Emerging Retail Payments Risk Issues:

An Industry, Regulatory, & Law Enforcement Dialogue

Federal Reserve Bank of Atlanta

Retail Payments Risk Forum

November 5–6, 2009

CONFERENCE SUMMARY**

NOTE: The speakers' 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.

**** Authored by Clifford S. Stanford, assistant vice president and director, Retail Payments Risk Forum**

Hosted by the Retail Payments Risk Forum at the Atlanta Fed on November 5–6, 2009, this event provided a forum for improved understanding and mutual effort among invited experts to help address emerging risk issues in the dynamic retail payments environment. Approximately seventy national experts from more than thirty different industry organizations, regulatory agencies, and law enforcement agencies participated. Speakers and five expert panels discussed a range of relevant themes. Separate breakout sessions then allowed participants to discuss and develop actionable ideas on how to enhance understanding and collaboration. This summary captures the key themes explored during the event. Additional presentation materials and the results of polling questions asked during the event are available separately on the Retail Payments Risk Forum's Web site at http://www.frbatlanta.org/rprf/.

Welcome and opening remarks

Richard Oliver, executive vice president of the Atlanta Fed and retail payments product manager for the Federal Reserve System, opened the session. He described the Federal Reserve System's overarching role in fostering the integrity of U.S. payments systems. This is done via "overseer," "operator," and "facilitator" roles. It is the last role that led to creation of the Retail Payments Risk Forum at the Atlanta Fed. The Forum is a "catalyst for collaboration" among the variety of interests that must come together to discuss and ultimately to act together to help foster a safe, effective, and efficient payments mechanism to support our economy. Oliver stressed that given the complexity and dynamism of retail payments today, if we don't work together, we will risk failing separately.

Keynote Presentation

The event began with a keynote presentation from Catherine A. Allen, chairman and chief executive officer of the Santa Fe Group, titled "Transformation in Technology, Transactions and Trust: Challenges and Opportunities for Payments Risk Management." Allen provided examples of how trust has eroded among consumers, financial institutions, and government. She articulated how a continued loss of trust represents the ultimate emerging risk. Consumer and business memories will cause the "trust recovery" to trail an economic one. Simultaneously, financial services companies must adapt to an array of transformative new technologies presenting new opportunities and challenges. In this environment, public and private sector collaborative efforts are imperative to address emerging risks and to avoid unintended consequences of poorly informed policy choices.

Imagining recent financial crisis events as the "equivalent of an oil spill," Allen described a range of causes and their effects on the trust

environment for financial services. She referenced general causes, including excesses in executive compensation, ineffective risk management, an unbalanced focus on short-term profitability, and loose oversight by regulators. As a more specific example, Allen cited figures indicating that more than half of U.S. banks would not have been profitable in 2008 but for overdraft fees. A focus on fee revenue has caused an erosion of consumer trust in banks as fee practices became heavy-handed, and now this revenue stream is under threat. There will be lasting bad memories for those consumers and businesses that have experienced a breach of trust with banks and bankers. She predicted that as soon as the economy improves, we will see dramatic shifts in relationships between consumers and financial institutions. In this environment, financial institutions need contingency plans for reputational risk just as they do for operational disruptions or terrorism.

Citing surveys, Allen recounted how bankers are less liked now than are attorneys. And as the media continue to expose fraud and portray financial institutions negatively, consumer trust will continue to decline. New legislation and regulation have been introduced largely in reaction to the diminished trust in the financial industry. Allen referred to some changes seen recently to address negative financial services practices, but emphasized that changes overall have been merely "window dressing" to prevent more regulation, rather than fundamental changes. Further, while we are re-evaluating regulation of financial institutions, an increasing number of non-regulated firms are competing in the financial services sector. The trust environment is creating openings for these new market entrants. She predicted we will see more activity from companies outside the regulated realm, such as person-to-person (P2P) lenders and even traditional brick-and-mortar merchants. Allen predicted that these kinds of companies will likely begin to address consumer trust concerns before banks realize the opportunity.

Moreover, we are witnessing an evolution in technology portending dramatic change for financial services itself and introducing new risks. Allen singled out social networks and anything "mobile." Allen noted that there are approximately 77 million "Generation Y" individuals between 18 and 29 years old, many of whom are using social networks to communicate instead of e-mail. Of concern, the privacy of information on social networks is often difficult to control. Cyber thieves are targeting social networks. As financial firms adapt to this environment, old ways of combating fraud may not work. With regard to social networks, Allen defined four categories of emerging risks for financial services firms to consider:

- Reputational risk: negative information can spread very quickly;

- Regulatory risk: greater oversight and unintended consequences may result;
- Security and identity theft risk: more civil suits may emerge; and
- Productivity risk: social networking can distract from working.

Allen described how more payment transactions will be processed remotely, including via the mobile phone platform by nontraditional institutions. This practice will raise new questions. For example, how will liability for losses be allocated among the various parties involved in a mobile payments transaction? She noted that consumers, despite such uncertainties, may nevertheless trust nontraditional players providing mobile payments services even if it means higher risk, so long as they distrust financial institutions in the current environment. Allen further stressed that the industry must be mindful of new uses of existing infrastructure in ways that may present unanticipated risks. For example, prepaid cards started as a product for the unbanked and now are becoming mainstream, raising new questions about consumer protection.

Despite a challenging overall picture, Allen noted that there is much the financial services community can do proactively. She emphasized that perhaps the industry has an unprecedented opportunity for transformative thinking. She is optimistic about the work of various public/private partnerships such as the Retail Payments Risk Forum, BITS, the National Foundation for Credit Counseling (NFCC) Advisory Board, and the Santa Fe Group Vendor Council, referring to the last group's work on an "identity theft bill of rights." A network of trust must be built through these types of forums. In order for these and other such efforts to work, they will need senior leadership involvement, a structure that creates an environment of openness and trust, and dedicated staff behind the scenes to keep momentum.

Allen suggested that industry leaders need to demonstrate leadership going forward, and most have not done so effectively. First, she believes that senior leaders of financial services firms need to apologize to customers in order to rebuild some of the trust. Second, firms collectively need to take a holistic, cross-channel approach to risk issues, putting customers in control. Customers can become a trusted partner to help fight fraud if given the right tools and information. Third, the industry has much to do to promote transparency in banking practices to consumers, such as by providing them with "just-in-time" information about a transaction in clear terms. Fourth, the treatment of customer data must have a secure environment. Finally, she advocated for improved consumer financial literacy education.

Allen concluded by challenging the assembled group and the Retail Payments Risk Forum to consider five focused initiatives:

- Creating a “trust coalition” to research and bring together consumer groups, educators, regulators, financial institutions, legislators, and nonbank entities to explore how to restore trust between consumers and financial institutions;
- Brokering discussions between the mobile carriers, device manufacturers, vendors, financial institutions, and regulators regarding security, liability, and standards issues in the emerging mobile payments arena;
- Facilitating discussions among appropriate government agencies—together with social networking companies, application providers, marketers, and financial services firms—to develop best practices regarding transaction security and policies on social networks;
- Developing frameworks for risk management of emerging uses of the ACH via remote channels such as the mobile phone; and
- Promoting industry and institutional focus on cross-channel fraud management.

Panel 1: Emerging payments market developments—trends and risks

Cynthia Merritt, assistant director of the Atlanta Fed Retail Payments Risk Forum, moderated the first panel, which included Marianne Crowe, vice president at the Boston Fed, and James Van Dyke, president and founder of Javelin Strategy and Research.

The panelists provided a high-level overview of the state of the retail payments environment, including market developments, emerging risks, and risk mitigation efforts and opportunities. Continued investment in innovation is driving the development of new payment devices and channels despite the economic downturn. This environment creates new choices for consumers and businesses and drives efficiency improvements overall, but may also introduce new challenges and risks for which stakeholders may be unprepared.

Panelists noted contactless payments using microchips and near-field communication technology, mobile phone-enabled platforms, and social networking platforms as areas to watch. While slower to take hold in the U.S., the growing ubiquity of cell phones in developing countries has encouraged a rapid adoption of mobile phones for P2P payments and remittances, as well as the use of stored value on phones for the purchase of goods and services. Social networks are emerging as potential payments intermediaries, particularly for small-value payments in e-commerce. For example, both Facebook and Twitter have permitted third-party developers to provide payment applications on their service platforms.

Marianne Crowe highlighted a range of factors that are influencing payments markets, including a continued shift to electronic payments (noting a lag for business-to-business (B2B) payments), increased non-bank competition, increased use of Internet-enabled payments, shifting demographics, changing consumer and merchant preferences, technology advances, emerging risks, and new regulation. As one example, Crowe discussed developments in the debit card arena. Recent data and the Federal Reserve's most recent retail payments study (2007) have shown debit cards as the fastest volume growth category, displacing cash, checks, and credit cards at the point of sale. Debit card products include signature- and PIN-based models, but also are evolving to include innovations like "decoupled" debit cards, prepaid card models, and contactless technology. Newer developments also include virtual, single-use debit card numbers and "floating" PIN-entry pads for Internet-based debit card transactions.

Crowe noted that more consumer bill payments are moving online, due in part to consumers' increasing comfort level with this environment and its convenience—a positive sign of value in a banking product. More broadly, the opportunity for increased Internet-enabled payments remains huge, although the current economic situation has temporarily resulted in negative growth in online sales.

Alternative payment methods span multiple models provided through a wide variety of online payment service providers. Crowe highlighted the P2P payments market as an area to watch for innovation. The Fed's 2007 retail payments study found that 6.6 percent of checks (206 million items) paid in 2006 were consumer "casual," or P2P, checks. This segment is currently dominated by independent service providers such as PayPal. However, the success of online banking is beginning to drive interest in bank-enabled P2P systems. In addition, mobile banking is postured as a feasible channel for P2P payments.

Most large banks in the U.S. today offer some form of mobile banking, permitting customers to check balances, receive alerts, pay bills, or transfer funds among accounts. Crowe provided a range of analysts' predictions of strong growth in U.S. mobile banking going forward. However, mobile payments, involving the use of a phone for purchasing goods and services, have seen less traction. Crowe described the obstacles to the growth of mobile payments in the U.S. These factors include a lack of technology standards for interoperability, regulatory gaps, unresolved liability issues, and concerns with security, privacy, authentication, and fraud. A business model encompassing customer ownership, support, and revenue-sharing must be developed, whereby the mobile payments customer is shared by a bank and a telecom carrier. Finally, an overarching need for consumer education to influence demand exists.

Crowe noted that in this evolving environment, where new, nonbank players will continue to enter the payments space, the risk attributes are changing and not well understood. Consumers are faced with many payment choices and may be unsure about benefits and risks, so consumer education and collaboration among payments stakeholders is needed to ensure a safe environment.

James Van Dyke introduced key trends from his perspective, drawing on research by Javelin. He emphasized that while we must always be attentive about what could go wrong in the emerging payments environment, we should not let our fears cause us to ignore positive opportunities. In particular, new technologies and payments models offer opportunities to partner with the customer, empowering them to offer better control over customer data and help prevent threats such as identity fraud.

According to Javelin research, the incidence of fraud in general has declined in the U.S. in recent years. However, identity fraud has increased to as much as $48 billion of losses in 2008 and touches all payments channels. Van Dyke indicated that the nature of fraud is changing and fraudsters are moving faster, although low-tech methods are still common. Security and fraud represent significant drivers of new technology expenses, and security is the key driver of consumer choice of payments products. A good deal of fraud is "friendly": one in ten victims can identify the perpetrator. Javelin's research found that fraud was four times higher among data-breach victims than consumers at large, but consumers have a poor understanding of their risk following a data breach despite receiving notice. Further, this lack of understanding may be increasing the time to detect fraud and causing higher out-of-pocket costs.

Van Dyke expressed that mobile finance introduces complexity and risk, but also creates new opportunities for authentication via the handset and mobile network operators. A key error of the past has been the failure of the industry to partner with consumers to protect their identity information, which limits the effectiveness of security efforts and excludes relationship-based profitability benefits. Going forward, he advocated a reassessment of the roles that companies and individuals play with regard to protecting identity records and the sharing of fraud costs, which can lessen the overall impact of fraud for everyone.

Panel 2: Industry perspectives on emerging risks and public/private engagement

Duncan Douglass, partner at the law firm of Alston and Bird, moderated the second panel, which included Jane Larimer, executive vice president and general counsel of NACHA; Dan Miner, principal with Treasury Strategies Inc.;

and Rue Jenkins, assistant treasurer of Costco Wholesale.

In her remarks, Jane Larimer described how NACHA seeks to monitor and respond to ACH risk events in a way that minimizes the long-term effects on consumers and financial institutions. ACH network volume has grown for many years as usage has expanded into new forms. NACHA has increased its attention to risk and fraud mitigation, and since 2001 the ACH network has experienced steadily lower rates of return for unauthorized ACH debit entries—a leading indicator of misuse of the ACH. This rate was at an all-time low of .04 percent for 2008. Larimer referred to anecdotal evidence to suggest this trend is correlated with a rising use of remotely created checks, which are less easy to monitor. This situation highlights a need for tools to manage risk across all payment channels.

Larimer noted that the 2009 Association of Financial Professionals Payments Fraud and Control Survey (AFP Survey) found that only 17 percent of companies that experienced ACH-related fraud attempts incurred actual losses. She expressed that those organizations that incurred losses likely failed to adopt best practices such as debit-block tools and ACH positive pay.

Larimer discussed the emerging risk represented by corporate account takeover schemes, in which fraudsters gain online account access and send funds via ACH credits and wire transfers to accomplices. Referring to the successful monitoring of unauthorized ACH debits, he said that the ACH network may be facing a paradigm shift to a focus on unauthorized ACH credits, an area that is challenging to monitor and where insufficient benchmarking data exist. NACHA works with law enforcement and regulators to communicate risk issues and best practices to financial institutions and others in an effort to preclude future fraud schemes. Larimer also expressed support for industry efforts to better partner with business account holders to empower and encourage them to keep their personal data more secure.

Dan Miner considered the payments risk and fraud picture from the perspective of banks and their business customers. He noted the challenge that financial institutions face as they must consider, by his count, more than one thousand different standards in the payments legal and regulatory context. This burden is made more complex as financial institution risk management and compliance efforts are fragmented by the product type, with their own management structures attached to separate profit centers. Often, no central repository for information about risks affecting an institution exists, which can foster a lack of consistency in risk management, ineffective governance, and poor compliance.

Considering the risk to businesses from payments fraud, Miner suggested that businesses should take greater responsibility for their

accounts and make better use of bank monitoring services, third-party tools, and internal controls. Echoing Larimer's comments, Miner reiterated that businesses are not taking full advantage of available tools like positive pay and debit blocks. He suggested that among other options, businesses should reduce the number of bank accounts used, monitor them daily, and reduce or even eliminate check payments, particularly given the persistence of check-related fraud as seen in the AFP Survey. He also suggested time-tested practices such as ensuring operational dual controls and segregating duties.

Rue Jenkins described the payments environment for Costco Wholesale. In terms of outbound payments to suppliers and service providers, while check usage does persist, Costco has significantly increased its use of the ACH. On the inbound side, Costco has limited credit card acceptance for Visa and MasterCard. In the alternative payments area, Costco is now accepting payments online via eBay's BillMeLater service, piloting a closed-loop PIN debit/ACH card product in Puerto Rico, and exploring other point-of-sale alternatives.

Jenkins, also chair of the AFP's Payments Advisory Group, noted that the 2009 AFP Survey reported the highest amount of attempted or actual fraud in checks. Even while check volume is declining, the survey found that median fraud loss to businesses from checks rose from 2007 to 2008. Jenkins noted that fraud attempts on merchants are hard to monitor, so constant corporate and bank communication is required, and education of staff is increasingly critical. He also advocated protecting corporate accounts with tools such as filters and blocks. Costco views payments breakdowns as reputational risks. He recounted scenarios in which Costco effectively avoided losses but had difficulty getting law enforcement interested in investigating the sources of the fraud attempts. He expressed that this was a common challenge in the corporate environment.

Duncan Douglass asked the panelists if they felt that tools available to businesses were adequate in light of the newer fraud schemes such as account takeovers, which he analogized to "corporate identity theft." The panelists agreed that the tools are generally effective but indicated that both the business and the financial institution have to implement them properly. More education is needed for less sophisticated business customers, who are more like consumers. Larimer pointed out that NACHA is developing toolkits for financial institutions to educate their customers. Miner noted a need to develop transaction patterns and to add more neural intelligence into monitoring systems for check and ACH payments, akin to card systems.

Acknowledging that the regulatory landscape today is very protective of the consumer, Douglass asked the panel if they saw a need for

additional regulation to protect businesses. The panel agreed that sufficient regulations and commercially reasonable control mechanisms already exist, but much more can be done by enforcing what is already in place. The very threat of new regulation could motivate banks. Some felt banks already carry a significant burden, whereby they are "deputized" to assume liability for enforcing payments-monitoring regimes, such as with anti-money laundering compliance, Office of Foreign Assets Control (OFAC) screening in the context of international ACH, and illegal online gambling prevention. Some considered the OFAC requirements embedded in the new international ACH transaction (IAT) rules from NACHA as especially onerous, pointing out that the ACH system was designed for low-value payments and the low cost did not anticipate additional compliance burdens.

Data breach presentation

The conference shifted focus to emerging risks to payments systems arising from cyber security threats. Chris Novak, managing principal at Verizon Business, described the overall environment for data breaches, drawing on Verizon's 2009 Data Breach Investigations Report. According to this report, most of the data breach incidents in 2008 involved external parties. However, 39 percent of the breaches involved combined external and internal or "partner" actors (meaning third parties with some authorized access), revealing a concern about collusion with trusted insiders. Distinguishing between a breach incident and the records exposed by such a breach, Novak said that more than 90 percent of the records compromised by external breaches were attributed to organized crime activity. One dramatic finding indicated that 8 percent of data breaches resulted in a compromise of more than ten million records per breach.

Novak described the highly-evolved black market for compromised records, such as payment card records, whereby buyers and sellers negotiate via "carding forums" or IRC chat communications. Payment card data is desirable because it is easily converted into cash. Hackers sell data to wholesalers, who break it up for retailers. Sellers sometimes offer money-back guarantees. "Mules" are used to fence stolen data for cash. Novak noted that stolen card data has a long shelf life. Authentication credentials are highly valued because they provide deeper account access. Carding forum sites are often hosted outside of U.S. jurisdiction. When shut down in one country, they easily switch over to a site hosted in another, making investigation and deterrence very challenging.

The majority of breaches are linked to hacking (64 percent) and malware (38 percent), with most malware installed by a remote attacker. A common malware installation technique is "SQL injection," whereby malware code is introduced

into a Web site. Novak noted that applying software patches to coding gaps is effective but these patches may not be applied comprehensively. Malware most commonly functions as a "keylogger," storing data such as online banking credentials, or it creates a backdoor opening for a hacker to enter a system. With regard to payment cards, malware may be used to monitor card authorizations, as hackers value accounts in good standing. Novak noted a trend toward customized malware—attackers specifically design code to attack a particular system. Targeted, as opposed to random or opportunistic, attacks have increased. Given that the most challenging breaches to accomplish account for nearly all of the compromised records, these trends collectively point to the increased sophistication of attacks.

Novak described the timeline of data breaches from pre-attack research through post-breach resolution. While the extent of necessary pre-attack research varies, once a breach occurs the information is usually compromised within days. However, Novak showed that victim awareness of a breach lagged significantly, with 49 percent of all breaches remaining undiscovered for months.

With regard to the Payment Card Industry Data Security Standards (PCI DSS), designed to provide minimum standards for protection of card data at merchants, processors, and elsewhere, Verizon's investigations indicated gaps in compliance were correlated with breaches. For example, in post-breach investigations, Verizon found that only 11 percent of breached firms were in compliance with the PCI DSS standards for protecting stored card data. Only 5 percent of these firms tracked and monitored access to data. Novak noted finally that of the recommendations Verizon makes to data breach victims, the majority were characterized as "simple and cheap," indicating that much can be done to avoid these data breach threats on the front end.

Panel 3: Data breaches in payments systems—Roles and best practices for the public and private sector response

Brad Beytien of the Federal Reserve Board's division of bank supervision and regulation moderated the third panel, which consisted of John Carlson, senior vice president of BITS, Jim Devlin, special adviser for operational risk at the Office of the Comptroller of the Currency, and Don Rhodes, director of risk management policy at the American Bankers Association.

Beytien emphasized that data breaches are precursors to payments system risks, and described examples. These threats are publicized and related alerts provided to banks, but the techniques evolve constantly and quickly. Given the increasing incidents of payments fraud, some commentators have begun to question the efficacy of the current customer authentication

standards deployed across the industry. Others have suggested that these exposures could threaten the viability of smaller banking institutions, particularly in cases where institutions have outsized payments business relative to their capital.

Jim Devlin described a public/private sector framework, known as the Financial Banking Information Infrastructure Committee (FBIIC) - Financial Services Sector Coordinating Council (FSSCC) Cyber Security Committee, whose mission is to work with the financial services sector to strengthen cyber security and the resiliency of the sector's current and future IT operations. The committee's objective is to create a shared view of cyber threats by leveraging federal government resources. Among other activities, the committee develops and executes cyber security exercises to identify risk issues, with the latest exercise, known as "Cyberfire," accomplished in September 2009 and involving more than ninety different organizations. The committee is developing a framework for improved information sharing, including by gaining security clearances for more than 100 critical private-sector individuals. Devlin discussed international issues of interest to the committee, including mobile devices and international telecommunications infrastructure. Included in the committee's long-range efforts is developing a financial services sector "threat matrix" to help focus future collaborative efforts with organizations such as SANS, U.S. Computer Emergency Readiness Team (CERT), and the Financial Services-Information Sharing Analysis Center (FS-ISAC). Devlin noted that top threats today include identity theft via malware, loss of telecommunications, and threats from insiders.

Rhodes described corporate-account takeovers as perhaps a logical extension of criminal activity using phishing and other such techniques. Phishing is the fraudulent activity criminals use to acquire sensitive information such as user names, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. While phishing attacks are sometimes targeted espionage on key individuals with large accounts ("spear-phishing" or "whaling"), fraudulent access to non-consumer accounts can be especially attractive to criminals because one successful breach can result in major financial gain. To illustrate the point, Rhodes described a 2009 case in Kentucky. A county treasurer's credentials were compromised by the Zeus Trojan, a key-logging malware that allowed criminals to log in to county bank accounts from the treasurer's computer. The Zeus Trojan malware can be loaded just by opening an email, which is usually sent to treasury management staff and may draw attention by looking official, like a fake subpoena. In the Kentucky case, similar to many other recently reported cases, fraudsters transferred funds in increments of less than $10,000 from the compromised account to

"mules" set up as county employees. The fraudsters had recruited the mules through work-at-home job Web sites. These mules kept a portion of the funds and sent the remainder through non-bank money transfer systems to accounts in the Ukraine. The county lost more than $415,000 to this fraud. This and numerous similar cases were uncovered in 2009 by the Washington Post, which recently reported FBI estimates of $40 million in actual losses from similar attacks in recent years.

Rhodes suggested that awareness is critical—businesses need to understand what data is the most sensitive, know where it resides, and assess controls according to the risk. Some experts have suggested taking practical steps to address specifically the corporate-account takeover threat, such as using a stand-alone computer with a non-Windows operating system and no e-mail capability to access business accounts online. Rhodes also reviewed an array of resources available to help banks and business customers understand and address cyber threats, and discussed various initiatives sponsored by the American Bankers Association.

John Carlson reviewed BITS and FSSCC security, fraud, vendor management, and regulatory compliance activities, including outreach to academic, technology, and government communities and developing initiatives to improve the resiliency of the financial services sector. Specifically, Carlson discussed the following BITS efforts:

- Public/private partnerships among financial institutions, third-party (non-bank) payments providers, and law enforcement to address payments fraud and cyber security threats;
- Initiatives to improve Web security and ongoing engagement with the Internet Corporation for Assigned Names and Numbers (ICANN) concerning a proposal to establish new generic top-level domains that could include domains with finance-oriented names;
- Development of e-mail authentication protocols to reduce spam and the transmission of malware through e-mails;
- Surveys on current authentication practices for financial institution customers, employees, and business partners; and
- Expansion of the BITS Shared Assessments program, which helps financial institutions more efficiently oversee third-party providers.

Carlson noted that BITS is involved in continuous dialogue with experts in the federal financial regulatory agencies and is also involved in efforts to monitor legislative proposals regarding cyber security. Carlson added that in 2010, BITS plans to focus on

"cloud computing" and the security effects of social networking technologies and consumer behavior.

Carlson concluded by describing several research and development activities within the FSSCC structure that Delvin discussed, including outreach to academic, technology, and government communities. In particular, Carlson mentioned discussions with senior White House officials on strategies to improve identity management and a proposed research project to establish a financial services "sub-net" within government-controlled domains to enable experimentation with strong B2B and business-to-government (B2G) authentication technologies.

Panel 4: Law enforcement perspectives

Jay Lerner, assistant chief for strategy and policy, Fraud Section, Criminal Division of the U.S. Department of Justice, moderated the last panel of the first day, along with supervisory special agents Andrew Bonillo of the U.S. Secret Service and Michael McKeown of the FBI.

Jay Lerner discussed the Fraud Enforcement and Recovery Act of 2009, including the key provisions relevant to financial frauds. He described the recently formed Payments Fraud Working Group, an interagency group representing law enforcement, financial regulators, and other agencies seeking to improve information sharing and awareness of payments fraud trends and issues. This working group was one of the ideas that emerged from a 2008 event that the Retail Payments Risk Forum sponsored. Lerner also described the Justice Department's ongoing work to address cyber threats and related frauds.

Bonillo emphasized that efforts to promote trusted collaboration among government agencies and with the private sector are critical to address cyber crime. Fraudsters are sharing information in sophisticated ways already, such as on Web forums, so it takes dedicated efforts to keep up. He emphasized that criminal hacker activity is now about stealing money, not about "ego-tripping." Personal and payments-related data such as card information has become a commodity on the black market. In some sense, privacy protections for consumer information can be at odds with effective enforcement, and the fraudsters know this. Bonillo indicated further that as soon as the industry adopts a standard, such as end-to-end encryption of payments data, hackers will be trying to break through. These kinds of security measures may serve to shift civil liability, but they will not deter hackers for long.

Bonillo described how the Secret Service is partnering with technology firms to understand emerging issues and technologies, including, for example, social networking sites. Bonillo said that law enforcement has a thirst for data on an

ongoing basis to help with its efforts, even if it is old data, citing examples when such data has been helpful to spot "signatures" of fraudsters in investigations emerging years later.

Michael McKeown described how the FBI is working through a public/private partnership known as the National Cyber Forensics Training Alliance (NCFTA) to develop new means to track and investigate account takeover frauds. The FBI is investigating money mules, and McKeown mentioned a recent FBI alert on the issue. He said that in this regard the FBI is going after all cases and not just the high-dollar cases. Through the NCFTA, the FBI is working with the U.S. CERT group at Carnegie Mellon University to analyze the Zeus malware and provide law enforcement with intelligence for their work to address this problem. McKeown also discussed various other past investigations, including the successful DarkMarket carding forum sting.

McKeown stressed that law enforcement wants to know about cases of attempted fraud without losses. He noted further the importance of suspicious activity reports (SARs) filed by financial institutions, which are actively used by law enforcement to detect trends and accomplish investigations—for example, to help identify money mules. While McKeown said that Zeus is the biggest problem currently, tomorrow's vulnerabilities may come in the areas of telecommunications and social networking. We can expect old-school exploits on these emerging delivery services for payments.

Panel 5: Practitioner's perspectives on emerging payments risks

Shirley Inscoe, director of financial services solutions for Memento Security, moderated the final conference panel, which also included panelists Mark King, senior vice president at Bank of America; Devon Marsh, senior vice president at Wells Fargo; and Erik Stein, vice president at Fiserv.

Mark King noted that the industry and its customers today face crime rings with long-term plans, sophisticated communications, and capital to fund their enterprises, constituting what King referred to as "Fraud Incorporated." Among other things, this threat is driving change in the way that banking services are offered and protected. Bank of America created cross-channel and cross-product fraud monitoring programs to ensure better internal sharing of intelligence. He suggested that this sharing model needs to be replicated in a cross-institutional environment as well. Further, he suggested a more holistic engagement with law enforcement to increase timely intelligence sharing and improve prosecution of fraud perpetrators. King expressed that banks have strong incentives to protect their customers. Citing regulatory limits on consumer liability for card fraud losses as an example, King

questioned whether consumers have sufficient incentives to do their part as well.

Devon Marsh noted that while emerging payments mechanisms often also bring forth new risks, he reflected on how Wells Fargo is using a mix of old and new risk management methods simultaneously to address them. Some tried-and-true techniques like dual operations controls remain valid and should not be abandoned with new payment methods.

Erik Stein discussed some relevant trends from an international perspective. He noted that while the United Kingdom has moved to chip and PIN card technology to stem card fraud losses, card fraud has now migrated to card-not-present transactions on online and telephone channels, and to cross-border transactions in countries where chip and PIN is not used. A similar fraud migration might be expected to come to the U.S. from other countries that adopt chip and PIN, particularly as Canada is now moving to adopt this technology as well. Stein indicated he did not see the U.S. moving to chip and PIN as a security solution as the U.S. market has too much invested in legacy systems. With the advent of near-field communications (NFC) used by mobile phones, Stein noted that the U.S. may bypass chip and PIN by using a mobile phone at the merchant terminal, avoiding the costly transitional step of updating card technology.

Stein noted how merchants in the U.K. are driving changes in consumer payments behavior. For example, two of the largest retail grocery chains post signs at the tills refusing to accept checks, driving consumers to use debit cards or cash instead. Emerging economies, Stein noted, show evidence of the disintermediation of banks in emerging payment schemes, such as M-PESA in Kenya, Tanzania, and Afghanistan. M-PESA is a P2P payment scheme requiring no bank account and available to registrants on the Safaricom mobile network. In its first two years of operation, M-PESA had more than six million registered customers, and is processing more than two million transactions a day.

Shirley Inscoe then led the panel and the audience in a lively discussion of various key topics. She described how most information sharing relies on private-sector initiation, and you have to “give to get.” She also discussed Early Warning Services (EWS), an industry joint venture providing transaction and account verification services among banks and check acceptance companies. For example, EWS has been successful in link analysis of demand deposit account, check, and ACH transaction-related information provided by banks, but also noted that, as yet, no link to other information, such as card transaction data, exists to enable cross-channel analysis and detection. EWS has an aggressive strategic plan to expand their fraud prevention capabilities across all payment systems.

The panelists discussed complications and costs resulting from diverse identity management systems in the U.S. (e.g., state drivers' licenses). Further, citing the $5 inquiry charge imposed by the Social Security Administration for verifications, they agreed that costs for banks to authenticate identity are untenable. Currently, industry discussions and efforts regarding the use of tokens for authentication and of separate channels to authorize transactions are taking place. The use of dual controls such as callbacks to verify a transaction is a traditional method used by small banks that is still very effective. However, panelists noted that this kind of effort is expensive for banks, and banks may be reluctant to burden their customers. Moreover, due to the sunk costs in existing systems, banks are reluctant to invest in new risk management tools overall.

Remotely created checks (RCCs) have been abused by fraudsters, in some cases resulting in liability for the bank accepting the deposit of those items by their customer. Marsh described how banks can mitigate their risk by adopting an onboarding and screening process for likely RCC depositors so that they can monitor them in the same way they do ACH originators. Also, at account setup, banks could modify their "know your customer" (KYC) process to detect potential money mules by asking the account opener whether they are opening the account at the behest of an employer they recently found on a job posting board. Another panelist commented further that it is important to leverage transactional analysis tools to detect fraud early and to look for opportunities to blend in image analysis given that most checks are now collected in image form.

Panelists called for improved public/private collaboration efforts, including more inclusive forums. They noted that many law enforcement task forces do not include financial institutions as members, and that financial institution investigators have information valuable to law enforcement and may in many cases be duplicating efforts. Panelists expressed support of law enforcement efforts to arrest money mules to send a deterrence signal to others caught up in these widespread scams, and suggested that resources were better deployed in that effort than in having law enforcement monitor transaction patterns directly.

Breakout sessions

Participants were then asked to discuss key topics in smaller breakout groups. The task presented to each group was to develop some actionable ideas to promote improved understanding and collaboration on emerging retail payments risk issues, and to then report on those ideas to the full session. The groups derived a range of such ideas:

- Given the multifarious efforts of the public and private sectors to address payments risk issues and the potential for conflicts or duplication, a matrix identifying these efforts, their stakeholders, and possible gaps and overlaps is needed to guide future action. The Retail Payments Risk Forum was suggested to foster this effort.
- A law enforcement-driven task force that engages the private sector could help to drive collaborative action to address the threat of "Fraud Inc."
- A policy effort to address authentication costs imposed on payments providers by inefficient and diffuse identity management systems provided by government could improve the odds of effective private-sector deterrence of fraud.
- Educational efforts to help consumers, companies, financial institutions, and others understand fraud threats are needed.
- Support for early development of standards that include effective risk management controls in the mobile payments arena will help avoid problems as this market develops.
- Better data is needed from surveys, regulatory reporting, and other means to help the industry understand risk trends, benchmark risk levels, and identify mitigation efforts.
- Given the continued emergence of non-banks as key players in payments, one group suggested that more could be done to integrate those firms into existing financial services collaborative forums.
- An ongoing assessment of regulatory gaps is needed with regard to the continued emergence of new players in payments markets.
- To address authentication concerns in online banking environments, some suggested a legislative or regulatory mandate, or strengthening of existing regulatory guidance, such as by mandating multi-factor authentication.
- Combining bad-actor databases and records among various payments networks, such as between the card and ACH environments, would improve efforts to prevent fraud migration and mitigate cross-channel fraud risks.

Conclusion

This conference offered the participants a deep and broad update on trends and issues of the day as the payments industry, regulators, and law enforcement all seek to work together to understand, mitigate, and deter risks and fraud in the emerging payments environment. Clearly, further work remains to be done, and the landscape is ever changing. But the challenges faced are common to all parties, presenting an

imperative for common understanding,
information sharing, and collaborative action.