC entered into a revised settlement with Wachovia subsequent to this conference that directed the bank to issue checks to consumers that may have been harmed by payment processors for telemarketers that had account relationships with Wachovia. http://www.occ.treas.gov/ftp/release/2008-143.htm

compliance burdens, they generally are supportive of efforts such as NACHA initiatives and regulatory guidance because they see the value of maintaining safe payment networks. Highlighting the importance of information sharing for effective enforcement, Fink noted that while the OCC generally lacks enforcement authority over bank customers, it can quickly address bank issues when made aware on a timely basis. For example, OCC has addressed situations based on spikes in unauthorized return volumes detected via ACH operator processing data.

Elliot Burg, assistant attorney general of the State of Vermont, provided a state law enforcement perspective. First, consumers do not understand what protections they have and either do not know they have been victimized or otherwise fail to report it. Given this situation, he suggested reforms including direct compensation in lieu of claims-based restitution mechanisms, amending the Federal Trade Commission's Telemarketing Sales Rule to make new scams *per se* illegal, requiring banks and processors to review telemarketing scripts of their customers, providing a publicly available list of known bad actors, noting the nature of a transaction in account statements, and mandating that banks better explain funds availability to their customers to head off check scams. Second, remotely created checks (RCCs) are inherently risky. Barring an outright ban, he suggested requiring written consumer authorization as a means to mitigate fraud. Telephone-initiated RCCs, as well as TEL items within ACH, are particularly susceptible to fraud and therefore might justify bans. Finally, federal/multistate cooperative models need to be revisited. Leaving aside preemption issues, the states often have closer proximity to fraud victims, offering critical perspective, witnesses, and information, and have authority to bring together the banks, third-party processors, and originators. The states do parallel the enforcement work of the Federal Trade Commission, a model that has stood the test of time. Burg further noted that enforcement actions overall could be better tailored and made more effective by improved sharing of templates and remedial options.

Jay Lerner, assistant chief for strategy and policy in the Fraud Section of the Criminal Division of the U.S. Department of Justice (DOJ), discussed the roles of DOJ and federal

law enforcement in combating payments fraud, and provided case examples. He stressed the need for increased coordination and interaction among the banking, regulatory, and law enforcement communities; indeed, law enforcement could stand to learn more about payments systems and processes. Law enforcement relies on the technical knowledge of expert witnesses in investigating matters and presenting cases to a jury; the complexity of payments frameworks and globalization make this endeavor particularly challenging. He also emphasized federal interagency coordination efforts via working groups and task forces; in some instances, a regional approach is appropriate because fraud occurs across the country and may be local in nature. Sharing useful information is very important in these interagency coordination efforts, and much information can be shared despite certain legal restrictions.

Conference participants expressed interest in the development of the NACHA originator watch list and other "negative lists" efforts. Challenges noted included potential tort liability and easily reconstituted businesses under new names. With regard to fraudulent RCCs, more could be done to measure frequency and impact, and some felt that attention paid to RCCs was misplaced in the absence of good data. Also, discussion ensued regarding how available check and ACH processing data can best be used for supervision and enforcement purposes.

Consumer Issues in a Changing Environment

The third panel delved deeper into consumer protection and enforcement issues in the evolving retail payments environment. Mark Budnitz, professor of law at Georgia State University, discussed how consumers are affected as banks allocate risks and responsibilities in payment transactions. He cited numerous impediments to consumer protection arising from legal complexity, lack of knowledge or notice, highly confusing account agreements, a lack of control over how a payment is processed, confusing and even misleading banking jargon, and lack of clarity in options for redressing errors or fraud. Courts issue conflicting rulings, and the public cannot determine what laws govern which payment vehicles. Destruction of checks after conversion to electronic

format hinders the ability to prove counterfeits and alterations after the fact. Account holds can cause consumer overdrafts. Consumers are confused by convenience checks that credit card companies issue. Check 21 warranties and account agreement terms regarding truncation complicate matters. Cashier's checks used to be understood by consumers to be "good funds," but now they are often counterfeit. Consumers are forced to use costly arbitration processes where the arbitrator is not required to follow the law and where private proceedings prevent exposure of bad conduct by financial institutions to regulatory agencies or the public. Given all these concerns with transparency, consistency, and complexity of payments, placing additional responsibility for errors and fraud losses on the consumer does not make sense.

Asked what reforms might support improved consumer protections, Budnitz suggested uniform error resolution rights across payment types. The audience discussed some of the costs and benefits of uniformity. Some felt that while good data are available regarding bank losses, a lack of data likely hinders consumer protection reform efforts. Further, available data such as consumer complaints may be inadequate because they do not reflect the concerns of the "silent majority" of those affected. Additional mention was made of the problem of banks refusing to honor consumer revocation of electronic funds transfer (EFT) authorizations unless the company receiving the EFT payments also agrees to the revocation.

J. Reilly Dolan, assistant director of the Division of Financial Practices at the Federal Trade Commission (FTC), discussed two broad areas of FTC focus: (1) use of retail payment systems as a tool for fraud and (2) deceptive marketing of retail payments products. In May 2008, the FTC, in cooperation with more than thirty other law enforcement agencies, announced a telemarketing fraud enforcement sweep that included more than 180 cases, with both civil and criminal actions in the United States and Canada against fraudulent telemarketers. The FTC has brought successful enforcement actions against payment processors for unfair and deceptive acts and practices that may facilitate fraud. The FTC is concerned about some payment processors facilitating telemarketing frauds, such as by failing to perform or require adequate due diligence to confirm

consumer transaction authorization or by ignoring high return rates. Anecdotally, it appears that fraudsters may use processors rather than creating their own remotely created checks. The FTC is also concerned with some payday lenders, who can be "gateways" to other frauds such as identity theft and misuse of account information. With regard to deceptive marketing, Dolan provided examples of poorly disclosed fees for consumer cards that may lead to overdrafts or may wipe out the value of the card itself.

Discussion followed on how and when the FTC and state enforcement agencies share information with the banking regulators—for example, where there is action taken against a payments processor, who may in turn have business relationships with a particular bank. It was noted that despite efforts to deal with the banks' roles and the payments processors, the real challenges were in prosecuting the actual fraudsters. Dolan responded that a multipronged approach focusing on each "leg of the stool" is necessary. Dolan also noted that the FTC has a criminal liaison unit that refers appropriate cases to criminal authorities, often after the FTC brings a civil enforcement action.

Brainstorming, Debate, and Action

Conference participants participated next in cross-disciplinary breakout group discussions. Key themes and potential action items discussed included the following:

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 by 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.
- A more systematic, organized mechanism for information sharing, perhaps by establishing "brokers" for relevant information such as payments data.

Policing of Bad Actors

Beyond improved information sharing, participants were asked to bring forward ideas about how to better police bad actors. 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 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.
- 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.
- 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.
- Improving the clarity of consumer account statements by instituting standards and reducing jargon.

Potential Future Efforts of the Retail Payments Risk Forum

Finally, the assembled group was asked to identify areas of particular opportunity to leverage the Retail Payments Risk Forum. In addition to continuing the momentum by facilitating additional discussion among the participants assembled and furthering many of the efforts identified above, the participants also suggested:

- Sponsoring a special subgroup to improve ACH data sharing.
- Expanding focus beyond ACH and check systems.
- Formalizing a charter for the assembled group.
- Focusing on emerging risks.
- Performing consumer research, perhaps via focus groups, to identify opportunities to address gaps in consumer protection.
- Leading a project to create a roles/responsibilities matrix.
- Facilitating examiner, law enforcement, financial institution, and possibly consumer training and education.
- Sharing minutes/summaries of forum events.
- Hosting subgroups/different participants.
- Providing an inventory of collaborative efforts.
- Devoting resources to the highest-risk issues.

Conclusion

In summary, the diverse group of attendees gathered discussed numerous themes and issues of mutual concern, identified area of future action, and generally expressed a desire to continue the conversations begun at the conference. To that end, the Retail Payments Risk Forum intends to continue to host similar meetings to act as a catalyst for continued collaboration.