FEDERAL RESERVE BANK *of* ATLANTA

PORTALS & RAILS

2009 COMPENDIUM

Retail Payments Risk Forum

A CATALYST FOR COLLABORATION

Founded in 2008, the Retail Payments Risk Forum is housed at the Federal Reserve Bank of Atlanta. The forum is designed to bring together expertise residing within the Federal Reserve, financial institutions, other industry participants, regulators, and law enforcement. The forum facilitates collaboration among these diverse parties, all of whom share common interests in improved detection and mitigation of emerging risks and fraud in retail payments systems. The forum accomplishes this by providing resources to research issues and sponsor dialogue.

PORTALS&RAILS, a blog sponsored by the Retail Payments Risk Forum of the Federal Reserve Bank of Atlanta, can be found online: **portalsandrails.frbatlanta.org**

PORTALS & RAILS

2009 COMPENDIUM

CONTENTS

THIRD QUARTER 2009

FOURTH QUARTER 2009

FEBRUARY 02, 2009

Welcome to Portals and Rails

It is my pleasure to welcome you to Portals and Rails, a blog sponsored by the Retail Payments Risk Forum of the Federal Reserve Bank of Atlanta. The purpose of Portals and Rails is to encourage ongoing dialogue on emerging issues in retail payments and to inform and guide the work of the Retail Payments Risk Forum.

The Retail Payments Risk Forum was established to address the challenges faced by the industry, bank regulators, and law enforcement in managing retail payments risks and to enhance collaboration among these parties to detect and mitigate fraud. As the U.S. retail payment systems continue to shift from paper to electronics, bringing with them the introduction of innovative payment instruments and channels, the risk profiles of payment participants are also shifting. The most recent Federal Reserve payments study, conducted in 2007, revealed that the use of electronic payment methods is growing rapidly in response to technological advances in computing power and telecommunications, as well as changes in user preferences. This growth is accompanied by increased nonbank participation in payment systems. While nonbanks play a vital role in a variety of different payment activities, their increased role in retail payment systems introduces new and often unanticipated risks.

All this is not to say that legacy payment instruments and channels are outside the scope of our radar. Paper and electronic checks remain important components in the retail payments landscape and unfortunately are increasingly products targeted by bad actors as entries to retail payment systems to conduct fraudulent transactions. The Retail Payments Risk Forum is initially focusing on trends in checks and in the ACH network, drawing on the expertise housed within the Federal Reserve System's Retail Payments Office, also geographically situated at the Federal Reserve Bank of Atlanta. The Retail Payments Risk Forum will seek out opportunities for collaboration with other existing forums, such as those for card-based payments, where appropriate.

To meet the challenge of addressing the myriad new risks in retail payment systems, the Retail Payments Risk Forum has established Portals and Rails as a means of introducing ideas, asking questions, and facilitating communication among interested parties on various topics relating to retail payments risk and fraud. We hope Portals and Rails provides you a virtual arena for collaboration and discussion of issues of common interest.

We encourage your participation in Portals and Rails and look forward to ongoing collaboration with you.

By Richard R. Oliver, executive vice president of the Retail Payments Risk Forum at the Atlanta Fed

FEBRUARY 02, 2009

Retail payments risk and fraud: detection and mitigation

The Retail Payments Risk Forum hosted a conference titled "Risk and Fraud in Retail Payments: Detection and Mitigation" at the Federal Reserve Bank of Atlanta on Oct. 6–7, 2008. This conference provided a collaborative forum to facilitate information sharing among experts and 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.

The proceedings of the conference are summarized in the full-length conference summary, which can be found as text or pdf. We encourage you to review the conference summary and also to provide any comments you may have within Portals and Rails. In particular, we want to know what you thought of the topics addressed. Did the discussions reflect your understanding of the issues? Did we miss anything? What topics would you like to see addressed in future such events? How do we best ensure ongoing collaborative work among industry, regulatory, and law enforcement parties in the detection and mitigation of retail payments risks and fraud? Your thoughts are very valuable to us!

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

FEBRUARY 23, 2009

Why should I work with you?

At some level, we're all selling something, even if it's just ourselves. Everyone has a reputation and a résumé to build. Information is power. We all have bosses to please, goals to meet. So when and how do these stars align such that we can work together?

Payments is a network industry with chicken-and-egg problems. It requires someone to step forward, perhaps to risk losses, in order to build networks of users and providers that enable a payments network to operate. Think of a simplistic credit card network—users need to know that merchants will accept it, banks need to know that they can make money to provide the lending that backs it, and merchants need to know that they'll be compensated with business in order to justify the costs.

The same dynamics apply to those who are minding the store when it comes to addressing risk and fraud in payments networks. Who's willing to step out (at some risk) to take on the tough challenge of pulling the variety of industry, regulatory, law enforcement, merchant, and consumer interests together? Where's the money to be made? Where's the competitive advantage?

In the best sense, law enforcement is imbued with an altruistic drive to do good by catching the bad guys, and bank supervision is all about ensuring a safe and sound banking system.

In the best sense, payment services providers seek to provide a safe and efficient environment for the exchange of value. But will any service provider risk exposure to reputational and other risks just because it's good for the payment system?

Payments is also an industry that offers opportunities to leverage positive "network effects"—the more users of a payment mechanism make it more valuable for all as it becomes more ubiquitous, commonly understood, and efficient. The same network dynamics should apply to those who are minding the store when it comes to retail payment systems risks.

All these interests and perspectives can align if we are realistic in our approach to interest alignment and continue to collectively look for opportunities of mutual benefit.

Where do you see alignment and opportunity?

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

MARCH 10, 2009

B2B: Will checks ever really go away?

While check writing in the aggregate is on the decline, one last bastian may remain in the business-to-business (B2B) arena. While consumers are adopting electronic payments at an increasing rate, most B2B payments continue to be made by check— roughly 74 percent according to a 2007 survey conducted by the Association of Financial Professionals (AFP). This study found that the average business surveyed makes 65 percent of its B2B payments to suppliers by check, with 18 percent by automated clearinghouse (ACH) credit, and 11 percent by wire transfer. With the myriad of payment choices available to suit a variety of user preferences for both consumers and businesses, why has the migration to electronic payments by businesses lagged that of consumers?

The adoption of electronic payments by consumers has exceeded analysts' projections in recent years as a result of a confluence of a number of different variables, namely convenience, security, and efficiency, which have provided the necessary incentives for adoption. The Internet has emerged as an increasingly trusted payments and product distribution channel as well, facilitating the initiation of electronic payments via both card networks and the ACH. While the same benefits of electronic commerce are desirable to the B2B payments segment, the complexity of the B2B payments landscape along with technology constraints for smaller business partners contribute to a less rapid adoption than seen in the consumer-to-business segment. What are the major B2B barriers to adoption, and how are they being addressed?

The problem with cards

Cards are an expensive proposition for payments between trusted and known business partners, particularly for large value payments. While they offer advantages such as financial management and control, they also impose a hefty interchange fee of roughly 2 percent of the transaction. If you know and trust your customer, you are probably more inclined to write a check, which has no transaction fee. This scenario is likely to be particularly true during times of economic downturn such as we are now experiencing.

ACH and wire transfers

Wire transfers are important for payments that are high dollar and require immediate settlement. Their high-cost limits their use, however. Also, wire transfers tend to be used by larger versus smaller business organizations. The ACH is growing more popular for larger organizations for payments between major trading partners but is used more to receive than to make payments. It is also important to note that NACHA rules currently prohibit the conversion of business checks in the ACH. While the ACH format permits the transmission of payments and remittance data, there are a number of other alternative methods to deliver remittance information.

Obstacle: no standard remittance information

One clear obstacle to the migration from paper to electronic payments is the lack of standardization in the way remittance information is sent with the payment. Because of variations in data formats, trading partners may not be able to send or receive automated remittance information with electronic payments, inhibiting the automation of accounts receivable systems. Smaller organizations typically lack full integration between electronic payment and accounting systems, as their incentives to invest in the enabling technology are likely to differ from their large corporate counterparts.

Since electronic payments are typically faster than checks, an accounts receivable function might embrace an electronic payment in order to reduce the time to collect receivables, in direct contrast to an accounts payable function. Sophistication and size generally correlate to willingness to invest in the technology to adopt electronic payments.

Moving from checks to electronic payments can reduce fraud

In the AFP's 2008 Payments Fraud and Control Survey organizations of all sizes reported more attempted or actual payments fraud in 2007 from checks than from other payment methods. However, the report also notes that the majority of survey respondents did not actually suffer financial loss from the fraudulent activitity, suggesting that effective use of risk mitigants to control fraud once it is identified.

Continued on next page

MARCH 10, 2009

Continued from previous page

Payment Methods Subject to More Payments Fraud in 2007 Compared to 2006
(Percent of Organizations Subject to Greater Amount of Attempted or Actual Payments Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Checks	90%	88%	89%
ACH debits	16	20	11
Consumer ACH and/or Card Payments*	10	8	17
Corporate cards	9	11	6
Wire transfers	2	2	*
Prepaid Gift Cards	1	2	*
ACH credits	1	*	3

* receive only

Source: 2008 AFP Payments Fraud and Control Survey

B2B future is likely electronic

While the pace of migration to B2B electronic payments may not accelerate in today's distressed financial environment, eventually the obstacles to the electronification of B2B will be resolved. For now, the bottom line is that businesses want to send payments in the most cost-effective way possible, and no one payment type may suit every payment need. Just as consumers will continue to avail themselves to the full spectrum of payment alternatives, depending upon what is cheapest, trusted, and most convenient, so too will businesses choose payment options that makes the most business sense.

Electronic payments are growing in the B2B space, but not by leaps and bounds, even in recent times when the economic outlook was favorable and financial institutions were readily investing in payments technology. While the future of B2B payments will likely be electronic versus paper-based, there is no clear evidence to show whether businesses will choose one electronic option to the exclusivity of another. For now, checks continue to represent a good value proposition to businesses, particularly when they can be imaged during the collection process to avoid transportation costs.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

MARCH 19, 2009

Can information sharing reduce fraud?

I was doing some research recently to see what I could find on the legal impediments to information sharing among law enforcement agencies and bank regulators when I ran across a report published by the U.S. Government Accountability Office (GAO) in March 2001 titled "Financial Services Regulators: Better Information Sharing Could Reduce Fraud." The paper identified some benefits as well as barriers to sharing information and proposed a recommendation for moving forward. While little has changed since the GAO first issued that report, there still remains much to be gained in addressing these issues.

One of the things we hear from the financial services industry, law enforcement, and bank regulators is that we need to collaborate by sharing information to better detect and mitigate fraud in retail payments. Most of the law enforcement representatives we talk to say that payments fraud is on the rise as global and domestic fraud rings alike are gaining access to consumer data for identity theft and financial transactions. According to these representatives, the bottom line is that fraudsters are talking to one another and sharing information over a number of channels including the Internet, chat rooms, and even within the prison system. With this information in mind, perhaps now is the time to rethink the way we share information to prevent and mitigate fraud and risk in retail payments.

Databases for sharing information are decentralized among separate bank regulators

Decentralization of information by bank regulators is one of the barriers noted in the GAO report. Because the systems and databases that maintain records on individuals and businesses, consumer complaints, and disciplinary actions are decentralized among the separate regulators within the banking industry, an investigation of a rogue actor realistically could involve separate inquiries of the different bank regulators.

Most information sharing is limited to public information

The GAO report also concluded that while financial regulators agreed about the benefits of sharing regulatory and criminal data, there were concerns about how to do that without creating confidentiality, liability, and privacy issues as well as the potential for inappropriate use of information. Regulators expressed concern about the potential for premature disclosure of information obtained through regulatory activities or criminal investigations.

Once they are final, formal enforcement actions taken against banks, as well as cease and desist orders and civil money penalties, are all public documents that identify

individuals and entities responsible for criminal, civil, and otherwise unsafe and unsound banking practices. However, the lag time between the identification of the risky or fraudulent practice and issuance of the formal action can be considerable and does not make information available for other victims or potential targets.

Information sharing is still in separate silos at the institution level

One caveat to the potential benefits derived from an industry-wide information sharing mechanism is the fact that data are often isolated among disparate silos within a financial services company. Enterprise-wide risk management is often designed to aggregate information from separate lines of business, each often equipped with its own fraud prevention process and data collection. The successful business model going forward might enable the sharing of information across a bank's payment products and channels to prevent a fraudster from hitting the same institution multiple times.

Private industry efforts are emerging to collaborate

There are a number of private industry initiatives in play, such as third party–sponsored consortiums for financial institutions to share information among one another. These services are provided at a cost that some financial institution participants are unwilling or unable to bear. The cost for information serves as a barrier in this sense, potentially driving the fraudsters to the weaker links in the system that cannot afford to participate in the cost of building a data-sharing mechanism.

Conclusion

Financial modernization efforts have resulted in more electronic transactions of payments and information. While non-technological means of fraudulently obtaining confidential consumer information remain prevalent (dumpster diving, etc), the use of the Internet and chat rooms makes it increasingly easy for rogue actors to communicate and share information to perpetrate fraud. Social networks are growing in popularity as consumers are increasingly comfortable in sharing information over the Internet. This technologically inspired trend was not entirely envisioned when the laws and rules designed to protect rights to privacy were crafted. Changing the legal boundaries established among regulatory and law enforcement agencies may be necessary to enable truly effective detection and mitigation of fraud, but this practice can't happen overnight.

What steps can we take to break down the barriers to information sharing? How do we balance one party's "need to know" with another's need to safeguard sensitive information? How do we determine what data are most universally useful in our mutual efforts to predict and recognize fraudulent activity and identify the bad actors? We would like to hear from you, so please let us know your thoughts.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

MARCH 27, 2009

2008: A year of thought on retail payments risk and fraud

Looking back, 2008 saw an array of Federal Reserve Bank–sponsored conferences and events focused on retail payments risk and fraud issues, as well as a number of highly relevant papers. It's worth compiling and highlighting a few of those Federal Reserve efforts (at the risk of leaving some out!). I think all these developments reflect a renewed interest in public-private partnerships both in the Fed and in the industry, interest that will promote collaborative efforts to address common issues.

First, here are links to three conference summaries and related papers resulting from Reserve Bank–hosted events in 2008:

- April 2008 – Philadelphia Fed Payment Cards Center: "Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud"
- June 2008 – Chicago Fed Payments Studies: "Payments Fraud: Perception Versus Reality"
- October 2008 – Atlanta Fed Retail Payments Risk Forum: "Retail Payments Risk and Fraud: Detection and Mitigation"

In addition to the results of these conferences, there were a number of papers published last year from Fed staff that I would also highlight to our readers on relevant issues:

- Braun, et al., "Understanding Risk Management in Emerging Retail Payments"
- Gerdes, "Recent Payment Trends in the United States"
- Jacob and Summers, "Assessing the landscape of payments fraud"
- Weiner, "The Federal Reserve's Role in Retail Payments: Adapting to a New Environment"

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

APRIL 14, 2009

Why aren't we seeing fraud in remote deposit capture?

The growth in electronic payments and a distressed economy together have created an environment ripe for new payment fraud opportunities, according to the Association for Financial Professionals' 2009 Payments Fraud and Control Survey. But while the report notes that more than 70 percent of firms surveyed were the victims of attempted or actual fraud during 2008, no increase was reported in attempted fraud associated with the adoption of remote deposit capture (RDC) services. While nearly half of the respondents indicated that their organizations had offered services to customers to transmit check images using remote deposit, only 1 percent reported that they experienced payment fraud as a result.

Fraud as a Result of Remote Deposit Capture Service

(Percentage Distribution of Organizations That Use Remote Deposit)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Experienced fraud	1%	2%	1%
Did not experience fraud	99%	98%	99%

Source: AFPonline.org

Does nascence explain lack of reported fraud?

While RDC adoption has been rapid, it remains at an early stage in the technology adoption lifecycle. Anecdotal evidence suggests that some financial institutions and their customers have initiated service offerings judiciously to known business customers and thereby mitigated the inherent risk exposure from RDC. However, less sophisticated adopters may lack the operational systems and control processes to identify fraud when it happens or are otherwise not forthcoming to admitting when they are victimized. Time will tell if fraud trends emerge or become more transparent as RDC grows into a more mature service offering by financial institutions.

Risk management and regulatory oversight

We spoke with examiners in the Atlanta Fed and learned that they've had RDC on their radar for some time and have promoted sound risk management practices during bank examinations in advance of formalized interagency guidance. In January, the Federal Financial Institutions Examination Council (FFIEC) published its official guidance for banks' risk management of RDC services. This guidance provides a comprehensive summary of the risks inherent in this service and the necessary elements of an effective risk management program. As prescribed in the FFIEC guidance, the same disciplines that apply to the risk management of other bank products and services apply to RDC. First and foremost, it is critical to have proper due diligence in the selection and monitoring of third-party service providers to whom certain operational functions are outsourced, along with accurate and ongoing self-risk assessments of the financial institution's internal and external business environments.

Conclusion

No one can be sure why firms that offer RDC aren't experiencing fraud as they are from other payment services, particularly those that are check-related. It could be the way that information is captured and reported within an organization. One thing we know for sure is that RDC adoption is expected to continue to grow as businesses and consumers convert paper checks to more cost-effective electronic payments. Will fraudsters find vulnerabilities to exploit in the risk management efforts on behalf of product vendors, bank regulators, third-party servicers, and the financial institutions themselves? We would like to hear from you. Feel free to share your thoughts with us.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

MAY 12, 2009

Patenting the payments system: Navigating confusing and congested waters

Anybody looking to innovate in the payments space may need to tiptoe carefully to avoid stumbling upon patent infringement. What's more, the complex patent landscape may raise interesting questions about the ability of the payments industry to collaborate.

Some years ago I ran a thought experiment to consider whether U.S. "payments patents" could be assessed easily using the U.S. Patent and Trademark Office (USPTO) classification system. Unfortunately, the classification system does not label patents as "payments-related" per se, so there is no scientific manner to search for related patents without studying claims on thousands of patents individually. However, one can derive an impression of the landscape by using a simplified approach of counting patents across a limited set of USPTO patent classifications that most strongly exemplify "payments-related patents" (drawing particularly on subclassifications 705/39-45 and 705/64-79). In these subclassifications, 3,659 patents were issued from 1998–2008, with 653 (17.8 percent) issued in 2008 alone. If one considers these back-of-the-envelope calculations and even controls for the "noise" between the USPTO classification system and what is considered "payments-related," there is nevertheless a revealing picture of the complexity and potential for patent infringement for any firm trying to innovate in the payments space.

What's more, an understanding of the payments patents landscape is also useful when considering the possible impact of patents on a highly segmented market like payments, which is characterized by network effects, first-mover advantages, large sunk costs, and lock-in effects. Some existing research examines the impact of patents on financial services innovation generally.

In the payments market, on balance, will patent holders hinder market entry, or will they enable new market entry for new innovations? How do patent rights affect payments industry efforts to set standards, develop and implement innovative risk management tools, or create new products that improve the integrity of the payments system overall? Does a concern about patent rights further hinder industry efforts to share information necessary to address risk issues collectively?

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

MAY 19, 2009

State attorneys general shine light on gray areas of payments risk

When considering due diligence standards in payments relationships, banks and others may want to look beyond bank regulators, legal requirements, and NACHA rules to also include considerations developed out of the work of state attorneys general. During the last several years, state attorneys general have found their way into the payments risk management space as they have sought to inhibit merchants from evading taxes, promoting internet tobacco sales to minors, and other illegal behaviors. In their pursuit of wrongdoers, states have investigated the payments processors who aggregate and/or initiate ACH payments or remotely created checks, and the banks who accept these items through their account relationships as well. In doing so, these states have negotiated settlement agreements, which include due diligence policies for banks and payment processors. The results of these efforts may raise interesting questions as to whether or not existing regulatory guidance, NACHA rules, or legal requirements are sufficiently specific or clear standing alone.

One instance is instructive. Beginning in 2006, the states of California, Idaho, and New York began to investigate Internet tobacco sales activities in violation of various state laws. These investigations led to negotiated settlements with ECHO Inc., a payments processor, and with First Regional Bank, a California-based financial institution. These settlements included detailed requirements for the processor and the bank to perform due diligence on their customers (or, for the bank, their customers' customers). In particular, First Regional Bank was required to institute a "Tobacco Policy" under which the bank would perform specific steps to ensure it did not permit illegal tobacco sales activity to be facilitated using payments originated via its accounts. As an example, the bank's policy would include terminating accounts with any processor who failed to terminate processing for any customer who a) switched ACH activity to "demand drafts" (presumably focused on remotely created checks) once notified of a problem or b) offered "demand drafts" as a means to avoid ACH return scrutiny. This provision highlights a particular concern with illegal activity, including frauds, switching between ACH payments, and remotely created checks to avoid the network scrutiny instituted by the ACH operators and NACHA.

The efforts of the states, such as in the example above, raise potential questions about the specificity and clarity of the guidelines issued by the banking regulators, such as those issued by the OCC and FDIC with regard to payments processor relationships. The bank supervisors promote banks taking a risk-based view of due diligence requirements rather than prescribing specific actions. NACHA rules require commercially reasonable standards generally, suggest contracts should be in place with third-party senders, and make clear the ODFI bears the responsibility for the items it introduces into he ACH network but do not otherwise prescribe due diligence standards for processor relationships.

Subject to the principles-based standards described in supervisory guidance, NACHA rules, and other considerations, banks and even payments processors themselves might want to consider the standards included in state attorney general settlements in developing their own due diligence policies.

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

MAY 26, 2009

SARs trends, SAR Review teams, and fraud

A February 2009 report from the U.S. Government Accountability Office (GAO) found that between 2000 and 2007, suspicious activity report (SAR) filings by depository institutions nearly quadrupled, from 163,000 to 649,000 per year, with 2008 promising even further growth. The GAO report posited two key forces driving the overall increase in filings: a) the deployment of automated monitoring systems that can assess suspicious activities using customer profile information and b) heightened diligence in light of several high-profile cases involving poor account monitoring by some institutions, which may have led to institutions filing more SARs "defensively" to avoid criticism.

SARs were initially associated with money laundering and terrorist financing concerns, but now, some experts note, SARs are increasingly filed for other potential suspicious activities such as identity theft and consumer fraud. Possibly this trend is a further reflection of the sophistication of integrated and automated systems deployed by some financial institutions which can detect suspicious activity of all types, or possibly this development is a manifestation of the "defensive filing" phenomenon. FinCEN Director James Freis was recently quoted in the American Banker: "I think that more bankers are realizing that the same due diligence required for AML (Anti-Money Laundering) compliance is also a powerful weapon against fraud."

Another contributing factor not mentioned by the GAO report is growth in the overall volume of banking transactions such as mortgage activity. However this factor is not likely to fully explain the very rapid growth in SAR filings in these years. Moreover, there is the question of whether the increase in SAR filings is reflective of an increase in criminal activity itself.

The 2001 National Money Laundering Strategy called for the establishment of "SAR review teams" in every federal judicial district, drawing together federal law enforcement (U.S. attorneys offices, Internal Revenue Service, U.S. Immigration and Customs Enforcement, Federal Bureau of Investigation, Secret Service, U.S. Postal Inspection Service, etc.), federal banking regulators, and state and local law enforcement. While SARs have typically been used as supporting documents for existing cases, these SAR review teams look to SARs also for the purpose of initiating new investigations. SAR reviews by these teams may uncover links among superficially distinct SARs that can lead to criminal prosecutions, civil forfeiture actions, federal or state regulatory actions, warning letters, and/or referrals to other agencies or districts. Further, these teams help to coordinate efforts and more efficiently allocate scarce resources.

Will the confluence of increased reporting, improved data monitoring by many institutions, and proactive monitoring of SARs by SAR review teams have a measurable impact on abuse of payments systems and associated fraud?

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

MAY 29, 2009

Do market forces drive fraud?

In today's U.S. markets for payment and credit services, have we overshot the mark in keeping personally identifiable information private, thereby lowering the bar to fraudsters?

Providers of credit and payment services traditionally required customers to have a public identity, such as by providing references, allowing the provider to verify the person's identity and creditworthiness before opening an account. This required the potential customer to be socially engaged and sacrifice some privacy to establish a public identity. Some non-Western cultures still look to public personas to help ensure good conduct. Consider Qifang, a new Chinese peer-to-peer lending business, which requires potential borrowers to provide not only personal information but also information about family members, thereby raising the penalty for default as it may cause the whole family to "lose face."

U.S. consumers have come to expect instant gratification in their ability to open accounts, obtain credit, and complete payments. Further, they tend to demand privacy and security of their personally identifiable information and want to share the least information that will facilitate the transaction. These market demands may drive payment services providers to impose the least amount of privacy requirements and security risk on their customers to facilitate the most "frictionless" transactions possible. While perhaps inevitable and likely a positive driver of payments innovation, this confluence of market forces may nevertheless increase the vulnerability of payment systems to risks such as those resulting from identity theft and new account fraud—less information is demanded of a legitimate customer, so similarly the hurdles to wrongdoers are lower.

Some thinkers in this arena have applied economic analysis to the trade-offs between privacy, data security, and fraud prevention. Others have advocated re-evaluating entirely how we view privacy, by severing the link between identification information (which should be harmless and public) and privacy, in effect permitting individuals to preempt imposters by making their identity fully public and allowing anyone to verify it easily.

While there is great emphasis on protection of personally identifiable information (driven by law and regulation, consumer demand, fear of reputational impact from data breaches, etc.), as long as such information can be used effectively to perpetrate fraud, risks will persist. As payment providers simultaneously compete for the most user-friendly, hassle-free, fast, private, secure services model, they also may have incentives to require less personally identifiable information. This is less intrusive for their customers and also helps avoid storage of such information. This may drive providers to require the lowest level of information and, as mentioned before, lower the bar for fraudsters as well.

Do these market incentives in effect foster an environment where identity theft and resultant payment frauds can proliferate? If so, how can this problem best be addressed?

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

JUNE 07, 2009

How much risk lurks in the shadows of daylight overdraft?

With the U.S. banking system in financial distress, the Fed provides payments services to a greater number of problem banks. So how much of an issue is the credit risk associated with retail payments today? As you know, financial institutions, much like the commercial and retail customers they serve, from time to time experience the need for overdraft credit—short-time loans to accommodate the management of incoming and outgoing funds. The Fed provides daylight overdraft protection to financial institutions that experience timing differences in ACH service offerings so that they can meet their cash flow obligations, in the same way a financial institution provides overdraft protection. The Fed, like any prudent lender, also maintains a responsibility to carefully manage the credit risk exposure from these provisions of credit. The need for the Fed to monitor ACH activity for overdraft exposure becomes critical when a financial institution's health is in question.

How does the Fed monitor the financial health of financial institutions?

It is important to remember that the Fed is also a bank regulator, and it works collaboratively with other bank regulators to monitor bank conditions. When a bank's financial condition deteriorates, the agencies communicate the institution's regulatory rating and other relevant information to the Fed in its U.S. payments oversight role. Wearing that hat, the Fed may choose to restrict lending in a number of ways, such as limiting access to daylight credit.

Real-time monitor

One tool that can be used to restrict daylight credit access is "real-time monitoring" (RTM), which is implemented through the Account Balance Monitoring System (ABMS). With RTM, the Fed can reject certain transactions from posting to an institution's account if that posting would cause the institution to exceed its daylight credit limits. Under RTM, any funds transfers from the account or ACH credit originations (which are required to be prefunded) that would cause an institution to exceed its daylight credit capacity would be rejected.

Interest on reserves and daylight overdrafts

One conundrum in this equation is that the need for overdrafts has diminished recently as banks began maintaining higher reserves, prompted by the Fed's decision to start paying interest on reserve balances. Before, banks were reluctant to hold too many reserves because they were a nonearning asset. Since the Fed didn't compensate banks for holding the reserves, banks could find more rewarding uses for their funds. With more reserves in the system, the need for intraday borrowing from the Fed has decreased. Whether that trend will continue as the economy improves and the financial condition of the banking sector stabilizes, thereby creating more lucrative uses for excess reserves, remains to be seen—but then maybe we won't have as many high-risk banks as the economy improves. Let's hope not.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

JUNE 15, 2009

Zero balance? Credit card companies may zero in on "deadbeats"

Payment industry experts suggest that credit card companies will make up for lost income from congressionally-mandated curtailment of fees and penalties by going after credit card "deadbeats," which may not mean what you think. To credit card companies, "deadbeats" are customers who pay off their balances regularly and provide little or no revenue to the card issuers. Because banks are expected to lose substantial revenues as a result of the new legislation, they are looking to replace those revenues, more than likely through a revival of annual fees and the elimination of reward programs that the credit card deadbeats currently enjoy.

Congress passed credit card reform legislation in early June to limit some of the unscrupulous pricing schemes that have evolved in recent years—sudden, unexpected hikes in interest rates and double-cycle billing, for example. The law goes beyond codifying the Federal Reserve's regulatory rules already scheduled to go into effect in July 2010 by adding tougher restrictions and extending consumer protections.

Reform may have been necessary, but will the current legislation result in unintended consequences for consumer retail payment behavior?

Pricing for risk

In the early days of the credit card product, banks charged a flat interest rate and an annual fee, which made sense since they only gave cards to their most creditworthy customers. The development of credit scoring models in the late 1980s enabled banks to expand their market by allowing them to measure their potential credit risk for an individual cardholder and price for that risk accordingly.

As the competition for credit card business heightened in the 1990s, competitive pricing schemes evolved with teaser periods permitting low- or no-interest payments on new accounts and transferred balances. This practice permitted consumers to transfer balances frequently for introductory period financing. At some point, the transfer game would inevitably get out of hand and the consumers would become overextended financially. As those overextended cardholders began to experience debt service problems, the credit card issuers responded by repricing their card products to compensate themselves for the additional risk. In fact, some issuers targeted the subprime customer segment exclusively.

Since the reform effectively reduces revenue potential at a time when charge-offs are rising, card issuers will likely rethink their pricing models. If they shift these lost revenues as additional costs or reduced benefits for creditworthy customers, will these customers opt for other payment mechanisms?

Credit or debit?

Will increased costs for credit card products drive credit card deadbeats to use their debit cards instead? While they are different products governed by different sets of laws, many issuers now provide the same consumer protections for debit cards that they do for credit cards. Yet credit cards still have their advantages in terms of the "pay now" or "pay later" decision option. And if you have a dispute over a credit transaction, you still don't have to make the payment until the problem is resolved. With a debit card dispute, the money has already left your account, and your arguments are focused on how to get it back. So a few distinctions favoring credit cards remain. Whether or not deadbeats will pay for them remains to be seen.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

JUNE 22, 2009

Payments fraud no longer just a white collar crime

White collar crime: *a crime committed by a person of respectability and high social status in the course of his occupation. — Edwin Sutherland, 1949*

I recently ran across a news article that was a shocking reminder of the widening criminal network involved in payments fraud. On May 13, the district attorney in San Diego announced the arrest of 60 people on felony charges in connection with an elaborate bank fraud scheme. It was the culmination of a 10-month-long investigation of a $500,000 check cashing scam at Navy Federal Credit Union. Not an unusual story until I read who masterminded the scheme—a San Diego street gang.

According to the press release, this was the first time a violent street gang was targeted for its involvement in complex bank fraud in California. The gang members worked in cooperation with existing account holders to deposit counterfeit checks into their accounts and then withdraw the cash before the credit union could determine the check was fraudulent. In return, the account holder would receive a commission of up to several hundred dollars on checks ranging from several thousand to tens of thousands. The District Attorney concluded that the size, scope, and sophistication of the operation indicated that the criminal street gangs in San Diego are expanding their criminal enterprise into white collar crime.

A similar case of check fraud and gang activity occurred in Phoenix last year. "Operation Blank Check" was a year-long investigation that uncovered a check fraud scheme totaling nearly $3 million. Postal inspectors initially contacted the Phoenix Police Gang Enforcement Unit about gang members being involved in mail theft and fraudulent schemes. Further investigation revealed that the suspects had been involved in violent gang activity and transitioned to white collar crime. A broad partnership of local, state and federal law enforcement agencies worked on the case and was able to arrest more than 100 individuals, 77 of whom were "hard core gang members" representing 22 local gangs.

There have also been several cases of identity theft involving street gangs in recent years. An April 2007 report by the President's Identity Theft Task Force noted that law enforcement agencies across the country have observed a steady increase in the involvement of groups and organizations of repeat offenders or career criminals in identity theft. Some of these groups are formally organized and well-known to law enforcement because of their longstanding involvement in other major crimes, such as drug trafficking. Others may be more loosely organized but are able to connect and coordinate their activities through the internet.

The comparative ease of committing financial crimes has made it more appealing to street gangs as a way to support other criminal activities. The investigators in the Navy federal case speculated that the gang members used the half-million dollars to help fund illegal gang activities and pay for a lavish lifestyle.

Multiagency collaboration key to combating fraud

The key to apprehending the defendants in this case was a coordinated operation involving the U.S. Secret Service, San Diego Regional Fraud Task Force, San Diego Police Department Gang Detectives, San Diego District Attorney Investigators, U.S. Postal Inspection Service, Naval Criminal Investigative Service, Navy Federal Credit Union, and the California attorney general's office.

Each agency played a significant role in the investigation that was initiated when the Naval Credit Union investigators noticed suspicious activity in 2005 and reported it to the Secret Service. For example, the San Diego Police gang detectives helped to identify and interview the suspects. The U.S. Postal Inspection Service helped locate suspects and investigate the counterfeit checks. The San Diego Regional Fraud Task Force, district attorney's office, and attorney general's office became involved due to their experience handling complex fraud investigations.

This case is just one example of the importance of cooperation between local, state, and federal law enforcement in effectively combating payments fraud. By forming interagency task forces that allow for expertise and intelligence sharing, law enforcement can be in a better position to prosecute and, hopefully, deter fraudsters.

By Jennifer Grier, senior payments risk analyst in the Retail Payments Risk Forum at the Atlanta Fed

JUNE 29, 2009

Fraud Enforcement and Recovery Act of 2009

On May 20, President Obama signed into law the Fraud Enforcement and Recovery Act of 2009. Among other things, the law "authorizes" substantial funding in 2010 and 2011 for various federal agencies, including the Department of Justice, the Postal Inspection Service, the Securities and Exchange Commission, and the Inspector General of Housing and Urban Development, to investigate and prosecute financial frauds of all types. (Note that an authorization does not necessarily mean any appropriation of additional funding to these agencies above their existing funding will result.)

One of the law's chief sponsors, Sen. Patrick Leahy, included the following in his comments on the law:

> "At its core, the Fraud Enforcement and Recovery Act authorizes the resources necessary for the Justice Department, the FBI, and other investigative agencies to respond to this crisis. In total, the bill authorizes $245 million a year over the next two years to hire more than 300 Federal agents, more than 200 prosecutors, and another 200 forensic analysts and support staff to rebuild our nation's 'white collar' fraud enforcement efforts. While the number of fraud cases is now skyrocketing, we need to remember that resources were shifted away from fraud investigations after 9/11. Today, the ranks of fraud investigators and prosecutors are drastically under stocked, and thousands of fraud allegations are going unexamined each month. We need to restore our capacity to fight fraud in these hard economic times, and this bill will do that."

Supporters of the law have promoted the idea that this funding of efforts to fight financial crimes will in effect result in a good return on the government's investment as it will result in higher recovery of funds lost to fraud. Some cite Justice Department estimates that each dollar spent to prosecute fraud results in more than $20 being ordered in restitution and fines for victims and the government.

This law (if funded) could result in a sea change in the focus of federal law enforcement to address a wide array of financial crimes in the future. It bears watching to see if this effort has a measurable impact in tamping down the growth and spread of financial-related fraud and whether it will in particular have any impact on payments fraud issues, such as the persistence of check fraud schemes or the development of new fraud schemes leveraging gaps in emerging payments modes.

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

JULY 06, 2009

Remotely created checks: Distinguishing the good from the bad

There are no hard numbers to quantify that remotely created checks (RCCs) pose greater risks than other payment types. However, there are known instances of RCC fraud, the impact of which can be significant. So the depository banks liable for RCCs may want to keep a vigilant eye on the situation.

What are RCCs?

These are checks that are not created by the paying bank and do not include the account holder's signature. In lieu of an actual signature, the check's signature block typically contains the account holder's printed name or standard language indicating authorization. RCCs have been used for recurring transactions, such as insurance premium payments, for quite some time. This solution offers consumers an alternative to the hassle of manually writing out checks each month. More recently, RCCs have also been used in nonrecurring transactions, such as purchases or bill payments made over the telephone or Internet. Though a useful form of payment, RCCs introduce risk into the retail payments system.

What are the risks?

As stated above, RCCs do not require a signature for authorization. As a result, they are vulnerable to misuse by fraudsters who can, for example, use an RCC to debit a victim's account without receiving proper authorization or delivering the goods or services. The risk of fraudulent RCCs is amplified in one-time purchase scenarios where the merchant is relatively unknown to the customer.

To address the fraud risk of RCCs, in July 2006 the Federal Reserve modified the liability structure for this particular type of check. The liability for unauthorized RCCs shifted from the paying bank to the depositary bank, which must now warrant to the collecting and paying banks that the RCC presented has been properly authorized. The Federal Reserve's amendment provides economic incentive for the depositary bank to perform additional vigilance when accepting RCCs given the warranties they must make. Since the depositary bank maintains the relationship with the bank customer depositing the RCCs, it is in the best position to mitigate the fraud risk. The challenge is that banks cannot readily identify RCCs in an automated fashion through the existing MICR line format. Generally, review of incoming RCCs requires manual intervention.

How pervasive are they?

In light of this identification challenge, the Fed applied a modified definition of RCCs to a sample of check transactions in order to establish a reasonable estimation of the volume of RCCs. As a result, the Federal Reserve's 2007 Check Sample Study concluded that less than 1 percent (0.95) of the checks sampled were RCCs. It is unclear how accurate this result is when considering the regulatory definition, but it is probably fair to say that RCCs are only a very small portion of check volumes overall. Moreover, the analysis did not discern within that estimate the number of illegitimate RCCs. It is the cases of misuse that have prompted some to call for a ban of RCCs altogether. While there is anecdotal information and well-publicized cases (such as the 2008 Wachovia case) highlighting abuses committed using RCCs, there is a lack of concrete data reflecting the portion of RCCs that are fraudulent or returned for other reasons.

Conclusion

RCCs represent a relatively small subset of checks overall. However, applying the Check Sample Study methodology and results of the Federal Reserve's overall 2007 Payments Study, the number of RCCs in 2006 alone would still have represented approximately 286 million items.

We know that some portion of these RCCs represent fraudulent cases where the payment was never authorized. However, we also know that when it does occur the consequences may be substantial in terms of adverse consumer impact. Therefore, despite the lack of complete data, it is unwise to allow RCCs and the known misuses to fall completely off the radar.

By Crystal D. Carroll, senior payments risk analyst of the Retail Payments Risk Forum at the Atlanta Fed

JULY 13, 2009

Consumer complaints may be "canary in a coal mine" for payments risk

For many years in the coal mining industry, a caged canary would be brought into the mines to detect whether toxic gases were present. The canary served as an early warning system of potential danger for the miners. Similarly, consumer complaints data could serve as a harbinger of potential risks in payments for law enforcement and other industry professionals.

Several regulatory agencies receive fraud-related complaints from consumers, including those involving financial institutions. Some of the consumer complaint databases are shared among agencies to help better facilitate fraud investigations and to track trends and developments in consumer fraud activity.

One example is the Federal Trade Commission's (FTC) Consumer Sentinel Network (Sentinel), a secure online database of consumer complaints that is only available to law enforcement. In addition to storing FTC complaints, the Sentinel also includes complaints filed with more than 100 different U.S. and Canadian federal, state, and nongovernmental organizations. Among the leading partners and data contributors are the Internet Crime Complaint Center, Better Business Bureaus, Canada's Phone Busters, the U.S. Postal Inspection Service, the Identity Theft Assistance Center, and the National Fraud Information Center.

Established in 1997 to collect fraud and identity theft complaints, the Sentinel database was expanded in 2008 to include complaints about credit reports, debt collection, mortgages, and lending, among other subjects. According to the 2008 Consumer Sentinel Network Data Book, the database has more than 7.2 million complaints.

FTC complaints provide insight into consumer fraud trends

The Sentinel received a total of 1.2 million complaints during calendar year 2008. Of the 30 complaint categories, identity theft ranked first with 26 percent of the overall complaints. Credit card fraud (20 percent) was the most common form of reported identity theft, the majority of which involved new accounts (12.3 percent). Another significant category of identity theft reported by consumers was bank fraud (11 percent). Although identity theft bank fraud, which includes fraud involving checking and savings accounts and electronic fund transfers, has declined since 2006, the most common type continues to be electronic fund transfers.

Continued on next page

Continued from previous page

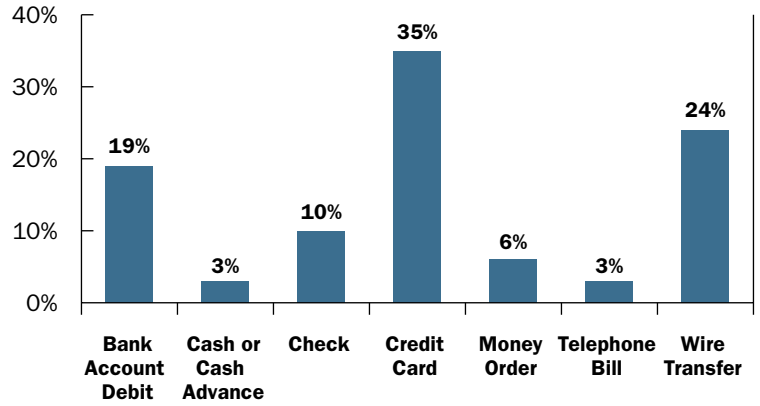
Top 10 Consumer Sentinel Network Complaint Categories January 1 – December 31, 2008

Rank	Category	# Complaints	Percentages
1	Identity Theft	313,982	26%
2	Third Party and Creditor Debt Collection	104,642	9%
3	Shop-at-Home and Catalog Sales	52,615	4%
4	Internet Services	52,102	4%
5	Foreign Money Offers and Counterfeit Check Scams	38,505	3%
6	Credit Bureaus, Information Furnishers, and Report Users	34,940	3%
7	Prizes, Sweepstakes, and Lotteries	33,340	3%
8	Television and Electronic Media	25,930	2%
9	Banks and Lenders	22,890	2%
10	Telecom Equipment and Mobile Services	22,387	2%

Source: Federal Trade Commission

The data also give some indication of the preferred payment channel for consumer fraud. In 2008, for those fraud complaints where the consumer reported the method of payment, credit cards was the most common (35 percent) followed by wire transfer (24 percent), bank account debit (19 percent), and check (10 percent). The rankings have been consistent over the past two years, but credit cards have increased from 30 percent and 33 percent for 2006 and 2007, respectively.

Consumer Sentinel Network Fraud Complaints by Methods of Consumer Payment, January 1 – December 31, 2008



Source: Federal Trade Commission

Consumer complaint databases can be an important resource in detecting fraud issues

FTC Sentinel data only gives a snapshot of the consumer fraud and risk issues occurring in the payments system. A consumer who has a problem involving an account held at a financial institution may file a complaint with the appropriate bank regulator. The Retail Payments Risk Forum is currently analyzing consumer complaints filed with the Federal Reserve Consumer Help over a four-year period to track whether there are trends that may indicate underlying payments risks. At the very least, the consumer complaints data may provide leading indicators of areas where we may need to focus our attention with research and/or education.

By Jennifer Grier, senior payments risk analyst in the Retail Payments Risk Forum at the Atlanta Fed

JULY 24, 2009

Transparency: Seeing through International ACH

There are anecdotal reports that some financial institutions are treating their preparatory efforts for the new international ACH transaction (IAT) rule and format like a Y2K event. However, they shouldn't lose sight of the fact that the industry stands to reap substantial benefits from the new rule, largely because of improved transparency in the ACH network. As you may be aware, the new IAT rule and format go into effect on Sept. 18, 2009. NACHA, the rulemaking body for the ACH network, has conducted extensive industry outreach to provide education on the new rule and format.

In many respects, the change in the international ACH transaction format is attributable to the Office of Foreign Assets Control (OFAC). OFAC administers and enforces economic and trade sanctions in accordance with U.S. foreign policy and national security goals against targeted foreign entities such as international drug traffickers, terrorists, and other threats. Beginning in the late 1990s, OFAC began to have concerns about abuses from terrorists in cross-border ACH transactions. OFAC had reason to believe that we needed better safeguards for our financial system, especially after 9/11. The ACH network today is increasingly vulnerable to potential abuse with respect to the international cross-border movement of funds because of the expanded use of the ACH for one-off transactions from the practice of recurring transactions between known and trusted parties, as well as the speed and efficiency of the ACH network in general.

To address their concerns, OFAC worked with NACHA to construct a payment format that would permit sufficient information to identify parties to the cross-border transaction. In 2004 NACHA began working with OFAC on a proposed rule change for international ACH transactions and a new format that would include the data elements from the Bank Secrecy Act's (BSA) "travel rule." Essentially, the BSA travel rule includes more robust information about the payment originator and beneficiary so that a financial institution can review the transaction for OFAC compliance. When the IAT rule goes into effect, all transactions that meet the new definition of international ACH transactions made via the ACH Network will be required to use the IAT SEC code.

The IAT code will make it easier for financial institutions to identify international payments in the ACH network since currently many transactions are mistakenly coded as domestic. This mistake occurs because today many international payments are introduced into the U.S. ACH network through domestic correspondent relationships and are then inadvertently transmitted as domestic transactions. So the new code will make it easier for financial institutions to identify these payments and comply with their OFAC obligations, which incidentally, have not changed. IAT really creates more transparency in two significant ways: by identifying the transaction as international and by revealing all parties to the cross-border transaction. In the end, transparency in retail payment systems is a good thing and should help the banking industry combat fraud and other abuses in the ACH network.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

AUGUST 03, 2009

Accounting for ACH losses: What are the right numbers to crunch?

From talking with a number of industry players, it has become increasingly clear that there is both a healthy desire for ACH origination loss data to help understand risks and also business practices that limit the extent to which data to benchmark ACH losses are available in the first place. The challenge is to reconcile these two conflicting objectives.

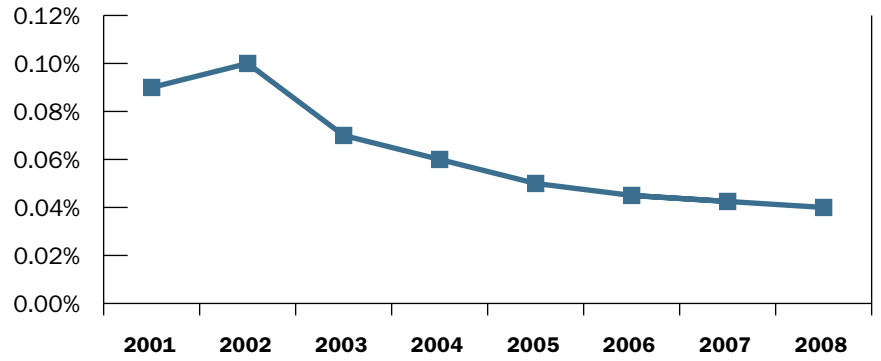
Many banks today treat ACH origination as credit underwriting, particularly for business customers. Given this, one way banks may account for losses as a result of ACH origination is as credit losses against loan loss reserves or other similar accounts. This method is entirely appropriate as a risk management practice given the potential for losses the ACH originating bank may incur as a result of unauthorized debit items that are returned by the receiver through its bank. The originating bank, having already credited its customer's account, may find itself unable to collect the returned item and thus may incur a loss.

NACHA does publish aggregate trend data on what is probably the best metric it has available—unauthorized returns as a percentage of all ACH debits in the network. While this is a good starting point, it is not a fully accurate picture of the actual losses banks may incur as a result of ACH origination (whether for debits or credits). While the trend of unauthorized debit returns is instructive, it does not explain the dollar losses to banks.

Further, while it is likely that most banks track or have the ability to track their losses from ACH origination, there is no standard regulatory or other financial reporting for banks to report ACH loss information. Such losses may be attributable to fraud or not, but the extent of these losses in terms of aggregate dollars and velocity is likely to be a more robust data point for analysis of ACH fraud and ACH origination risks than the data available today. Improved data on banks' ACH loss experience would go a long way to explain the true extent of ACH origination risk within the network overall and may promote banks' ability to benchmark their own losses in an effective way. It also would enable both the network and individual banks to better tailor their risk management efforts. Most importantly, having more data could help dispel any mistaken assumptions about how much financial loss banks are experiencing from operational and fraud risks in ACH origination activities.

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

Unauthorized Debit Return Rate, 2001 – 2008



Source: NACHA, 2009

AUGUST 10, 2009

Collaboration to address payments risks and fraud

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

Continued on next page

Continued from previous page

- 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

Oliver: Funding of risk initiatives faces risky times

This week, we have a special guest blogger: Richard Oliver, an executive vice president with the Federal Reserve Bank of Atlanta. Oliver was a pioneer in electronic payments, working on a Fed system project with the U.S. Treasury to develop direct deposit. He was also instrumental in the Atlanta Fed becoming the second automated clearinghouse (ACH) operation in the United States. Since 1998 he has served as retail payments product manager for the Federal Reserve System. In this capacity, he has responsibility for managing the Fed's check and ACH businesses nationwide.

As we look forward to a slow but steady emergence of the banking industry from the current financial firestorm, the question arises as to how investments in the payment system will fare. More specifically, will banks and other payment system players secure funding for initiatives critical to mitigating payment fraud and risk?

Experiences gained from previous economic crises have reshaped individual and corporate attitudes and practices. Certainly, the folks who experienced the Great Depression turned into a generation of savers, conservative spenders, and cautious borrowers. Recent discussions with payment leaders have given rise to the possibility that conservative spending habits may be with us for some time. These habits may be manifested in restricted, prioritized spending on payment initiatives in general and fraud and risk mitigation efforts more specifically.

Given the already narrowing margins in retail payment profits, coupled with enterprisewide scrutiny of expenses across business silos, it is likely that payment organizations will have to prioritize spending in ways not typical of the last decade of innovation and constant change. These limitations will create choices concerning which investments are mandatory and which are discretionary. Investments in initiatives directed at data security and fraud detection might take a back seat to investments in relieving the pent-up demand for maintenance and enhancements of core payment and settlement systems or investments in exciting new technology.

In an ideal world, focused and well-reasoned business case analysis would dictate the priority of spending. My personal experience, however, has revealed that investments in fraud reduction, data security, etc., face an uphill battle when competing for scarce dollars. This phenomenon stems from three major factors. First, there is always a perception that risk/fraud expenditures are discretionary. It remains to be seen if

the staggering cost of poor risk management that led to the financial crisis, coupled with the everyday visibility of fraud schemes, will help shed the discretionary label. Discretion, by the way, not only involves expenditures on new artificial intelligence software or high-tech encryption devices; it also involves more subtle decisions about the number of staff authorized to monitor systems, notify customers of breaches, and research problems. After all, the risks involved in past lending and investment practice that were at the heart of the financial crisis largely involved "payment" of obligations and not "payments."

Second, to do effective business case analysis, good data must be present. It is not at all clear whether banks and other payment providers have transparent and reliable systems in place to detect, measure, and categorize fraud in a way that allows its financial impacts to be estimated. Certainly, banks have historically been reluctant to share such data externally. Further, do banks have in place systems that can collect and allocate fraud management costs in such a way as to complete a meaningful cost-benefit analysis? Without good data, business case analysis becomes an art, not a science. Clearly, for bad actors fraud is their core business; there is no business case to explore and no budget committee to satisfy. In fact, their pursuits are recession proof.

Finally, investments are about the future, not the past. My personal experience in this area is that the past is a poor predictor of the future. In that light, how does an organization forecast likely trends in fraud losses? Is the past a good predictor of the future? Can recent trends such as the reduction of unauthorized activity in the ACH network reasonably be extrapolated, or will the fraudsters simply move to another payment channel where controls are weaker? More importantly, will new technology help bad actors commit fraud more easily or help banks do a better job of detecting and preventing fraud? Should the business case for the future depend on average industry trend data or should it protect against "the big one," the major incident that culminates in a $100 million–$200 million loss? Answers to these questions will ultimately separate the prepared from the unprepared.

Regardless of the answers to these perpetually difficult questions, most of which will stem from core experiences and individual philosophies, one thing is certain in the wake of our recent experience: Reputation is more important than ever. Positive reputations are difficult to build, hard to maintain, easy to lose, and even harder to reclaim. The value placed on reputation must be carefully considered by senior decision makers in setting the course for the future.

AUGUST 24, 2009

Forum launches "Payments Spotlight" podcast series

Since February 2009, the Retail Payments Risk Forum has regularly posted to the Portals and Rails blog interesting and thought-provoking topics related to retail payments risk issues. This online forum provides a dynamic platform to spark conversation and foster ideas about these topics. In an effort to further expand the dialogue, we are excited to announce the launch of the Payments Spotlight podcast series this month.

Payments Spotlight will be posted regularly on the Federal Reserve Bank of Atlanta's Web site. The podcast will feature recorded interviews with leading experts in the payments industry on relevant issues. The first installment features a conversation with Woody Tyner, payments strategist at BB&T Bank in North Carolina. In his comments, Mr. Tyner provides an insightful perspective that is definitely worth a listen on how the payments industry can balance innovation and risk management.

We hope that you will not only check out this installment but also tune in on a regular basis as we feature other leading thinkers and practitioners representing a wide array of perspectives. You can listen to the Payments Spotlight podcast using any computer audio software that will play MP3 files. To subscribe to the podcast series directly, go to the Atlanta Fed podcast page, click on the "subscribe" button next to Payments Spotlight, and follow the instructions for adding the series to your aggregator. You can also follow the series by staying tuned to Portals and Rails, where we will post information about new podcasts as they become available.

Let us know what you think, and please submit any suggestions you have for future podcast topics.

By Jennifer Grier, senior payments risk analyst in the Retail Payments Risk Forum at the Atlanta Fed

AUGUST 31, 2009

Will micropayments thrive in social networks? (Part 1 of 2)

This is the first of a two-part series on micropayments and social networks.

One of the most recent, and indeed interesting, phenomena is the entrance of social networks into the micropayments arena. Micropayments, generally defined as small-dollar transactions of $25 or less, are inherently inefficient. Converting them into electronic payments from the traditional cash market is costly, since fees such as interchange can consume a large percentage, if not all, of the transaction.

However, things have been changing recently as the environment for small payments has grown more hospitable. Credit card companies have introduced contactless payment devices to address the costs associated with unattended purchases such as parking meters and vending machines. The emergence of online payment network contenders such as PayPal, Amazon, Google, and others has fueled the growth of online micropayment transactions, as has the growth in online media sales, such as the 99-cent songs on Apple's iTunes.

Several social networks have gained popularity recently as trusted sites for the exchange of information, digital media, and communication. This popularity and trust can help foster the network effect necessary for establishing an effective payment system. However, developing a new payment system is a risky venture, and many micropayment provider start-ups are not successful.

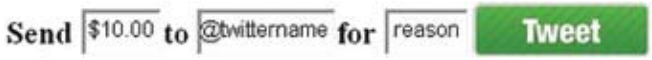
While some social network sites are exploring the opportunities to offer payment services, they are also permitting outside payment providers to place their applications on the social network platforms. These payment providers are able to leverage the social network platforms providing online payment solutions and monetizing digital currency.

The demand for digital currency via social networks and the ability to monetize transactions in virtual economies are garnering attention from venture capitalists—and they've captured our attention, for the moment. The remainder of this blog as well as next week's will examine a few examples of the emerging micropayment service providers that we found. Keep in mind, our list is by no means an endorsement or an exhaustive list.

Twitpay

First, consider Twitter, a social networking site that lets users give short updates to other users about what they are doing. Twitter has, in essence, created an ecosystem in which third-party service providers are leveraging it to enable micropayments. A recent person-to-person (P2P) start-up called Twitpay allows Twitter users to send payments to other Twitter users—that is, as long as they both have PayPal accounts. As a third-party application that merely uses the Twitter platform, Twitpay has no formal ties to Twitter, aside from the similar name.

Here is how the application looks on the Twitpay site.



The user fills in the payment instructions and presses the "tweet" link at https://twitpay.me. The application delivers the payment to the recipient's Twitter Twitpay account. The recipient pays the cost of the transaction, which currently consists of PayPal's commercial transaction fee of 2.9 percent of plus 30 cents. A user also can replenish his Twitpay account using PayPal.

Twollars

Another third-party application that recently started using the Twitter platform is Twollars, a vehicle for charitable giving in small-dollar denominations that allows Twitter account holders to donate to a charity or cause of their choice. Twollars was conceived in January 2009 as a way for people on Twitter to thank one another for sharing digital content and giving advice and information. Symbolic currency on "twollars" can be converted by charities into real currencies, such as dollars and euros, for example, again via PayPal. The Twollars Web site contends that Twollars can only be converted into real currency through donations to good causes. Charities can start campaigns on Twitter to raise funds. Any Twitter user starts with 50 Twollars. The Twitter platform allows even the smallest charity to reach a large audience. The site even allows businesses to reward customers with Twollars to be used for a charitable cause of their choice.

Next week in Part 2, we look at Facebook as well as other players in this emerging market such as Spare Change, Zong, and BOKU.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

SEPTEMBER 08, 2009

Will micropayments thrive in social networks? (Part 2 of 2)

Last week's blog posting discussed how some social network sites are exploring the opportunities to offer payment services or are permitting outside payment providers to operate on their social network platforms. Twitpay and Twollars, two third-party platforms used on the Twitter platform, were discussed in Part 1. This week, we examine other players in this emerging market.

Facebook

Facebook is likewise evolving as an ecosystem for emerging micropayment service providers. Users are increasingly spending real money buying virtual goods on the applications that run on Facebook's platform as well as Facebook credits. Facebook credits are funded using major credit cards and available in U.S. dollars as well as foreign currency denominations. The social network has realized tremendous success since its inception. Recently the research firm Nielsen revealed that Americans spent more time on Facebook sites than other top Internet sites in its June 2009 report.

Table 1: Top 10 Parent Companies/Divisions for June 2009 (U.S., Home, and Work)

Rank	Parent	Unique Audience (000)	Time Per Person (hh:mm:ss)
1	Google	155,606	02:31:08
2	Microsoft	139,099	02:12:20
3	Yahoo!	134,304	03:15:55
4	AOL LLC	92,705	02:43:10
5	News Corp. Online	90,308	01:54:59
6	Facebook	87,254	04:39:33
6	InterActiveCorp	67,283	00:20:05
8	eBay	67,208	01:17:59
9	Apple Computer	59,663	01:19:33
10	Amazon	59,552	00:25:41

Source: Nielsen NetView

In addition to providing the platform for other payment application developers, Facebook recently launched its own virtual currency payment service for applications on its network called "Pay with Facebook." The new service is currently live with its application GroupCard, which allows users to purchase items from $3 to $25 and pay for them with a credit card or Facebook credits.

It will be interesting to see if the growth of the Facebook network drives adoption of the newly introduced payment service.

Spare Change

Spare Change is a payment application currently on social networks Facebook, MySpace, and Bebo that lets users make purchases from social network applications and games and then make payment via PayPal. Users can open a Spare Change account and fund it with a credit card, PayPal, bank account, or mobile phone. According to the Web site, consumers can use Spare Change balances to purchase hundreds of applications easily—an "iTunes-style business model for social networks." Spare Change markets itself as the largest micropayments system for social networks, claiming acceptance by more than 700 different games and applications.

Zong

Zong is a payment provider that allows consumers to purchase virtual currency, gifts, and other applications on social networks via the mobile phone in lieu of traditional payment methods. Zong uses the mobile carriers with whom it partners to bill customers for their transactions. Once the consumer has paid his or her mobile phone bill, Zong in turn pays the merchant. The distinguishing feature for Zong's business model for micropayments is its nine-year relationship with mobile carriers globally. However, at this time Zong is currently available for digital goods and services only.

BOKU

BOKU functions similarly to Zong in that it enables micropayments for games and applications and doesn't require users to pay via a credit card or traditional bank account. Instead the transaction charges are itemized on the user's monthly cell phone bill. BOKU's partnership with social network hi5 affords it an international presence where users in 24 countries can purchase virtual currency with their mobile phones. BOKU recently expanded into the United States through agreements with mobile carriers AT&T and T-Mobile.

This certainly isn't an exhaustive list (and is not an endorsement), but it is enough to give you a general idea of some emerging trends. And while the market audience for the goods and services available on social networks is focused on games and applications, it could change as social networks become increasingly ubiquitous. As social networks evolve, the risk environment for virtual and electronic micropayments will be on our radar.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

SEPTEMBER 14, 2009

Stickers and skins: The next phase in proximity payments and mobile payments

I just became the owner of a GO-Tag, an example of a sticker that contains contactless payment technology that you can adhere to an item of your choice. I removed the adhesive backing and attached it to the back of my iPhone, enabling it as a proximity payment device. The sticker contains an embedded chip that uses a technology called near-field communication, or NFC for short, which allows short-range contactless payments. This embedded chip technology is more ubiquitous than you might think. It's also used in transit cards and toll road transponders, in addition to plastic payment cards. In developing countries that did not invest as heavily in magnetic stripe infrastructure as we did here in the United States, chip cards are much more prevalent. And the lack of a legacy infrastructure in those countries has accommodated a smoother transition to the adoption of mobile handsets embedded with contactless technology.

Another innovation is the mobile phone payment "skin," which wraps and adheres to the phone and is embedded with a contactless payment chip. One product we found is called Phoolah. The skin-wrapped phone can be waved at a merchant's point-of-sale reader to effect a transaction. Both the skin and the sticker are similar in that they work as open-loop, stored-value payments that are limited to a specific population of merchants participating in the rollout phase of both products. And what might make them the next phase in contactless payments is that they separate the payment functionality from the legacy plastic card to some other device, typically a mobile phone.

Both examples of the mobile phone skin and sticker are issued by Metabank and run on the major card association rails. Some of the retailers accepting stickers and skins include 7-Eleven, McDonald's, and CVS, to name a few.

Magnetic stripe inertia

Advocates of chip technology assert that chip technology is more secure than the magnetic stripe variety because it is more difficult to duplicate, a process known as "skimming." Furthermore, because they store more information than stripes, the chips can accommodate more sophisticated security functions such as encryption and authentication. These enhanced security features have influenced the European Payments Council (EPC) to announce recently that it is considering a ban on magnetic stripe cards within the next few years in favor of chip cards augmented by PIN authentication.

However, chip technology has faced some hurdles in the United States as merchants and consumers are comfortable with legacy magnetic stripe products. The infrastructure has been long established in the United States and is expensive to change. Pilot contactless cards have been introduced running the parallel technologies, affording the use of both the chip and the magnetic stripe. The distribution of readers for both contactless and stripe is not consistent and has resulted in a certain degree of confusion for both consumers and operators at the merchant's point of sale. What may overcome this confusion is the use of mobile phones as devices with embedded chips. The prevelance of mobile telephones in the marketplace may increase the likelihood that consumers will try out the technology.

Implications for mobile payments

The industry is hard at work addressing the obstacles to mobile payments—different legal frameworks for telecom and financial institutions, the large number of carriers and handset makers, and the need to establish technical standards for consistent interoperability among all industry participants. For now, stickers and skins may provide a low-cost opportunity to both test consumer and merchant acceptance and transition the industry to the next phase of payment innovation.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

SEPTEMBER 21, 2009

Not all payments are equal under "good funds" laws

Anyone who has participated in a real estate closing can attest that it can be a daunting experience. There are many parties with their hands out at the closing table to consummate the deal—the buyer, seller, and attorneys, to name a few. However, it can all collapse like a house of cards if the funds underlying the transaction are not collected or "good."

Ripple effects can be devestating when a lender fails to properly fund an escrow closing transaction. A notable case is the collapse of mortgage lender Abbey Financial in 1994, which resulted in hundreds of consumers over six states stranded with either unfunded mortgages or double mortgages because their first mortgage was not paid off in a loan refinancing. Many of Abbey's checks were dishonored, which left several attorneys with shortfalls in their trust accounts.

The aftermath of Abbey sent shock waves through the mortgage industry and prompted many states to enact "Good Funds" laws to ensure that the money funding a real estate purchase and refinance transaction is secure and ready for disbursement. The purpose of the law is to provide assurance to the consumer and other parties that the funds are in the proper hands before the deed or mortgage is recorded. This thereby protects the seller from conveying property to a buyer whose check is drawn on an account with insufficient funds.

What makes a payment "good"?

Typically, a closing agent will deposit all funds connected to a real estate transaction into an escrow account for disbursement at the closing. Most good funds laws stipulate the type of funds (e.g., cashier's checks, or wire transfers) that an escrow agent can accept. However, what is considered "good funds" can vary by state. In Georgia, for example, the law expressly permits certain types of checks:

> A settlement agent may disburse proceeds from its escrow account after receipt of any of the following negotiable instruments even though the same are not collected funds: (1) a cashier's check from a federally insured bank, savings bank, savings and loan association, or credit union…; (2) a check drawn on the escrow account of an attorney or real estate broker…; (3) a check issued by the United States or Georgia…; and (4) a check or checks not exceeding $5,000 in aggregate per loan closing.

Several states have taken a stricter approach in defining acceptable funds. Specifically, wire transfers are often the only funding mechanism allowed and, in some cases, are required for transactions over a certain dollar amount.

Although not an exhaustive list, a general Internet search revealed that Indiana, Minnesota, Missouri, and Texas are among those states with good funds laws that limit electronic funds transfers to "wire transfers" instead of the broader "electronic payment," as defined in Regulation CC (12 CFR 220.10 (p)), which would otherwise permit funding using automated clearinghouse (ACH).

For example, the Indiana Good Funds Law defines wired funds as "good" but requires that they be "unconditionally held by and irrevocably credited to the escrow account of the closing agent." Only funds transferred through Fedwire or CHIPS are immediate, final, and irrevocable. Consequently, it appears that Indiana's law excludes electronic fund transfers through ACH since consumer Regulation E rights with regard to unauthorized ACH credits may create some risk that ACH funding of a real estate transaction could be reversed long after the closing.

Secure funds important in uncertain times

The current housing crisis has undoubtedly caused some anxiety for all parties in a real estate transaction about the risk of a deal falling through. Numerous bank failures and increased real estate fraud have further complicated the process. Although there are differences by state, the good funds laws help to mitigate some of the risks by helping to ensure that the funding of real estate transactions is reliable.

By Jennifer Grier, senior payments risk analyst in the Retail Payments Risk Forum at the Atlanta Fed

Coordinating roles in mobile payments: Who will we trust?

The concept of mobile payments is beginning to gain some traction as the industry grapples with environmental complexities—namely the myriad participants in the mobile payments arena, the mulitiple channels for a mobile payment to follow, and the ever-present questions about security. Who can be trusted to intercede among the various entities with an interest in the payments process? While a number of roles in the mobile payments arena are taking shape, the least known and possibly the most confusing is the concept of the trusted service manager (TSM). However, this role is also possibly the most critical to establishing a secure and trusted environment for mobile payments. So what exactly is a TSM and what are its responsibilities?

Complex environment for mobile payments

While anecdotes sometimes dismiss the anticipated speed to market of mobile payments as industry hype, the fact is that the ubiquity of the mobile phone is driving the convergence of telecom and payments. This convergence creates a far more complex environment for payments than ever before. Telecom participants and financial institutions have different regulatory and legal frameworks and distinctly different risk exposure, for example. Furthermore, the U.S. mobile payments environment will leverage existing payment channels, such as the automated clearinghouse (ACH) and the card networks. No one knows if the industry and market will ultimately prefer a particular channel. The result is an array of business models with a vast number of unrelated players with competing interests for customer revenue.

Stakeholders in the mobile payments business model

In addition to the traditional payments model that includes the customer, financial institutions, and perhaps payment processors, the developing mobile payments ecosystem also includes large groups of mobile network operators and handset makers who have no previous payments life cycle experience. For payment system interoperability, all participants must agree to operate under uniform technical operating and security standards. In this context, the role of a TSM is to manage collaboration among the various stakeholders.

Role of the TSM

The concept of the TSM was introduced by the Global System for Mobile Communications Association (GSM) in 2007 in an effort to improve interoperability among various and unrelated proprietary mobile networks. The core function of the TSM is to serve as a neutral and independent middleman between financial institutions, payment network operators, customers, and the mobile network operators.

Responsibilites envisioned for the TSM include managing contractual relationships with the large number of mobile network operators (MNOs) as well as acting as a single point of contact for banks and other payment service providers to communicate with customers they share with the MNOs and handset makers. The key to the TSM's success clearly is the financial wherewithal to inspire trust on behalf of the other payment participants and to support agreements with a large number of partners. Finally, the TSM should also provide the oversight for various systems among participants to ensure secure transmission of payments and personal data in the transaction.

Who should fill the role?

While the need for a TSM is recognized, there is no consensus on who should fill that role. MNOs, payment network operators, and financial institutions lack the economic incentives to form alliances with other participants in the payment ecosystem because of their competing interests for customer revenue. Whether the role is filled by a consortium of existing players or by a new entity yet to be formed will depend on an ability to fulfill these critical responsibilities from a position of neutrality and independence.

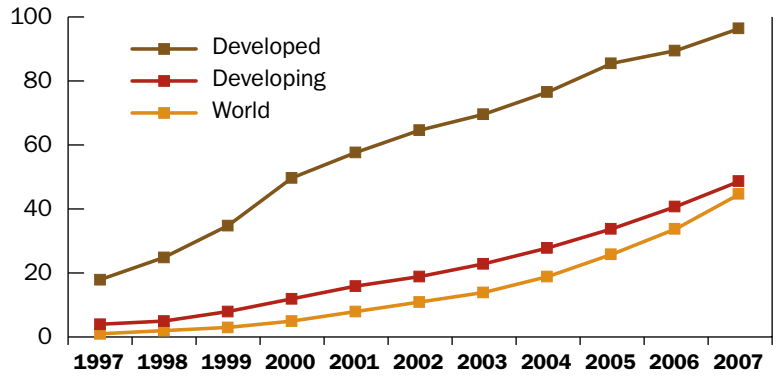
By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

OCTOBER 05, 2009

Mobile top-up for international remittances: New opportunities and new risks

The growth in the mobile telecommunication industry worldwide is driving the ubiquity of handsets, which in turn is expanding the reach of financial services across wireless networks in less developed countries.

Mobile telephone subscribers per 100 inhabitants, 1997-2007



Source: International Telecommunications Union

Adding air-time value (industry parlance known as "mobile top-up") to a mobile phone represents a new method that some mobile network operators (MNOs) are using to provide payment services, particularly in emerging countries where financial services are scarce. One example is Safaricom's M-Pesa, offered in Kenya and Tanzania. This service uses money agents, often small village stores, to sell additional air time on mobile phones. This air time can then be used for nontelecom purchases of goods and services, or sent via text message (SMS) as a person-to-person (P2P) payment transfer, allowing the recipient to use the prepaid value.

A recent case study found improved financial access in years following the 2007 launch of M-Pesa. The availability of mobile payment services lessened the population's reliance upon more risky hand-to-hand transfers and has been widely reported as a positive development for these emerging economies. Initiatives such as the Mobile Money for the Unbanked (MMU) program supported in part by the Bill and Melinda Gates Foundation, are contributing to the expanded use of mobile financial services in emerging markets.

Mobile top-up is also emerging as a means for international remittances by allowing users in one country, such as the United States, to purchase mobile air time for users in other countries, thereby "topping-up" the recipient's account in the local currency. For example, Western Union recently announced a service to provide mobile top-up remittances within the United States for users of phones issued by LIME in the Caribbean. Because many international telecom operators have roaming agreements that span geographic borders, mobile top-up remittances can be far-reaching, with the recipient using the prepaid value on the mobile phone to purchase goods and services in the home country.

While these innovations have been shown to have positive impacts in terms of access to financial services in emerging markets and may offer a number of other efficiency benefits, they also alter the risk profile for service providers and those who monitor payments for criminal activity. Depending upon the business model and parties involved, regulatory and law enforcement agencies will have new issues to consider in terms of anti-money laundering and monitoring international payment flows under existing laws. These developments in the mobile top-up market deserve continued attention to ensure that effective policing of payment flows can ride alongside the positive developments in the emergence of a new means for movement of money internationally.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

OCTOBER 13, 2009

Patenting the payments system: New developments in patent law may have dramatic impact on payments players

A seemingly obscure point of interpretation of U.S. patent law could have meaningful impact on innovation in the payments market. This interpretation could affect new players and existing players alike and deserves attention. Investments in innovative new payments technologies always carry risks. Investments can fail if the business model does not come to fruition. Poor understanding of vulnerabilities in new technology could open up new opportunities to fraudsters or simply could alter risks for parties to the transaction or providers of the transaction service itself. However, those same investments in payments innovation could also serve to strengthen the defenses to various risks, thereby improving the overall picture for all.

On November 9, 2009, the Supreme Court will hear the *Bilski* case, which draws into question the viability of business method patents. This is a subcategory of the range of patents that have been issued in recent years for payments-related innovations described in a previous Portals and Rails post. In particular, *Bilski* will address the issue of whether U.S. patent law requires that the subject matter of patents be reflective of machines or some physical transformation of matter. Included in this issue is a question of whether abstract ideas that mention computers as a means to reduce the idea to practice are patentable as well. This case could affect the calculus for making new payments technology investments overall.

Some feel that a ruling by the Supreme Court that limits patentable subject matter to exclude business methods will negatively affect a wide array of innovations, including those for the manipulation of information, whether or not implemented by computer. Others, including some from the financial services industry, feel that business method patents should be limited or eliminated and that progress and innovation will in fact be strengthened as there will be less threat of suit by those who obtain monopoly patent rights on "abstract ideas."

Payments innovations are firmly ensconced as part of the "knowledge economy." In the payments context, as reported in this blog and elsewhere, there are a dynamic array of technology and business model developments and an ongoing stream of new patents and patent applications. Just think of the array of new ways that payments can be accomplished using the Internet in the past 10 years or so. Many of these existing and future innovations may be affected by the *Bilski* decision one way or the other.

Patents have been seen as a key tool to reward financial services innovations and as a means for new entry into various market segments. Patents also serve to disclose publicly the nature of the invention, which helps to drive other, follow-on innovations. Over the long term, limiting patent protection for business methods could alter the reward incentive structure for payment innovations. Or it could remove an impediment to product investments in payments as there is less threat of suit, which may allow for more rapid deployment of innovative new products and services.

The Supreme Court's decision in *Bilski* could have a dramatic impact on the payments marketplace as competitors may have to adjust their sights in terms of how they protect and deploy their innovations. New players in the marketplace may find it more difficult to enter the payments markets while existing players may or may not have their market positions strengthened.

For now, the jury is out, so to speak. To get a deeper sense of the issues being considered, see the related briefs filed with the Supreme Court.

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

OCTOBER 20, 2009

Building a bridge: Will proactive discussions of fraud concerns help drive financial services and telecom industry collaboration in the emerging mobile payments context?

Much has been written in this blog and elsewhere about the emergence of mobile phone-enabled payments. Recently, we had the pleasure of attending two excellent conferences that stimulated thinking about how the lines between two major industries, telecoms and financial services, are beginning to blur. First was the Finovate 2009 conference in New York. Among a wide array of financial services technologies and business model demos presented was a fascinating lineup of emerging methods for accomplishing payments transactions using the mobile phone. Clearly, much new innovation is emerging in this area. Technology providers are building bridges between banks and telecoms in this environment. All of this fertile stew of ideas bears watching in the years to come.

Second, we recently attended a joint session put together by the Santa Fe Group Vendor Council and the Communications Fraud Control Association in Atlanta. This meeting offered an opportunity for those thinking about fraud controls in the payments arena and those concerned about fraud in the communications (telecoms) industry to begin to discuss issues of mutual concern as mobile payments emerge in the United States and abroad.

For example, issues at the table included the following:

- Registration protocols vary significantly between mobile services and bank payment services. This variation can complicate the forensics on a fraudulent transaction in the aftermath as either investigators within banks or telecoms or law enforcement may find it very difficult to map a transaction to a particular person through mobile payments channels.
- Authentication protocols are also differentiated because of regulatory requirements and industry practices. These protocols complicate investigations as varying audit trails create complexities.
- Malware concerns such as SMiShing in mobile phones are emerging and may be creating new and poorly understood vulnerabilities and hacker threats in the payments environment.
- Fraud detection "flags" may not be translated or communicated well between the two industries. What happens when a phone is reported as lost to the mobile carrier, and it is a fully enabled mobile wallet? Does the bank with whom the customer is affiliated also need to be notified? Does a compromised account at a bank also need to be reported to the telecom provider when the phone is a transaction device?
- Are fraud investigators duplicating efforts when they investigate a fraudulent episode involving a mobile payments transaction? How could these efforts be better coordinated?
- Do privacy restrictions in the banking and telecom environments create undue barriers to sharing of useful information to help track down bad actors?
- If a payment transaction is reliant upon an "always on" mobile connection, what happens to the transaction when and if a connection is lost midstream? Who is responsible? What about the fraud risk?

These and other issues were raised in the context of the discussion, and all agreed that further elaboration of these issues was needed to determine the best opportunities for collaborative action. However, it seemed clear that when it comes to fraud, open channels between the two industries could go a long way to ensuring effective deterrence and loss mitigation in the mobile payments environment.

On a larger scale, these conversations are likely to deepen as many of the emerging mobile payments business models take hold. In this emerging environment, collaborative cross-industry work on fraud issues could be a positive launching point for breaking down industry silos for the good of financial services and telecommunications companies, and it could benefit their customers, which will in turn further support the utilization of all those innovative mobile payments models we heard about at Finovate.

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

OCTOBER 26, 2009

Survey shows risk concerns slow adoption of cell phones for mobile payments

Cell phones may be everywhere, but adoption of the devices as mobile payments delivery channels by financial institutions and consumers faces an array of obstacles. These include concerns about security risk, consumer demand, and revenue according to a 2008 survey of New England depository financial institutions on mobile banking by the Federal Reserve Bank of Boston (FRBB) and the New England Automated Clearing House Association (NEACH). The results are published in a joint paper titled "Mobile Banking in New England: The Current State of the Market." The paper describes the enabling technologies, barriers, and associated risks with mobile banking services from the perspectives of the more than 300 banks and credit unions in the New England region that participated in the survey.

The state of mobile banking in the United States

Financial institutions have different value propositions for mobile banking services. Most financial institutions are absorbing the expenses associated with mobile offerings to remain competitive and retain depositors while some view it as an extension of their online banking services, including routine call center inquiries with self-service bank inquiries. Mobile banking may also appeal to unbanked consumers, particularly for remittance services.

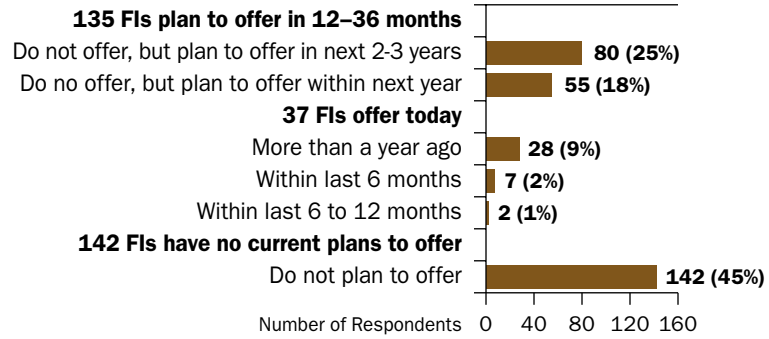
The report noted that consumer adoption might be improved with efforts to provide better education on the benefits and risks of mobile banking and payment services. Concerns with security may be addressed by implementing multifactor authentication controls on handsets, using antivirus software, as well as imposing transaction limits, to name a few.

Perhaps the most notable conclusion presented in the report is that better collaboration between mobile participants is necessary. The entry of mobile network operators (MNOs) into the payments arena may create competition for financial institutions providing mobile payment services. Numerous conflicts exist between MNOs and financial institutions because of their starkly different business models and disagreement over customer ownership. Wide-scale adoption of mobile banking and payments going forward may depend upon the future cooperation of the telecom and banking industries to establish a sound and effective mobile banking environment.

Security risk a key barrier for mobile banking

While 43 percent of the respondents indicated that they plan to offer mobile banking services in the next three years, almost half reported no plans to offer mobile banking. The reasons for not offering mobile banking included the lack of customer demand, inadequate resources, and concerns about security.

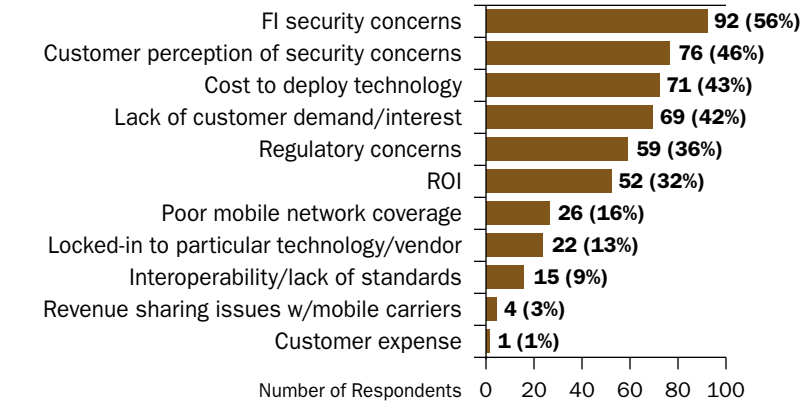
When did you start offering mobile banking to your customers? (n = 314)



Source: Federal Reserve Bank of Boston

In fact, when ranking the top three barriers to adopting mobile banking services, the survey respondents ranked security as their top concern.

What do you perceive to be the top three barriers to banks implementing mobile banking? (n = 164)



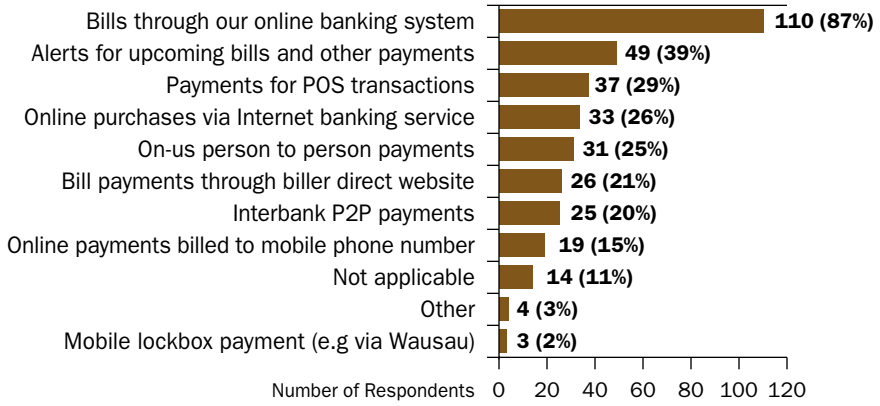
Source: Federal Reserve Bank of Boston

Most planned services bill-pay related

For financial institutions that currently offer mobile payment services (in addition to mobile banking services) or plan to do so, the most popular response, at 87 percent,

was bill payment through online banking systems. Other popular choices included sending bill payment alerts, payments at the point of sale, and online purchases through the Internet.

If you offer/will offer mobile payment services, please select all features that your FI is considering? (n = 126)



Source: Federal Reserve Bank of Boston

A fledgling market in transition

The survey concluded that much work needs to be done to encourage adoption because of the current state of customer demand, safety, and value proposition for financial institutions, especially for the smaller FIs and Credit Unions. It reports that despite media excitement about the future of mobile banking and payments, the market needs time to engage the numerous parties at the proverbial table, including the MNOs, the handset makers, and financial institutions themselves, to alleviate real and perceived barriers to adoption.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum, and Jennifer Grier, senior payments risk analyst at the Atlanta Fed

NOVEMBER 02, 2009

Payments Spotlight Podcast: WACHA's Gilmeister discusses commercial account takeovers and other emerging risks

We invite you to listen to an interview with Mary Gilmeister, President of the Wisconsin Automated Clearinghouse Association (WACHA) and a member of the Retail Payments Risk Forum's Advisory Group. Launched in August 2009, this is the second iteration of the Retail Payments Risk Forum's Payments Spotlight podcast series.

In this interview, Ms. Gilmeister touches upon the following topics:

- the roles of regional payments associations like WACHA,
- thoughts on managing the emerging risk of commercial account takeovers which result in fraudulent ACH transfers,
- protecting the elderly from financial fraud,
- the role of the NACHA Risk Management Advisory Group, and
- new risk issues in the emerging payments environment.

If you have not already, we also invite you to give a listen to the first installment of Payments Spotlight, which featured a conversation with Woody Tyner, payments strategist at BB&T Bank in North Carolina.

We hope that you will not only check out this installment but also tune in on a regular basis as we feature other leading thinkers and practitioners representing a wide array of perspectives. You can listen to the Payments Spotlight podcast using any computer audio software that will play MP3 files. To subscribe to the podcast series directly, go to the Atlanta Fed podcast page, click on the "SUBSCRIBE" button next to Payments Spotlight, and follow the instructions for adding the series to your aggregator. You can also follow the series by staying tuned to Portals and Rails, where we will post information about new podcasts as they become available.

Let us know what you think!

NOVEMBER 09, 2009

Will interchange provide the driver for disruptive payments innovation?

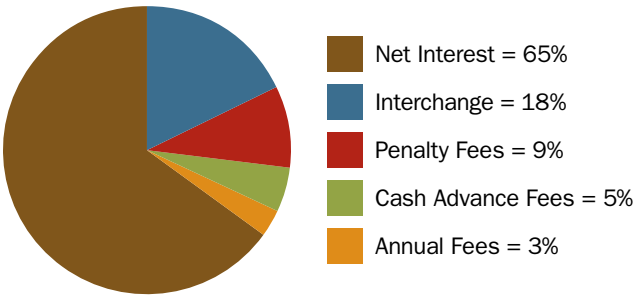
Many start-up payment providers have emerged recently with an eye on competing with traditional credit and debit card networks by undercutting interchange fees. Will the ongoing public debate concerning interchange fees help drive their success?

The use of both debit and credit cards has been rising rapidly in the United States in recent years as an electronic alternative to paper checks and cash. However, recent credit card legislation as well as an ongoing debate concerning interchange fees could influence the direction of that growth.

In simplified terms, interchange fees represent the costs paid by merchants to their banks for processing card transactions. The card-issuing bank may also use revenue earned from interchange fees to fund loyalty rewards to attract customers. Recently merchants have contended that the interchange costs they pay for card transactions have become excessively high. Given the universal acceptance of the major card networks, merchants contend they have few meaningful alternatives for consumers to transact payments, especially at the point of sale. On the other hand, card companies indicate that interchange fees are fair compensation for providing a valuable service to merchants.

So how do card issuers earn revenue on cards? This example shows a breakdown of issuer revenue in 2004. In this example, interchange represents 18 percent of the card issuer's total revenue.

U.S. Card Issuer Revenue Sources, 2004



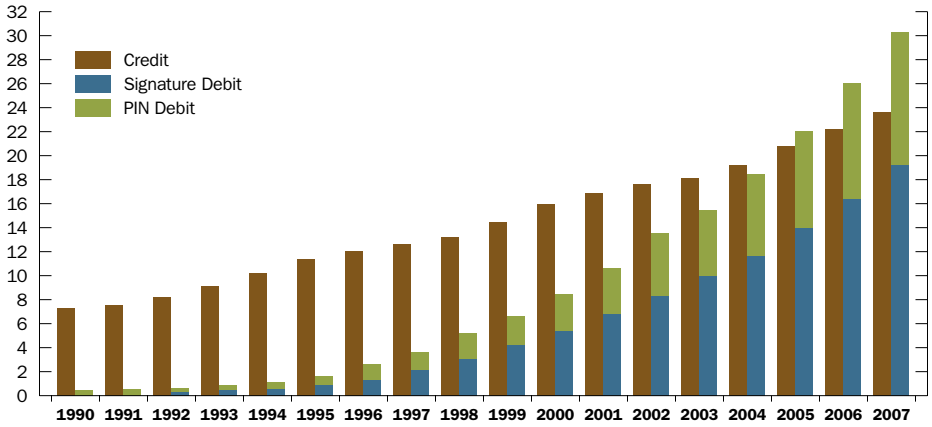
Source: *Charging Ahead: The Growth and Regulation of Payment Card Markets*, Richard Mann, Cambridge University Press, 2006

Various trends and policy debates regarding interchange fees and card revenue sources appear to be a factor in the development of innovative point of sale payment methods that seek to compete directly against card networks.

Growth in card use has increased payment processing costs for merchants

The Federal Reserve Board published a staff research paper in May 2009 titled Interchange Fees and Payment Card Networks: Economics, Industry Developments, and Policy Issues. This report considers the economics underlying interchange fees and the background for understanding the interchange fee debate. Merchants argue that recent increases in fee rates, along with transaction volume growth, have increased their card acceptance costs substantially.

Total Number of U.S. Purchase Transactions by Transaction Type (in millions)



Source: Author's calculations based on the ATM and Debit News EFT Data Book, The Nilson Report, sand other industry sources. Note: Credit includes charge cards and private-label credit cards issued by retailers.

According to this report, an argument in favor of interchange fees is that they support the universal acceptance of cards through the strength and efficiency of the card networks. The standard fee, set by the card networks, is established in a way that balances merchant costs with the economic benefits merchants realize through the value of the network. Further, consumer adoption is driven partly by consumer protections associated with the use of cards. Overall, merchants who accept cards may realize increased sales, particularly for large value transactions relying upon credit.

Another factor: The impact of credit card legislation
Recently passed credit card legislation limits or prohibits certain fee and interest charges imposed on credit cards. As a result, some expect card issuers to limit or even to eliminate loyalty reward programs and raise interest rates and fees for more creditworthy card holders. While it remains to be seen, these kinds of effects could alter the economics of card networks, potentially opening up avenues for new competition.

Will these developments create opportunities for innovators of payment alternatives at the point of sale?
Companies such as Revolution Money and Tempo, among others, are working to establish independent point-of-sale payment systems from the established card networks with alternative transaction pricing models. Both companies are offering cards (Revolution issues credit and Tempo "decoupled" ACH debit) that compete partly by bypassing the interchange fees of the major card networks. In addition, successful online payments providers like Paypal and others are reportedly looking to compete at the merchant locale as well. In all these examples, competitors will face the classic "network effect" problem in that success requires adoption by both consumers and merchants. The success of these business models at the point of sale remains to be seen and may depend on those very merchants that complain about the current interchange system.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

NOVEMBER 16, 2009

Threats to online banking security may alter payment choice

During the last several months, a variety of government agencies, industry organizations, and the media have alerted banks, their customers, and the public to hacking attacks resulting in fraudulent funds transfers using online banking interfaces. These attacks particularly affected commercial bank accounts. For example, the Federal Deposit Insurance Corporation (FDIC) issued an alert regarding this form of attack earlier this year. Both the FDIC and the FBI have recently issued alerts referring to how this hacker attack is being used in conjunction with "money mule" schemes to attempt to hide the fraudulent funds transfers.

In one variety of these attacks, hackers using phishing techniques direct people to spoofed Web sites where malware Trojans are then downloaded to the affected computer. This malware then allows the hacker to infiltrate online banking connections in a manner that can circumvent the customer authentication mechanisms put in place by banks. In simple terms, hackers have figured out how to "hitchhike" on a computer's secure online connection to a bank account and thereby initiate fraudulent funds transfers out of the account. We found a recorded webinar describing how this technique can work using the "Zeus" malware.

Multifactor authentication of the customer has been referenced but not required by bank regulatory guidance as a means banks should consider in protecting online banking systems generally. The guidance does not make technology-specific recommendations but leaves room for banks to make their own risk assessments regarding appropriate security means.

The recent events described above have now raised significant questions about the effectiveness and sufficiency of reliance on multifactor customer authentication as a means to keep fraudulent transactions out of payment networks accessible through online banking systems.

Some view this as another variant of the "whack-a-mole" problem, in which you might smack down one threat but another one just pops up quickly. In other words, we should not throw the baby out with the bath water by disregarding multifactor customer authentication as an effective method to mitigate fraud. Others have suggested the industry should rethink online banking security entirely by investing in systems that authenticate transactions instead of customers, as is common in card

Continued on next page

NOVEMBER 16, 2009

Continued from previous page

transaction security systems. Others suggest systems that provide out-of-band confirmations of transactions (by phone or by text) to avoid overreliance on the online banking channel alone for security.

While banks consider online banking security investments, their customers are increasingly faced with choices about their own use of these systems as they exist today. Some suggest standalone computers running open source operating systems as a security measure. Bank customers can make further use of "positive pay" arrangements with their banks and can better monitor their account activity daily. Each of these and other available security techniques brings new costs and "frictions" to online banking users. We considered the economic tradeoffs between privacy, data security, and fraud prevention in a prior Portals and Rails post.

At one extreme, some smaller commercial customers of banks may decide not to accept these added costs and instead opt out of online banking access to electronic funds transfer systems altogether if they feel unprotected in this environment. They might even choose to fall back to manual check payments. Is this choice an overreaction or a rational one?

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

NOVEMBER 23, 2009

Banks run more than just security risk with single-factor authentication

As described in a previous Portals and Rails post, various reports have indicated that business customers' online banking credentials are being compromised and the fraudsters are performing unauthorized EFT transactions using either the ACH or wire transfers to move money out of these accounts.

This recent phenomenon could be seen as part of a larger issue for security on the Web, prompting some to consider whether online banking security standards are adequate.

While a lot has been written on how this fraud happens, not much has focused on what happens next. The criminal side of this is fairly cut and dry. Law enforcement tries to track down the fraudsters and bring them to justice. If the FBI, Secret Service, or other agencies are able to track them down, apprehend them, and a conviction is made, the fraudsters spend some time in jail. The civil side of this is a little more complicated.

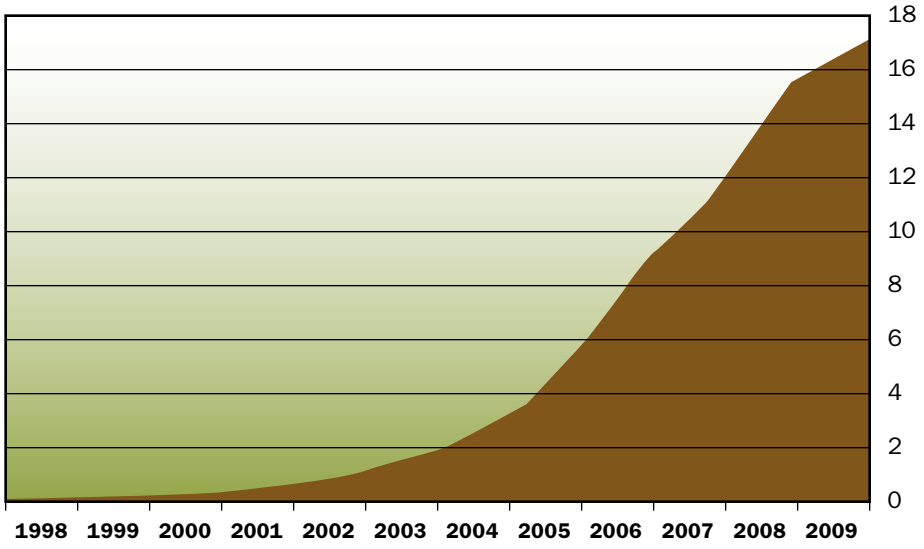
One civil case that has gotten some recent attention is the Shames-Yeakel case filed in federal court in Illinois. Marsha and Michael Shames-Yeakel had $26,500 stolen when an unknown person gained online access to the Shames-Yeakels' bank accounts by using Ms. Shames-Yeakel's username and password. The thief manipulated a line of credit and subsequently wired the funds out of the

Shames-Yeakel's business account to Hawaii and then off to a bank in Austria. While there is probably a good joke about yodeling while playing the ukulele buried in all of this, the Shames-Yeakels are not laughing. In fact, the hills are alive with litigation.

The plaintiffs first turned to their bank, who indicated that under the bank's online banking agreement, the plaintiffs were responsible for the lost funds. They next turned to the Office of Thrift Supervision (OTS), the bank's primary regulator, seeking protections under Regulation E and Regulation Z. The OTS found that these regulations did not apply as they were applicable to consumer loans and lines of credit.

Ultimately, the Shames-Yeakels sued their bank. The legal viability of their claims was considered by the Court in its Aug. 21, 2009, ruling on the bank's motion for summary judgment.

Vulnerability Disclosures Affecting Web Applications
Cumulative, year over year (in thousands)



Source: IBM X-Force®

While the court's opinion addressed a number of legal claims, it is the court's ruling on the plaintiff's negligence claim that bankers should pay close attention to. The basis of this claim is that the bank and its third-party Internet banking service provider did not follow the Federal Financial Institutions Examinations Council (FFIEC's) updated 2005 guidance on authentication in an Internet banking environment. At the time of the incident, the bank had user name and password access to their online banking system. The FFIEC's guidance does not require banks to use dual-factor or multi-factor authentication for these accounts, but it does state that the federal regulatory agencies consider single-factor authentication, like user name and password, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. In essence, the court indicated that while the facts must still be weighed by a jury, it declined to dismiss a negligence claim that the bank had breached a duty under Indiana law to protect the confidential information of its customers by failing to implement more robust security systems. The court stated: "In light of [the bank's] apparent delay in complying with FFIEC security standards, a reasonable finder of facts could conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access."

Another case to keep an eye on was filed in Maine this past September. The case involves a Maine based construction company, Patco, who is suing its bank for $588,000; the same amount of money that was stolen from Patco's account over the course of an eight day period in May. Similar to the Shames-Yeakel case, Patco is claiming that the bank failed to provide commercially reasonable protection because only a single-factor authentication system for its online banking system was in place. While no action has been taken as of yet, it will be interesting to see if the state court in Maine agrees that with the U.S. District Court in Illinois, allowing this negligence claim to move forward.

By guest blogger Michael T. Stewart, assistant vice president at the Boston Fed

NOVEMBER 30, 2009

KC Fed conference asks 'What's the future role for central banks in retail payments?'

On November 9–10, 2009, our colleagues at the Kansas City Fed hosted an international conference titled "The Changing Retail Payments Landscape: What Role for Central Banks?" This conference had a mixed format of paper presentations with discussants and more traditional panels of relevant experts from a range of perspectives. The conference offered a timely and unique opportunity to explore by international comparisons the roles that central banks and other public authorities can/should/should not play in various aspects of retail payments markets.

Themes of the event overall were described as follows:

- "Retail payments systems around the world have entered a period of dramatic change. This conference explored the changing retail payments landscape and assessed the extent to which central bank payments policies should correspondingly be altered. The conference brought together three principal audiences—industry participants, policy makers, and academics—for an exchange of views and thoughts.
- Questions addressed included: How do payments markets differ from other markets? How do consumer preferences affect industry outcomes? Are payments markets sufficiently competitive and safe? If not, what private and public policies would be beneficial? Should central bank policies to ensure smoothly functioning payments systems be adapted in light of the dynamic changes underway? More specifically, what role should central banks play as operators and overseers in the retail payments system of the future?"

Links to the papers and other presentations are available on conference Web site. Until the full conference summary and transcript are made available, we recommend to our readers that they start with a high-level summary of the discussions from the perspective of Bruce Summers.

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

DECEMBER 07, 2009

If nonbanks drive payment innovation, will banks pay for the risk management?

Nonbanks are driving significant investment in the retail payments space today, a healthy signal to the economy that contrasts starkly to some other economic sectors, and a sign that innovation in payments businesses and technologies is alive and well. This continuing and dynamic evolution is changing the retail payments landscape in new and unexpected ways, such that all industry stakeholders will need to consider risk issues in a new light as well.

What does this spell for the role of financial institutions as retail payments service providers going forward? More importantly, how will industry stakeholders ensure integrity in retail payments systems more generally?

Venture capital and M&A activity for nonbanks

The venture capital community has demonstrated a continued interest in payment technology start-up companies, particularly in the mobile information technology market. Investment banking firm Updata Advisors recently published research reporting that out of the 16 deals the firm tracked in the third quarter of 2009 in the financial technology sector, six fell into the payments subsector. Updata also reports that it believes that new payment technology providers "with their roots in social networking technology will be prime candidates for future acquisitions by larger merchants that do not want to spend on their own R&D."

2009 Payment Technology Transactions (in millions)

Date	Seller	Buyer	Enterprise Value	Target Description
12 Jun	HSBC Merchant Services 49% Interest	Global Payments, Inc.	$628	Provide payment processing services.
11 May	PayPassage, Inc.	Pipeline Data, Inc.	$4	Credit card processing solution offered to U.S. merchants in the retail, wholesale, mail/phone order, commercial and e-commerce space.
7 May	Custom House, Ltd.	Western Union Company	$370	Provider of business-to-business international payment solutions for small and medium enterprises (SME).
4 May	Commerciant, LP	BankServ	Not Disclosed	Provider of mobile, handheld payment processing hardware and technology.
21 Apr	Spare Change	PlaySpan	Not Disclosed	Micropayment solution on social networks whose platform enables buyers and sellers to transact safely easily and inexpensively.
15 Apr	National Merchants Solutions	Austin Ventures	Not Disclosed	Independent sales organization (ISO) operating in the payment industry.
30 Mar	Fifth Third Processing Solutions, LLC	Advent International	$2,350	Payment processing of Fifth Third Bancorp providing electronic funds transfer (EFT), debit, credit and merchant transaction processing.
18 Feb	Strategic Payment Services Pty Ltd	MasterCard Worldwide	Not Disclosed	Processing solution including transaction switching, device driving, back office and support functions.
11 Feb	Perpetual Payments	Voice Commerce Group	Not Disclosed	Specialist credit card and merchant services processing business.
10 Feb	FEXCO money transfer business	Western Union Company	Not Disclosed	Money transfer business.
5 Feb	Pipeline Data	ComVest Group	Not Disclosed	Provider of payment processing and services.
4 Feb	CB.Net	Accuity	Not Disclosed	Provides customers with sets of data for managing all aspects of straight-through electronic payment processing.
4 Feb	Optimal Payment Corp/ Card Present Division	Financial Transaction Services	Not Disclosed	Card present merchant processing division of Optimal Payment.
26 Jan	Payzone pic/stored value business assets	Branded Payment Solutions	Not Disclosed	Payzone pic/stored value business assets.
20 Jan	ChoicePay, Inc.	Tier Technologies, Inc.	$10	ePayments solution provider.
8 Jan	XiBuy	BizAps	Not Disclosed	Delivers a broad range of solutions for the procure-to-pay automation market.

Source: http://blog.updataadvisors.com/public/blog/236448

Continued on next page

Continued from previous page

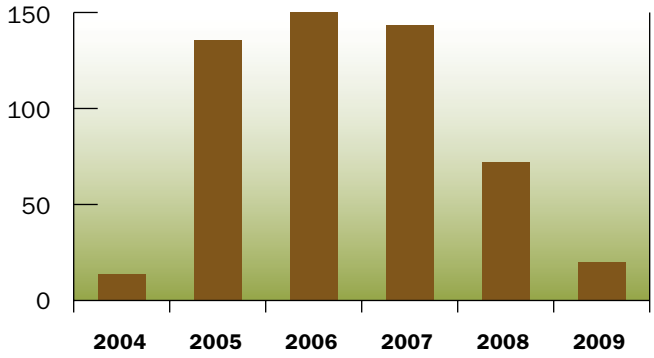
The migration from traditional to smart phones is helping drive these trends, with a number of venture capital funds investing in start-ups involved in developing smart phone applications (apps). Consider the $150 million BlackberryPartners Fund launched in 2008 by RIM, RBS, and Thomson Reuters to focus on mobile phone apps and services. Mpower Mobile, a firm that provides person-to-person (P2P) services and remittances, recently announced it had received a second round of investment to fund further technology developments such as debit and credit card functionality for mobile phones.

On the M&A front, Mint, a two-year-old, privately held personal finance service, agreed to be acquired by Intuit for $170 million in September 2009. Mint derived its revenue by directing subscribers to online financial products and services from participating institutions. Just this week, American Express announced it would acquire Revolution Money, a recently established alternative payment network, for $300 million.

Economic volatility may hinder banks' investment in payment technology

While tech firm investment in alternative payments is active and highly publicized, the same cannot be said of the banking sector. Established banks saddled with legacy payment system investments have had to balance new technology investment with existing costs while competing with de novo financial institutions.

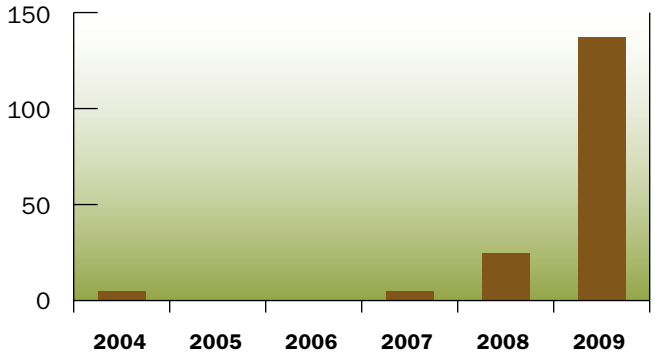
U.S. de Novo Charters by Year (Number of Institutions)



Source: SNL Interactive Financial

While new bank charters flourished at the economic peak years of 2005 and 2006, the following years witnessed the largest rash of bank failures in decades. According to the FDIC report of failed banks, more than 100 institutions have been closed in 2009 alone. The turmoil in the financial services sector suggests that prospects for significant bank investments in payment-related technology may be hindered for some time. This effect was described with regard to payments risk management investments in an earlier Portals and Rails post.

Failed U.S. Banks and Thrifts by Year



Source: FDIC

Will risk controls take a back seat to innovation?

The take-away from these environmentals is that nonbanks continue to drive technology investment opportunities, which in turn lead to the development of alternative forms of retail payments. The current economic environment may impede participation on behalf of the banking industry, where risk management and regulatory compliance are much more commonplace.

Within the telecom industry, by contrast, there are consortia worldwide discussing how to manage risk in mobile payments in a cross-border environment as bank-agnostic start-up firms provide new mobile remittance and money transfer services. If financial institutions are not part of that conversation on the front end, how will they address risk management and compliance issues with security and identity theft or money laundering? How will the solutions that arise from discussions on risk outside of financial institutions be implemented in a banking environment, and who will assume that responsibility?

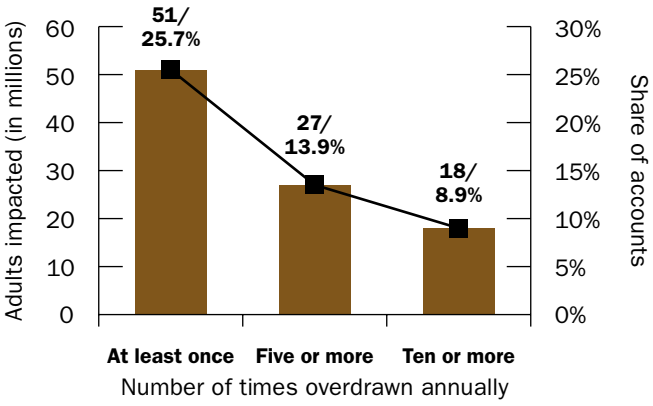
By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

DECEMBER 14, 2009

Consumer preference for opt-in guides Fed rule on overdraft protection

A recent report by the Center for Responsible Lending found that more than 50 million Americans overdrew their checking account at least once over a 12-month period, with 27 million accountholders incurring five or more overdrafts of nonsufficient funds (NSF) fees. The costs to consumers for overdrafts are significant, with many instances of fees exceeding the amount withdrawn. ATM and one-time debit card transactions have been a key driver behind the growth in the volume and cost of overdraft fees. Point-of-sale/debit overdraft transactions accounted for 41 percent of surveyed institutions' NSF transactions, according to an FDIC study. These POS/debit NSF transactions had a median dollar value of $20, while the median overdraft charge assessed by banks was $27.

Share of total checking accounts that become overdrawn during a year and total accountholders affected



Source: Center for Responsible Lending

To address high overdraft costs, last month the Federal Reserve Board issued a final rule amending Regulation E, which will provide greater consumer protection by limiting the fees financial institutions can charge consumers for paying overdrafts on ATM and most debit card transactions.

The new rule essentially eliminates a common practice by financial institutions of automatically enrolling consumers in overdraft services. In fact, the aforementioned FDIC study found that 75 percent of banks automatically enrolled customers in automated overdraft programs. Starting on July 1, 2010, financial institutions will have to provide a notice explaining its overdraft service and fees for ATM and one-time debit card transactions before the consumer can accept it. The rule includes a model form that institutions may use to satisfy the notice requirement.

Public comments and consumer testing help inform final revisions

The Board's final revisions to Regulation E were informed by comments received on its January 2009 Regulation E proposal and results of consumer testing. The Board received more than 20,700 comment letters (including 16,000 form letters) on its January 2009 proposal, the majority of which were submitted by individual consumers. In addition, the Board engaged a consultant to conduct consumer testing on a model disclosure notice that would effectively communicate information to consumers about how their overdrafts would be handled by the bank, what fees they could be potentially charged, and what choices they had related to overdrafts.

Consumer advocates, members of Congress, federal and state regulators, and the overwhelming majority of individual consumers who commented favored the opt-in provision because they felt that the harm to consumers from overdraft fees outweighed the benefits from permitting the payment of ATM and debit card overdrafts. In contrast, the majority of industry commenters contended that the opt-out approach was better because it provided consumers with the benefits of overdraft services with fewer disruptions to the consumer and bank operations.

In the end the Board determined that an opt-in approach to permitting overdrafts was the best decision for consumers. This decision was based partly on the Board's consumer testing, which indicated that consumers prefer to have transactions declined than incur fees for overdrafts.

Certain types of transactions not covered by the rule

Other types of transactions are not covered by the rule, including withdrawal by check, ACH, and recurring debit. The Board determined that with respect to checks, the payment of overdrafts may be preferable to having the check returned for NSF and paying the return fees charged by the bank and merchant. In addition, participants in the Board's consumer testing generally indicated that they were more likely to pay important bills using checks, ACH, and recurring debits. Debit cards were primarily used on a one-time basis for discretionary purchases.

Continued on next page

DECEMBER 14, 2009

Continued from previous page

Opting in is not requirement for other services
Consumers who do not accept an institution's overdraft service cannot be treated differently than those who opt in. For example, institutions are prohibited from declining payment of overdrafts of other types of transactions (e.g., checks and ACH) because the consumer did not opt in to that institution's overdraft service for ATM and one-time debit card transactions. The institutions are also required to provide those customers with the same account terms, conditions, and features that they provide to consumers who do elect to take the service.

Overdraft fee income for banks and credit unions rose 35 percent in the last two years. Although not a panacea, the Board's overdraft rules provide greater protection for consumers in navigating their personal finances. Ultimately, an informed consumer is the best consumer protection.

By Jennifer Grier, senior payments risk analyst in the Retail Payments Risk Forum at the Atlanta Fed

DECEMBER 21, 2009

"Money mules" carry load for global cybercriminals

In November, Portals and Rails explored the industry implications of hacking attacks that have resulted in fraudulent funds transfers using online banking interfaces. This week, Portals and Rails revisits this topic, focusing on the tactics these fraudsters use to dupe unsuspecting individuals and organizations.

The FDIC released a special alert on October 29, warning financial institutions of an uptick in schemes to recruit individuals to receive and transmit unauthorized electronic funds transfers (EFTs) from deposit accounts to individuals overseas. These funds transfer agents, also referred to as "money mules," are solicited online by criminals who have gained unauthorized access to the account of a business or consumer. Typically, the criminal will originate unauthorized EFTs from the victim's account to the money mule's deposit account. The money mule is then instructed to quickly withdraw the cash and wire it overseas minus a "commission" of from 8 to 10 percent.

Fraudsters perpetrate work-at-home scams using online job postings and social networking sites
A common hiring tactic for money mules are work-at-home

jobs or other seemingly legitimate positions. Fraudsters will use online job search Web sites and social networking sites to persuade individuals to receive and forward stolen funds. According to the Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA), victims are often hired to "process payments," "transfer funds," or "reship products." Other victims sign up to be "mystery shoppers" where they receive fraudulent checks with instructions to cash the checks and wire the funds to "test" the performance of a money service business.

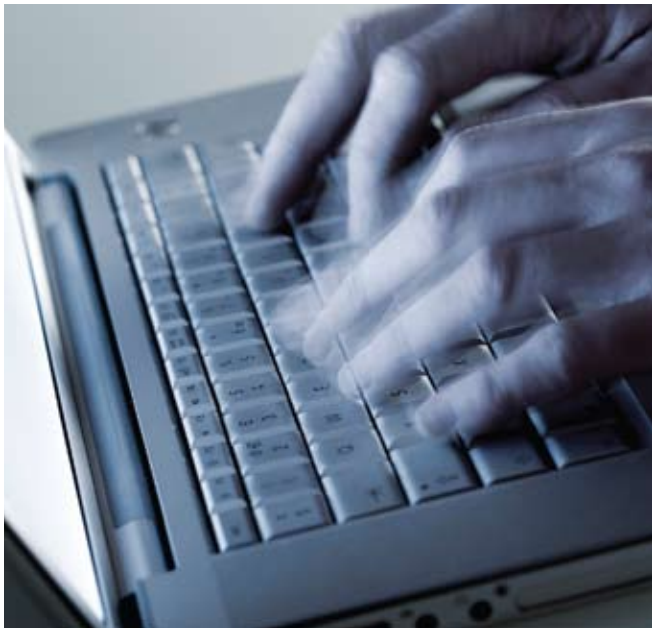
The job scams also provide the criminal an opportunity to commit identity theft against the money mule. The personal information provided on the "employment" application (e.g., Social Security number or bank account information) may be used to open credit cards, post online auctions, etc., in the money mule's name and possibly commit additional crimes.

Sophisticated fraudsters use malicious code and money mules to conduct unauthorized funds transfers

An FBI alert issued last month describes how fraudsters are increasingly using malicious code to conduct unauthorized ACH transfers with the help of money mules. Many of these cases involve exploiting the online banking credentials belonging to small and midsized businesses, municipal governments, and school districts.

A typical scenario involves a "spear phishing" e-mail being sent to someone within the company with either an infected attachment or directing the recipient to an infected website. Spear phishing is a phishing attack that targets a specific person and deceptively appears to come from an individual or organization that the potential victim would normally receive e-mails from. The email recipient would usually have authorization to make funds transfers on behalf of the company.

Once the recipient opened the attachment or visited the Web site, malware (malicious software code) containing a key logger would be installed on the recipient's computer. The key logger captures the keystrokes of the recipient's business or corporate bank account login information. Once this information is compromised, the perpetrator either creates another user account with the stolen login or directly initiates funds transfers through either ACH or wire transfer by assuming the legitimate user's identity. The transactions are typically in increments less than $10,000 to avoid currency transaction reporting. Money mules play an important role in these schemes by helping to facilitate the unauthorized transfer of funds.



Small and midsized businesses lose millions to online banking scams

Reportedly, small to midsized businesses in the United States have lost $40 million to online banking fraud since 2004. FBI analysis has found that the main threat from these schemes is not merely the malware but the vulnerabilities presented by the lack of controls at the financial institution or third-party provider. In most cases, the victims' accounts were held at local community banks and credit unions, some of which used third-party service providers to process ACH transactions.

Many believe that the uptick in these types of fraudulent payment activities directly relate to the decline in the economy. Consequently, financial institutions, businesses, and consumers have to be vigilant in looking for signs of this activity. The Federal Financial Institutions Examinations Council (FFIEC) provides guidance to financial institutions and technology service providers on authentication in an Internet banking environment. Money mule activity in particular is addressed by the Bank Secrecy Act and Anti-Money Laundering regulations. There are also resources available to consumers and businesses on how to protect themselves from these types of online scams.

By Jennifer Grier, senior payments risk analyst in the Retail Payments Risk Forum at the Atlanta Fed

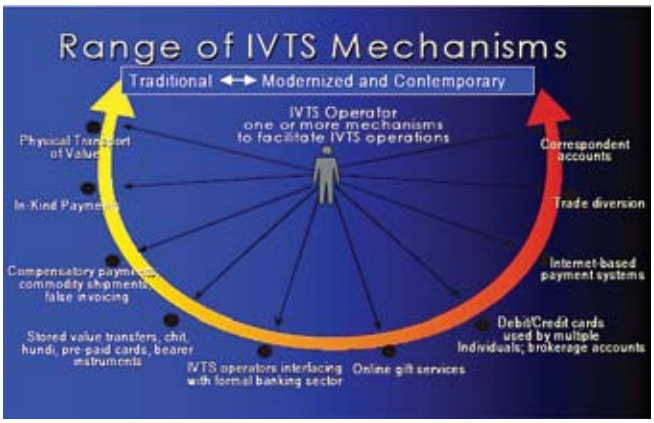
DECEMBER 28, 2009

Mobile money transfers: Benign P2P or hawala money?

Informal value transfer systems (IVTS) such as traditional trade and barter have existed since the beginning of time and still serve legitimate purposes today. While informal payments may provide benefits such as improved reliability and convenience to users over formal systems, they may also create regulatory and risk management challenges. Person-to-person (P2P) payments via the mobile phone, also known as mobile money transfers (MMT), represent an innovation with the potential for use in informal channels as nonbanks, many of which are start-up firms, extend services in a cross-border enviroment.

IVTS were defined by Nikos Passas to describe "any network or mechanism that can be used to transfer funds or value from place to place either without leaving a formal paper trail of the entire transaction or without going through regulated financial institutions." One of those systems is hawala, which has its origins in classical Islamic law and is mentioned in texts of Islamic jurisprudence as early as the eighth century. Hawala drew interest from the U.S. government after 9/11 because payments are exchanged on the honor system without a paper trail. With this arrangement, it could be difficult to determine if a transfer of funds was for legitimate purposes.

In addition to hawala, Passas identified other important IVTS to include gift and money transfer services via Internet sites, Internet-based payments and transfers, and stored value cards, such as prepaid telephone cards, to name a few. IVTS systems and mechanisms range from basic and traditional exchanges to modern and sophisticated ones.



Source: Nikos Passas IVTS World Bank presentation

Passas' initial work predated the recent developments in the mobile payments channel and certainly came before the growth in mobile enabled P2P and the use of prepaid airtime for remittances, as described in an earlier edition of Portals and Rails. When P2P payments are conducted by mobile carriers in a bank-agnostic ecosystem, do they potentially represent a more sophisticated, modern-day informal payment system?

MMT: The fastest-growing mobile payment

P2P payments represent possibly the fastest form of financial transaction enabled by mobile phones, driven by the steady growth in remittance markets, the ubiquity of cell phones themselves, and the desirability for an electronic P2P payment alternative in developed countries like the United States. Research firm Gartner recently identified mobile money transfer as the first of the top 10 consumer mobile applications in 2012, made possible by developments in smart handsets like the iPhone. Separately, ABI research predicts that almost three times as many consumers worldwide will use mobile phones to conduct P2P payments than those who will use them to conduct mobile banking functions by the end of 2011.

Formal versus informal

GSMA (Global System Mobile Association), the alliance of mobile network operators, launched the Mobile Money Transfer Programme initiative to promote the mobile channel and formalize international remittances. With low barriers to entry, roaming capacity, and a growing unbanked market in developed countries, start-up firms may offer informal MMT services, including international and domestic P2P in cross-border markets to expand their customer reach and network opportunities. While informal payment systems can provide means for legal transactions, the lack of transparency could potentially provide bad actors the opportunity for money laundering and other financial crimes.

Nonbanks, like telecom firms and others, are rapidly entering the financial services arena, creating an uncertain regulatory environment as laws and regulations vary from country to country. Will mobile P2P innovation permit service offerings that are characterized as informal payments with the potential for misconduct? Will violators of money-laundering laws go undetected as stored-value mechanisms move from the plastic card to the mobile device? These questions will no doubt be the focus for regulators in many markets going forward as they attempt to understand both the operational and regulatory risks money transfer services have the potential to introduce.

By Cindy Merritt, assistant director of the Retail Payments Risk Forum at the Atlanta Fed

STAFF AND ADVISORS

The Retail Payments Risk Forum works with financial institutions and industry participants, regulators and law enforcement officials to research issues and sponsor dialogue to help promote the mitigation of risks in retail payments, with a focus on check and automated clearinghouse transactions.

Staff

Richard R. Oliver
Executive Vice President
Richard.Oliver@atl.frb.org

Clifford S. Stanford
Assistant Vice President
Clifford.S.Stanford@atl.frb.org

Cynthia D. Merritt
Assistant Director
Cynthia.Merritt@atl.frb.org

Crystal Carroll
Senior Payments Risk Analyst
Crystal.Carroll@atl.frb.org

Jennifer R. Grier
Senior Payments Risk Analyst
Jennifer.Grier@atl.frb.org

Ana Cavazos-Wright
Payments Risk Analyst
Ana.Cavazos-Wright@atl.frb.org

Advisory Group

FEDERAL
RESERVE
BANK
of ATLANTA