POLICY STUDIES

Network Vulnerabilities and Risks in the Retail Payment System

Catharine Lemieux

Emerging Payments Occasional Papers Series
2003-1F

FEDERAL RESERVE BANK
OF CHICAGO

Network Vulnerabilities and Risks
In the Retail Payment System

Catharine Lemieux

Abstract

Changes in retail payments technology will impact the operational risk of commercial banks. This study provides a more in-depth discussion of the ramifications these changes have for bank supervision and policy makers. In addition to operational risk concerns identified by previous researchers, this paper identifies network vulnerabilities as a potential resiliency concern.

Vice President, Federal Reserve Bank of Chicago, catharine.m.lemieux@chi.frb.org. The author is indebted to Ed Green for guidance and Elizabeth Knospe, Katherine Schrepfer and Angela Wu for the review of laws and regulations. Thanks also to Tara Rice, Paul Kellogg, Margaret Beutel, Steve Vanbever and Bob Chakravorti for helpful comments. The views expressed here are those of the author and do not represent those of the Federal Reserve Bank of Chicago or the Board of Governors of the Federal Reserve System.

Policy Implications of Trends in Payments Technology

Increasingly, nonbanks are major players in the payments system. While payments must ultimately flow through a bank for final settlement, increasingly, value-added payment services are being provided by nonbanks. Chakravorti and Kobor (2003) discuss some of the drivers behind bank and nonbank investment in this financial service. Yet, a core reason for the regulation of the safety and soundness of individual insured depository institutions is the impact they have on the payments system and the functioning of commercial markets [Goodfriend (1989), Flannery (1998), Herring and Santomero (1999)]. While most retail payments ultimately involve the transfer of funds from one bank account to another, along the way payments information may flow through many networks. As nonbanks become increasingly important in the operation of these networks, existing bank regulation has less ability to assure the smooth functioning of these systems.

Recent studies have investigated the risks associated with new retail payments system technologies and found few systemic concerns (Bradford, Davies and Winer, 2002; Meister, 2000; Bank of England, 2000; McAndrews, 1999; Kuttner and McAndrews, 2001; and Roberds, 1998). Identified risks include concentration of third party providers, fraud, interdependencies, and risk of system failure. Similar issues are identified by Kellogg (2003) in his analysis of the impact new payment technologies are having on bank operational risk. Generally, the impact of these risks on the payments system is judged to be small due to modest transaction volume. However, recent events discussed below, highlight how vulnerabilities in networks can disrupt markets. The

degree to which these risks rise to systemic proportions is a debatable question. However, the objective of this paper is to begin a discussion on the appropriate level of oversight needed to ensure the smooth functioning of the payment system.

In the introduction two criteria were proposed for use in classifying a risk as systemic: contagion and the degree of loss. "Contagion" refers to the fact that the risk is easily transmitted through the financial system. "Degree of loss" refers to the fact that the loss due to risk must be sufficiently large in relation to the institution's capital. If both these criteria are met, then the risk meets the definition of systemic. The necessity of regulating systemic risks is not questioned; but there are risks that fall short of meeting the definition of systemic risk, and some argue, warrant regulatory oversight. Resiliency may be one such risk. This refers to risks that can limit the smooth functioning of the flow of funds on the economy. A risk meets this criterion if it is large relative to any individual bank and highly correlated among banks. For resiliency to be a concern, the risk must have the potential to impact the soundness of the institution or to harm consumers.

Concerns that do not meet these tests may create risk sufficient enough to warrant regulation at the individual insured institution level. These risks focus on limiting moral hazard incentives of individual bank managers. Because banks are opaque institutions, regulation is needed to ensure their safe and sound operation. Finally, banks are also subject to regulations that ensure fair and equal access to banking services. Yet, the degree of supervision must be balanced against the risk.

Building on the findings of the four studies in this series, this paper presents some thoughts on the risks posed by the trend in payments technology innovations. The

discussion below provides relevant examples based on recent events that present serious risks which deserve further research to identify mitigations that are appropriate to the degree of risk they represent.

Network Vulnerabilities

Network vulnerabilities refer to the possibility of unauthorized access to payments-related systems that could lead to a disruption in the flow of funds and compromise information associated with the payments process. Kellogg (2003) identified some of the issues associated with vulnerabilities. These include the impact of changing delivery channels on internal controls, fraud and vendor oversight. Recent payments innovations that focus on expanding access to delivery channels (Chakravorti and Kobor, 2003) and the rapid growth in the importance of the Internet in the payments process accentuate these risks. Traditional retail payment systems were paper-based, so there was always a physical document for payment authorization. Paper-based payments systems were conducted in closed systems where only "approved" parties had access to the flow of information and funds. Today open systems provide opportunities for anyone to participate in a payments network. In addition, Kellogg (2003), as well as Rice and Stanton (2003), and Chakravorti and Kobor, (2003) all found evidence that banks' ability to identify, measure, monitor and control aggregate risk from different payment channels is limited.

While network vulnerabilities clearly represent a significant risk to individual institutions, they may have broader implications. The introduction laid out three criteria for a risk to have systemic implications, contagion, degree of loss and resiliency. The relationship of network vulnerabilities to each of these criteria is discussed below.

Contagion

Increasing payments-system participation by nonbanks in a variety of arrangements (detailed in Bradford, Davies and Winer, 2002) creates linkages to diverse entities that may not maintain the same level of information system security banks are required to maintain. These linkages may come from outsourcers, joint ventures, partnership arrangements, equity investments in other firms or even bank customers. Demand for payments technology is driving many of these linkages, as consumers and businesses demand real-time access to their accounts and the ability to pay bills online. Economies of scale and scope incent consolidation in back-end processing and technology infrastructure, making all clients of the processor dependent on the vendor's information security practices and procedures. Banks could be at risk for security breaches, fraud and criminal activity as a result of these connections.

Two incidents in the first two months of 2003 illustrate this risk. The last weekend in January, 2003, Bank of America was the target of a virus that knocked out its entire ATM network. The virus exploited a known vulnerability in Microsoft SQL Server 2000. Even though the impact was limited because other companies had installed the Microsoft patch to correct the problem (O'Harrow and Cha, 2003) the virus did manage to shut down the 911 system for the city of Seattle, disrupt airline reservations at Continental Airlines and infect the Microsoft campus. At issue is the potential for a future virus to exploit an unknown vulnerability for which no patch may be available and knock out even more widespread and essential networks.

The second incident occurred in February, 2003. A hacker gained access to over 10 million credit card account numbers through an independent sales organization (ISO)

that acted as a third party consolidator of merchant accounts for Provident Bank of Cincinnati. The ISO handled sales and servicing transactions for merchants primarily engaged in catalog sales. ISOs are neither acquirers nor processors and must register with Visa and MasterCard but do not have to comply with the membership criteria imposed on banks that belong to the Visa or MasterCard network. Provident's chief credit and risk officer, Jim Gertie, said, "Just in the last year we've tightened this whole process up, but our ability to have detected a breach at a service provider like this would have been small. You're always playing catch up with Internet security" (Kuykendall and Lee, 2003). These two examples highlight how distant affiliates can impact information security.

These examples also give an indication of how far and how rapidly these attacks can spread. Few would dispute that network vulnerabilities have the potential to move quickly throughout the financial system. The worm responsible for shutting down Bank of America's ATMs circled the globe in 10 minutes and infected both financial and commercial businesses. As vendors that service banks increasingly market their services to insurance companies, brokerage firms and even nonfinancial firms, the likelihood of network vulnerabilities impacting multiple sectors increases.

Concentration of vendors that control access to specific payments channels is another factor impacting contagion. Credit cards and ATMs are two examples. Visa alone has over 14,000 insured depository institutions as clients, and Pulse, NYCE and Star combined have over 12,200 insured depository institutions as clients for their ATM

networks.[1,2] Any weakness in their operating systems would impact a substantial portion of the financial sector.

Similarly, one could view the breakdown in the payments system as a result of the terrorist attack of 9/11/2001 in New York City as a systemic vulnerability due to a different type of concentration. One of the problems in resuming normal operations identified by the GAO (February, 2003) was the number of financial organizations whose telecommunications service was affected by the damage to the Verizon central switching office at 140 West Street. This central office handled voice, data and Internet communications for lower Manhattan and created a single point of failure. Even some firms that had contracted for diverse and redundant network services found unexpectedly that their back-up telecommunications vendor used the same telecommunications lines as their primary vendor. Other firms that had mapped out their communications lines to ensure they used diverse paths found that their service providers had rerouted some of the lines over time without the firm's knowledge. While these events did not cause a financial institution to fail, they did disrupt transactions in the stock, options, money-market, and government securities markets, ultimately requiring Federal Reserve intervention.

The payments system increasingly relies on open networks like the Internet to transmit payments data. While 9/11 did not specifically impact retail payments systems, it is not unreasonable to compare the impact of a single point of failure relating to a telecommunications switch to the impact of a failure of a key payments system processor.

[1] FDIC reports that there were 7,887 commercial banks and 1,467 savings institutions at year-end 2002. NCUA reports that there were 9,984 federally insured credit unions at year-end 2002.
[2] First Data Corporation, which owns NYCE ATM network recently announced that it will acquire Concord EFS, Inc., the owner of the rival network, STAR.

While the situation discussed above was certainly more complicated than just the failure of the central switching office, it does provide insights into how bottlenecks in the flow of information can disrupt the economy. The increasing interconnectedness of retail payments networks increases the likelihood that failure of any single point in the network could cause bottlenecks in the flow of information, slowing the retail economy.

Degree of Loss

Few losses from external network vulnerabilities have been large enough to threaten the financial soundness of a financial institution.[3] Vice Chairman, Roger Ferguson, described Federal Reserve actions in response to September 11 in a speech given on May 9, 2002 in Chicago. "We bought a record number of repurchase agreements, injecting approximately $81 billion into the government securities markets. We also loaned approximately $46 billion from the discount window – typical levels are around $100 million. And, to address the collateral needs of foreign financial institutions doing business in the United States and to meet the demand for dollars abroad, we executed a series of agreements to do currency swaps, if needed, with the European Central Bank, the Bank of England, and the Bank of Canada, totaling $90 billion." While the cost of this liquidity is considerably less than these notional amounts, it does demonstrate the potential financial impact of a payment system disruption. Although this was a disruption in wholesale payments, the coordination issues have some relevance for retail payments systems also. McAndrews and Potter (2002) identify incoming funds as a source of liquidity for payments. While a disruption in wholesale payments creates greater strains on liquidity than a disruption in retail payments, the increasing access to

[3] The Office of Inspector General's report on the failure of Oakwood in Ohio identified payments fraud perpetrated by insiders as the reason for the bank to fail on February, 2002.

retail payments systems spurred by payments innovations can cause disruptions in payments coordination. A greater understanding of the potential for a disruption in retail payments coordination is needed before the systemic implications of this risk can be assessed and the appropriate mitigations identified.

Regarding the Microsoft virus that infected Bank of America, estimates of the cost to all businesses in the U.S. (the large majority of which were presumably "infected" through channels unrelated to the B of A or the banking system) are in the neighborhood of $1 billion. If the virus had been harder to contain and fewer industries had been protected, the costs could have likely been much greater.[4] The costs of identity theft associated with the 10 million credit card numbers are more difficult to quantify. For example, the risk that these stolen numbers will lead to identity theft will remain elevated for several years (Siegel-Bernard and Richmond, 2003). The cost of identity theft can be considerable. Costs to consumers include time spent straightening out the problem; out-of-pocket expenses related to finding out the extent of the problem and notifying creditors and credit reporting agencies; charges for purchases up to the legal or individual company's limits; and for some, the cost of being the subject of a criminal investigation.[5] Costs to merchants partially depend on the mode of payment. The merchant is liable for fraudulent purchases. For credit card purchases over $50 or debit card purchases over $50 or $500 (depending on the time elapsed in reporting the crime) card issuers are liable. For purchases paid for by checks, the merchant is liable. The cost to banks includes

[4] CNET News.com reports that the virus was eliminated by shutting down the infected servers and restarting the computer system (Lemos, 2003).

[5] The GAO (March, 2002) reported that victims of identity theft spent an average of 175 hours straightening out the problem and incur approximately $100 of out-of-pocket expenses. Of the 94,100 identity theft complaints received by the FTC in the 23-month period from November, 1999 through September, 2001, 203 lost more than $5,000 and 1,300 of the victims were subjected to criminal investigations, arrests or convictions.

heightened reputational and legal risk. In the incident cited above two banks elected to reissue affected credit cards at an estimated cost of $100 per card. If a significant number of the stolen credit card numbers lead to identity theft, it could represent a substantial cost to all of these groups. As these examples illustrate, the costs fall on a host of firms and consumers and extend beyond banks.

In these examples of contagion, size of the institution is not an indication of the level of risk exposure for the financial system. Due to the contagious nature of technological vulnerabilities and the interdependencies of system participants, the weakest link in the system can create some exposure to risk across a wide part of the financial system.

Resiliency

An additional rationale for regulation as discussed in the introduction is resiliency. Consolidation may increase the correlation of risk, as processes that were previously performed by numerous separate entities are now performed by fewer entities. Consolidation of payments processing in conjunction with banking consolidation may be an issue that meets this criterion. Currently when the largest banks[6] invite bids for systems processing they talk to approximately four large vendors and a few specialized firms (Gillis, 2002). Owing to their size and expertise, these same vendors also support other financial services firms specializing in insurance, brokerage, and payments for clients based in the U.S. and abroad. One example of the span of current outsourcing arrangements is the $5 billion contract IBM signed with JP Morgan Chase in December, 2002. IBM agreed to consolidate the data processing technology

[6] According to Y-9 reports, the 10 largest bank holding companies in the U.S. hold over half of the banking assets and approximately 45 percent of the deposits at all U.S. commercial banks.

infrastructure in more than 50 countries over seven years. Also in 2002, IBM signed large contracts with American Express and Deutsche Bank. It is easy to imagine how a vendor could gain significant control over the payment systems of several countries. The risk is that lack of performance by a single vendor could impact the functioning of multiple payment systems.

The international component of outsourcing is another increasing risk. Not only are the same service providers selling their processing technology around the globe, but they also are often linking US firms to vendors in other countries like India and the Philippines. Business Week (2003) predicts that within three years, 30 percent of large US companies will outsource programming related IT services and manage certain business processes through offshore vendors. In a KPMG survey of 800 Indian companies, 78 percent of respondents said their organizations had not recently evaluated the controls in relation to the risks they face (Boettger, 2002). The joint consolidation of service providers and banks, the international links between the many clients located in diverse countries with one service provider, and the use of firms in foreign locations with weaker internal controls to perform outsourced functions present potential risks to the resiliency of the US financial system.

On the other hand, there are several reasons why this risk may not impact system resiliency at this time. First, the consolidation among IT vendors is currently not to the point of impeding competition. Many large banking organizations deal with multiple IT vendors for different services, and there are multiple vendors providing similar services. Similar arguments can be made regarding concentration in retail payment networks. There are alternatives to making payments with credit cards and accessing cash through

ATMs. Failures in either network would represent a major inconvenience for consumers and could impact the cash flow of some firms, but the overall stress on the US payment system would be manageable.

Second, customer demand for technology solutions can be a significant incentive for vendors to focus on these concerns. Third, security technology like intrusion detection systems and firewalls, when used rigorously, can mitigate system vulnerabilities. Finally, reputational and legal risk provide additional incentives for vendors to self-regulate. For example, antitrust laws provide a vehicle for injured parties to address concerns.[7] All of these reasons mitigate resiliency concerns.

By identifying network vulnerabilities heightened by trends in technology adoption and outsourcing, we can better focus on appropriate regulatory policies to contain the risk. The following arguments point to classifying network vulnerabilities as a systemic risk:

1. Network vulnerabilities are susceptible to highly contagious forms of attack;
2. Single points of failure are difficult to find and to mitigate;
3. Losses have the potential to impact the financial system and move beyond the payments networks to other infrastructure components; and
4. Costs to resolve problems can escalate quickly and are born by financial and commercial firms as well as consumers.

[7] Wal-Mart, Sears Roebuck, Circuit City and other merchants sued Visa and MasterCard claiming they were forced to accept Visa and Mastercard online debit cards if they were going to accept their credit cards. As part of the recent settlement stores will no longer have to accept Visa and MasterCard debit cards if they want to accept their credit cards (Bayot, 2003).

If these arguments are convincing, then an argument could be made for further extending regulation to cover nonbank participants in the payment system. On the other hand, the network vulnerabilities could be containable if:

1. There are sufficient participants in the payments processing market to provide back-up in the event of disruptions;
2. Single points of failure can be found and eliminated;
3. Losses do not threaten the viability of a financial institution, the financial sector or the real economy; and
4. Network vulnerabilities are mitigated through redundancy, scalability, stress testing, use of firewalls and other proactive lines of defense.

If one believes that network vulnerabilities constitute a systemic risk, then there is a rationale for extending bank-like regulation to affiliated parties. Many payment system regulations already apply to nonbank payment system participants. The Appendix details key regulations and their applicability to nonbanks.[8] However, even when the legal and regulatory frameworks are synchronized, the enforcement regime may differ by organization.[9] Differences in the focus on proactive detection and enforcement can cause differences in compliance.

If, on the other hand, one believes that network vulnerabilities are containable, then appropriate regulation would focus on bank network security. However, as trends in retail payments continue the analysis should be revisited. Key issues that should be

[8] The Appendix lists laws and regulations that apply to different payment options and different payment providers emphasizing the differing legal frameworks.

[9] For example, the federal banking agencies employ over 800 compliance examiners whose job it is to determine banks' compliance with consumer protection laws and regulations. In contrast, the Federal Trade Commission, the agency responsible for enforcing federal consumer protection laws and regulations at non-banking companies, employs 55 people who are responsible for investigating complaints relating to compliance with consumer laws and regulations.

monitored include: market share by channel for banks and nonbanks, effectiveness of security technology, scenarios used in stress testing, redundancy and scalability in systems, degree of exposure to other countries, and network security of key vendors. BIS (March, 2003) identified monitoring developments in security standards, operating standards and infrastructure (outsourcing) arrangements for important retail payment systems as another minimum recommended action for Central Banks in regards to retail payment systems oversight.

Mitigation

Bank regulation relies on four primary tools: chartering requirements, capital regulation, supervision and disclosure. Each of these is discussed below in relation to the risks associated with network vulnerabilities.

Chartering

In the last decade most of the geographical and product restrictions applicable to the banking industry have been eased. However, finality in the settlement process is still a unique service offered by insured depository institutions.[10] Many payments innovations separate the flow of funds from the flow of information. There are no restrictions on who can participate in the transfer of payments related information. If the risks associated with network vulnerabilities are considered to be systemic, chartering regulations could be applied to all payments system participants. Short of regulating all participants in the payments process, standards relating to the content and format of payments information

[10] The FDIC considers the following seven factors before granting deposit insurance to a bank: financial history and condition of the bank, adequacy of the bank's capital structure, earnings prospects of the bank, general character and fitness of the bank's management, risk the institution presents to the bank insurance fund, convenience and needs of the community to be served, and consistency of the institution's corporate powers with the purposes of the Federal Deposit Insurance Act.

would ease the burden of review and mitigate some of the current difficulties identified by the industry such as researching processing errors with electronic payments and fraud.

Capital Regulation

Historically, capital regulations have only required capital support for assets held on the balance sheet. However, with the 1996 amendment, capital support was required for capital markets activities. The proposed modifications to the Basel Accord call for factoring risks from payment systems into calculations for determining the appropriate amount of capital an insured institution should hold. While it is likely that the modifications will only apply in the U.S. to the largest, internationally active banking organizations, it is a sound practice for all banks to be able to measure, monitor, manage and mitigate risks from these activities. If the unexpected losses from this activity are deemed significant, supervisors could consider making the link between network vulnerabilities and appropriate level of capital more straightforward independent of the implementation of the modifications to the Basel Accord.

Supervision

There are two ways to address the issues raised regarding network vulnerabilities, regulate all payment system participants or focus on making sure banks are protected from these risks. Currently, there are supervisory programs that attempt to do a little of both. Large data processors are subject to on-site examination of their operations. Bank supervision aimed at reducing network vulnerabilities includes requirements that banks verify the security safeguards of their vendors, periodic on-site reviews of IT security and sound practice expectations regarding operational risk management. Each of these is discussed below along with potential enhancements.

Multi-Regional Data Processing Service Providers (MDPS)[11] reviews currently involve, to some extent, the largest vendors providing payments services. Data are collected on the number of clients and business lines supported. These data need to be monitored on an ongoing basis for broader systemic implications. The Bank for International Settlements (BIS) Committee on Payment and Settlement Systems (March, 2003) identifies monitoring as a minimum recommended action for Central Banks in regards to retail payment systems. This is based on the premise that an important role for Central Banks in retail payments systems is to ensure that these markets are competitive or contestable. To do this the BIS Subcommittee recommends that Central Banks monitor information on market structures and conditions; composition of the market at various levels and in various market segments; operation of network effects; access restrictions; information asymmetries; and prices and costs.

Supervisory guidance requires banks to verify that their service providers have effective security safeguards. Banks are required to have procedures in place to perform necessary due diligence regarding their customers. Finally, banks are required to stress test their own systems for vulnerabilities. However, Kellogg (2003) finds that smaller banks are concerned that they do not have the knowledge to adequately monitor large service providers' data security or the leverage to effect change if vulnerabilities are discovered. This calls into question small banks' ability to comply with these regulations. Expecting banks to be the primary defense against system intruders may be unrealistic. BIS (March, 2003) notes the possibility of a dominant player disregarding the needs of smaller market participants when it comes to fundamental features of a payment

[11] MDPS reviews are discussed in greater detail in Kellogg (2003).

system (e.g., standards, technology or pricing policies) to the detriment of efficiency and safety. BIS identifies this as one reason Central Banks should play a role in developing policies to support effective standards and infrastructure arrangements.

Kellogg (2003) provides an overview of on-site IT reviews. Today, most supervisory reviews including IT reviews are risk-focused, meaning that the examination is structured to focus on key risks. Increased scrutiny is warranted when significant issues are detected. As part of this process, procedures already call for assessing the vulnerability of banks to network attacks and reviewing risk controls. Emphasis should be placed on the importance of this assessment, and specific guidance should be issued on when an assessment should be stepped up and when it could be stepped down. Greater awareness is needed on the part of examiners and the industry about the risks posed to banks from vendors, clients, and affiliates.

As part of these on-site reviews examiners can identify mitigations that would limit the banks' exposure to network vulnerabilities like stress testing and the use of firewalls. Redundancy (multiple pathways) and scalability (excess capacity) have also been identified as ways to mitigate the impact of contagion. There are few incentives for any individual payments system participant to build scalability and redundancy into their payments business because they add costs that are difficult to translate into increased revenue. Also, as part of a network, all participants must adopt controls (in this case building multiple pathways and excess capacity) or else the weakest link will disrupt network operations. For compliance purposes, this would provide a role for either an oversight body or an industry consortium.

Another area that supervision could address is encouraging aggregation of risk measurement. Supervisors must make an independent assessment of the risk in significant business lines of the organization. Additionally, supervisors must review and concur with banks' estimates of the capital needed to cover the risk of their activities. If risks in the payments line of business are not properly measured, bank supervisors can require the institution to hold additional capital to cover the risk, can ask bank management to voluntarily correct problems, or can issue legal sanctions against the bank for failure to comply with supervisory requests.

The above discussion has centered on the implementation of existing laws and regulations. But what if changes in technology make the rules ineffective? The difference in rules governing returns for ACH transactions and check transactions is one issue identified by bankers in Kellogg's (2003) survey and by corporate treasurers. The 60-day return period for ACH transactions no longer makes sense when businesses are using ACH transactions to substitute for checks. Regulations give banks two days to accept or reject payment of a consumer check. Yet banks have up to sixty days to reject an ACH transaction. This extended window for finalizing payments means the resolution of ACH problems is more difficult. BIS noted that arrangements for confidentiality, authentication, integrity, authorization and non-repudiability and other security arrangements should be reviewed to make sure they are adequate with changing technologies. One alternative is writing rules for each new technology or channel delivery that develops. The downside to this solution is that rules can stifle innovation or possibly create loopholes that provide opportunity for regulatory arbitrage. A better, but more difficult choice, would be to identify those core issues that should apply to any

retail payments channel and write rules that could withstand the test of time. Identification of the core issues is beyond the scope of this paper, but some issues that should be considered are synchronizing regulations on returns, funds availability and liability, fraud protections, and protection of consumer data.

Disclosure

Requiring release of information to the public provides them with sufficient information to make informed choices. In this way market forces can encourage desired outcomes such as appropriate security measures around consumers' financial information. Two groups have been identified that could benefit from increased disclosure, bank customers and banks.

An issue for bank customers is that they are often unaware of the difference in risk and rules governing the different payment channels. For example, few consumers are aware of the potential difference in their liability for fraudulent credit and debit card transactions that are not reported within two days. Kellogg (2003) finds that bankers are concerned that business customers are unaware of the differences in fraud controls as they migrate from check to ACH or Internet-based payments. In these cases fine print disclosures may not be enough. More active efforts to educate customers may be needed.

As for banks, they could benefit from increased disclosure about vendor security. This knowledge would help them make informed choices regarding the selection of the appropriate outsourcer. Also, if vendors are required to disclose information about their network security practices it may encourage them to adopt sound practices. However, there is a downside that disclosing security policies and procedures would play into the hands of criminals. Currently, many vendors provide clients with copies of audits.

Requiring a SAS 70 (type 2) audit, an in-depth assessment conducted by an independent IT auditor, may be appropriate both as part of the client's due diligence in vendor selection and as part of ongoing monitoring.

Supervisory MDPS reviews, described in Kellogg (2003), are another source of information for banks, but findings are only disclosed to banks that are already customers of the data processor. These reviews should increase data processors' attention to security. A wider distribution of the findings of these reviews would provide an additional incentive for these service providers to strengthen system controls. One way to do this is to make MDPS ratings of the largest firms subject to public disclosure. However, some of the same reasons other bank ratings are not disclosed may be problems here as well. These include legal liability that may accrue to examiners; potential for disclosure of unsatisfactory ratings to cause a rapid exodus from relationships with the affected firm, leading to network disruptions; or disclosures of vulnerabilities that could attract criminals.[12] Although the upshot of regulating large service providers might be to discourage those providers from being large (so that they escape regulation), that could limit the very industry concentration that exacerbates risk.

Finally, required disclosures of key risk measures would allow market participants to make informed decisions concerning with whom they should do business. Banks using the internal ratings based approach outlined in Basel II will be required to make disclosures about their risk assessments. If some banks are making such disclosures, competitive pressures may cause other or competing banks to disclose additional information about their risk management practices for the payments line of

[12] Horvitz (1996); Scott, Jens and Spudeck (1991a); Scott, Jens, Spudeck (1991b); and DeYoung, Flannery, Lang and Sorescu (1998).

business. BIS (March, 2003) advocates transparency as a means to ensure that markets are contestable, competitive and promote user protection. It recommends disclosures that include information about service quality (speed and convenience), price, security, reliability, confidentiality and potential legal liability to facilitate end user choices. They note that market incentives may not favor such disclosures, which carry a cost.

Summary and Conclusions

Appropriate mitigation depends to some extent on an evaluation of the potential for a risk to impact the functioning of the payments system and commercial markets. More work is needed to evaluate the cost benefit trade-off for mitigating this risk. As payments technology continues to evolve, network vulnerabilities are a resiliency concern, but not a systemic concern. Recent events have demonstrated the contagious nature of network vulnerabilities. Because of the network linkages that exist, these vulnerabilities can jump from the banking sector to other sectors of the economy. The weakest link in the network, be it a bank or a nonbank, can expose all other participants to risk. This risk can cause significant losses and again, these losses are not confined to the banking sector. Finally, consolidation of outsourcers and the increasing use of foreign firms with weaker internal controls to perform outsourced functions present resiliency concerns. However, the existence of multiple retail payments options, the absence of large losses as a result of network vulnerabilities in retail payment systems, the availability of alternative IT vendors, and the ability of technological solutions to limit the risk, all serve to reduce systemic concerns.

To mitigate this risk bank supervisors have four primary tools; chartering requirements, capital regulation, supervision and disclosure. Standardizing the

formatting of payments information flows, linking network vulnerabilities and capital required to support retail payments, and monitoring information on market structure and condition are some of the suggested policies associated with chartering requirements and capital regulation that could mitigate network vulnerabilities.

Encouraging market participants to build in redundancy and scalability, fostering improvements in risk management, developing additional guidance for supervisors on factors that would warrant extending an examination of network vulnerabilities, supporting effective standards and infrastructure arrangements are some of the suggested policies associated with using supervision. An additional recommendation is to identify rules that are ineffective because of changes in technology. Rules should be written to address core issues regardless of the retail payments system if they are to stand the test of time.

Improving disclosure/education of differences among retail payments options for consumers and businesses, increasing information on vendor security practices and requiring disclosure of key risk measures are some of the disclosure recommendations to limit the systemic nature of this risk.

Unresolved questions include: providing appropriate incentives for all payment system participants to invest in network security, ensuring effective security measures as payments system and criminal knowledge evolves, ways market power through the concentration of channel providers can expose the payments system to vulnerabilities, the analytical framework for determining the appropriate capital charge for retail payments risk, appropriate risk indicators for required disclosure, and the ability of incentives rather than regulation to achieve compliance. While the risks posed by network vulnerabilities

are being addressed in the current regulatory framework, advances in technology, concentration in market participants and linkages among diverse participants could cause the risks to change rapidly. Close monitoring is warranted. Further research is needed to explore the systemic nature of the risks identified in this paper.

Appendix

Elizabeth Knospe, Katherine Schrepfer and Angela Wu

PAYMENTS SYSTEM – LAWS AND REGULATIONS[13]

Truth-in-Lending Act (15 U.S.C. § 1601 *et seq*. [Subchapter I of Consumer Credit Protection]) and Regulation Z, (12 C.F.R. Part 226)

Purpose:

The primary purpose of the Truth-in-Lending Act ("TILA") is to promote the informed use of credit by requiring the meaningful disclosure of credit terms and costs to consumers. TILA also seeks to protect the consumer against inaccurate and unfair credit billing and credit card practices. Regulation Z, which implements TILA, contains rules and various disclosure requirements for open-end credit, closed-end credit, oral disclosures, mortgage transactions and requirements for electronic communications.

Applicability

The Regulation applies to each individual or business that offers or extends credit when 4 conditions are met:

(i) the credit is offered or extended to consumers;
(ii) the offering or extension of credit is done regularly[14];
(iii) the credit is subject to a finance charge or is payable by a written agreement in more than four installments; and
(iv) the credit is primarily for personal, family, or household purposes.

In more straightforward terms, TILA applies to creditors.[15] Similar to the 4 elements described above, TILA defines a "creditor" as one who (1) regularly extends, (in connection

[13] Laws and regulations covering credit transactions are also included because they apply to credit card issuers.

[14] "Regularly" is defined in a footnote within 12 C.F.R. § 226.2(17)(i), but generally, the term refers to a person who extended consumer credit more than 25 times (or more than 5 times for transactions secured by a dwelling) in the preceding calendar year.

[15] TILA also specifically exempts certain transactions including:

(1) Extensions of credit primarily for business, commercial, or agricultural purposes, or to government or governmental agencies or instrumentalities or to other than a natural person (e.g., organizations);
(2) An extension of credit not secured by real property or by personal property used or expected to be used as the principal dwelling of the consumer, in which the amount financed exceeds $25,000 or in which there is an express written commitment to extend credit in excess of $25,000;
(3) Transactions in securities or commodities accounts in which credit is extended by a broker-dealer registered with the SEC or the Commodity Futures Trading Commission;
(4) Extension of credit that involves public utility services provided through pipe, wire, other connected facilities or radio or similar transmission;
(5) Transactions for which the Board determines coverage is not necessary;
(6) Home fuel budget plans; and

with loans, sales of property or services, or otherwise), consumer credit which is payable by agreement in more than four installments or for which the payment of a finance charge is or may be required, and (2) is the person to whom the obligation is initially payable on the face of the evidence of indebtedness (e.g., note or contract) or, if there is no such evidence of indebtedness, by agreement. For purposes of certain sections or subchapters of TILA, card issuers, any person who honors the credit card and any person who originates 2 or more mortgages may also be considered "creditors". To further clarify the application of this Regulation, Official Commentary (FRRS 6-1161.3) to Regulation Z indicates that it has some foreign applicability: The Regulation applies to all persons (including branches of foreign banks and sellers located in the U.S.) that extend consumer credit to residents (including resident aliens of any state). For example, a U.S. resident's use in Europe of a credit card issued by a bank in the consumer's hometown is covered by Regulation Z. The Regulation would not apply, however, if a foreign branch of a U.S. bank extends credit to a U.S. citizen residing or visiting abroad.

Fair Credit and Charge Card Disclosure Act of 1988

Purpose

The Fair Credit and Charge Card Disclosure Act of 1988 amends TILA. It provides for more detailed and uniform disclosure by credit and charge card issuers with respect to information relating to interest rates and other fees which may be incurred by consumers through the use of any credit or charge card.

Home Equity Loan Consumer Protection Act

Purpose

Amends Truth in Lending.

The Home Equity Loan Consumer Protection Act amends TILA and establishes additional disclosure, advertising and other requirements for home equity loans and open end consumer credit plans secured by the consumer's principal dwelling.

Fair Credit Billing Act (15 U.S.C. § 1666)

Purpose

Amends Truth in Lending.

The Fair Credit Billing Act amends TILA and provides a mechanism for resolving billing errors.

---

(7) Loans made, insured or guaranteed pursuant to a program authorized by Title IV of the Higher Education Act of 1965.

Conclusion:

The provisions of TILA and Regulation Z are not restricted to financial institutions and may be applicable to non-financial entities, such as commercial entities that sell consumer goods or services on credit and credit and charge card issuers.

Equal Credit Opportunity [Subchapter IV of Consumer Credit Protection]– (15 U.S.C. § 1591 *et seq.*) and Regulation B (12 C.F.R. Part 202)

Purpose

The purpose of the Equal Credit Opportunity Act ("ECOA") is to make credit available to all creditworthy applicants without regard to (i) race, color, religion, national origin, sex, marital status, or age (provided the applicant has the capacity to contract); (ii) the fact that all or part of the applicant's income derives from a public assistance program; or (iii) the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act.

ECOA and its implementing regulations prohibit creditor practices that discriminate on the prohibited bases described above. The regulations require creditors to

- notify applicants of action taken on their applications
- report credit history in the names of both spouses on an account
- retain records of credit applications
- collect information about the applicant's race and other personal characteristics in applications for certain dwelling-related loans; and
- provide applicants with copies of appraisal reports used in connection with credit transactions.

Applicability

In general, Regulation B covers a wider range of credit transactions than Regulation Z. ECOA and Regulation B apply to creditors as defined in 15 U.S.C. § 1691(e) and 12 C.F.R. § 202.2(l). Under ECOA, a "creditor"[16] is defined as

- any person who regularly extends, renews, or continues credit;
- any person who regularly arranges for the extension, renewal, or continuation of credit; or
- any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

[16] A creditor would *not* include the following:

- A person is not a creditor regarding any violation of ECOA or Regulation B committed by another creditor unless the person knew or had reasonable notice of the act, policy, or practice that constituted the violation before becoming involved in the credit transaction.
- "Creditor" does not include a person whose only participation in a credit transaction involves honoring a credit card.

Or, as more simply stated in Regulation B, a "creditor" is a person who, in the ordinary course of business, regularly participates in deciding whether or not to extend credit, including a creditor's assignee, transferee or subrogee who participates in the decision. With respect to certain rules (i.e., 12 C.F.R. § 202.4 and 202.5(a)), creditor also includes a person who, in the ordinary course of business, regularly refers applicants or prospective applicants to creditors, or selects or offers to select creditors.

Exceptions

Limited exceptions apply to certain classes of transactions such as public-utilities credit, securities credit, incidental credit and government credit. These terms and the exceptions that apply to them can be found at 12 C.F.R. § 202.3(a)-(d).

Conclusion

ECOA and Regulation B are not restricted to financial institutions and may apply to commercial entities and other non-financial institutions who meet the definition of creditor set forth above. In addition, "creditor" includes all persons participating in the credit decision, including an assignee or potential purchaser of the obligation who influences the credit decision by indicating whether it will purchase the obligation if the transaction is consummated. "Creditor" has also included a real estate broker who does not participate in credit decisions, but who regularly refers applicants to creditors.[17]

Regulation AA – Unfair and Deceptive Practices (12 C.F.R. Part 227)

Background

Pursuant to the FTC Act (15 U.S.C. § 57a(f)), in order to prevent unfair or deceptive acts or practices by banks or savings and loan institutions, the Board of Governors of the Federal Reserve System was required to establish a separate division of consumer affairs and to institute a procedure to handle consumer complaints regarding unfair or deceptive practices.

Purpose

The purpose of Regulation AA is to establish a division of consumer affairs and a formal complaint procedure to handle consumer complaints about unfair or deceptive acts or practices. Regulation AA also defines and prohibits certain credit practices related to consumer credit contracts.

[17] FRRS 6-164.

Applicability

With respect to the consumer complaint procedures set forth in Subpart A (12 C.F.R. §§ 227.1, 227.2), the Federal Reserve Banks only handle consumer complaints regarding acts or practices of state member banks. All complaints regarding an act or practice of an institution other than a state member bank are referred to the federal agency that has jurisdiction over that institution.

With respect to the unfair credit practices and contract provisions, Regulation AA applies to all state member banks and their subsidiaries.

Conclusion

Regulation AA applies only to state member banks[18]. The complaint procedures set forth in Regulation AA can only be used in connection with state member banks, not with any other banks. Any person (not just customers of state member banks) with a complaint about an unfair or deceptive act or practice of a state member bank may utilize the complaint procedure in Regulation AA.

All state member banks and their subsidiaries are prohibited from including unfair contract provisions or engaging in the unfair credit practices prohibited by Regulation AA.

Gramm Leach-Bliley, Title V, Subtitle A – Disclosure of Nonpublic Personal Information – (15 U.S.C. § 6801 *et seq.*) and Regulation P, (12 C.F.R. Part 216)

Purpose

The purpose of Title V, Subtitle A of the Gramm-Leach-Bliley (GLB) Act is to (i) make customers of financial institutions aware of the privacy policies and practices of those financial institutions; (ii) set guidelines to enable financial institutions to disclose nonpublic personal information about customers in certain situations; and (iii) provide a method to enable customers to opt-out of such disclosure.

Applicability

Regulation P applies to the U.S. offices and entities for which the Board of Governors has primary supervisory authority. This includes state member banks, bank holding companies and certain of their nonbank subsidiaries or affiliates, state uninsured branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks and Edge and agreement corporations.

Financial institutions that provide financial products or services to consumers must comply with the privacy provisions of GLB, Title V and the privacy regulations. Institutions subject to the Board's supervisory authority must comply with Regulation P. Other institutions that are not must comply with the appropriate banking agency rule or, in the event the institution does not fall under any other agency's jurisdiction, it must comply with the FTC privacy rule.

[18] Other federal regulators have similar provisions.

Regulation P defines "financial institution" as one that engages in an activity that is financial in nature or incidental to a financial activity, as described in Section 4(k) of the Bank Holding Company Act of 1956.[19] Examples of such financial activities include

- lending, exchanging, investing for others;
- safeguarding money or securities;
- insuring, guaranteeing, or indemnifying against loss, illness, disability;
- providing financial advice
- underwriting, dealing in, or making a market in securities.

Conclusion

The privacy provisions of GLB and Regulation P apply to any financial institution that provides financial products or services to consumers. Regulation P primarily covers those institutions subject to the Board's supervisory authority, but the privacy provisions of GLB also apply to other entities, such as mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, check cashers, travel agencies and financial advisors. These entities are subject to the FTC's privacy rule (rather than Regulation P) because they are not under any banking agency's jurisdiction.

Credit Repair Organizations – (15 U.S.C. §1679 *et seq.*)

Purpose

The purpose of the Credit Repair Organization provisions is to ensure that buyers of credit repair services from credit repair organizations are provided disclosures sufficient to make informed decisions regarding their purchases and to protect the public from unfair or deceptive advertising and business practices by credit repair organizations.

Applicability

In general, these provisions apply to credit repair organizations (CROs). A CRO is defined as any person who uses interstate commerce or the mails to sell, provide, or perform any service for money
or other value in order to (i) improve any consumer's credit record, history or rating; or (ii) provide advice or assistance to any consumer with regard to any activity or service described in (i) above.

The Act requires CROs to provide certain disclosures regarding consumer credit file rights, enter into written contracts with certain terms whenever a CRO provides services to a consumer and refrain from engaging in unfair or deceptive practices. In addition, the Act prohibits any person (not just CROs) from providing any untrue or misleading statements about a consumer's creditworthiness, credit standing or credit capacity. Any violation of any requirement of these provisions with respect to CROs constitutes an unfair or deceptive act or

[19] The list of activities in section 4(k) (12 U.S.C. § 1843(k)) is not exhaustive. Additional activities may also include those the Board, in consultation with the secretary of the Treasury, determines to be financial in nature or incidental to a financial activity in accordance with section 4(k).

practice in violation of the FTC Act. The FTC Commission is granted the power to enforce compliance under these provisions.

Conclusion

The Act seems to apply primarily to non-financial institutions. The statute specifically excludes the following from the definition of credit repair organization:

- nonprofit organization which is exempt from taxation under 26 U.S.C. § 501(c)(3);
- any creditor with respect to any consumer, to the extent the creditor is assisting the consumer to restructure any debt owed by the consumer to the creditor;
- any depository institution (as defined in 12 U.S.C. § 1813) or any Federal or State credit union (as defined in 12 U.S.C. § 1752), or any affiliate or subsidiary of any of them.

Identity Theft

Pub. L. No. 105-318 – **Identity Theft and Assumption Deterrence Act of 1998**

Purpose and Applicability

The primary purpose of this Act is to make identity theft and similar unlawful activity a criminal offense. To address the lack of available resources for victims of identity crimes and to assist these victims, the Act also establishes a centralized complaint procedure and consumer education service.

This Act amends the federal criminal code to make it unlawful for anyone to knowingly transfer or use another person's means of identification with intent to commit, aid or abet any unlawful activity that violates federal law, or that constitutes a felony under any applicable State or local law. The Act also imposes criminal penalties involving fraud and related activity connected to identification documents (identity fraud).

In addition, this Act directs the FTC to establish procedures to (1) log and acknowledge the receipt of complaints by individuals having reason to believe that any of their means of identification have been assumed, stolen or otherwise illegally acquired; (2) provide informational materials to such individuals; and (3) refer such complaints to the appropriate entities, including national consumer reporting agencies and law enforcement agencies.

Conclusion

This Act applies to all persons. With respect to complaints relating to identity fraud, assumption, theft or other unlawful activity, entities such as national consumer reporting agencies may have additional responsibilities

PROPOSED BILL: H.R. 220 – Identity Theft Prevention Act *- A Bill was introduced on January 28, 2003 to prevent identity theft and fraud and to promote increased awareness of such crimes. The Bill was referred to the Committee on Banking, Housing and Urban Affairs.*

This bill proposes to amend the TILA to require the following:

- Credit card issuers who receive requests for additional credit cards on an existing credit account after receiving a change of address notice for that account must send the additional card and notify the cardholder of the request at both the new and former address and provide the cardholder with a means to promptly report incorrect changes.

This bill also proposes amendments to the Fair Credit Reporting Act (FCRA) that provide the following:

- Consumer reporting agencies are required to include a fraud alert in the file of a consumer at the consumer's request. Consumer reporting agencies must also notify each person seeking consumer credit information regarding a consumer of the existence of a fraud alert in that consumer's file. These provisions do not apply to resellers of information and institutions such as check services companies and demand deposit account information service companies. In general, the amendment would require the FTC to enforce this provision, but in other cases, as applicable, other federal agencies such as the OCC, Board of Governors, FDIC, OTS and NCUA, would be responsible for enforcement.

- At the consumer's request, and without charge to the consumer, a consumer reporting agency must provide disclosures listed under Section 609 of the FCRA (i.e., a credit report) to the consumer once during any 12-month period.

In addition, the bill seeks to prohibit any person (including firm, partnership, corporation or other entity) that accepts credit cards for business transactions from printing more than the last 5 digits of the credit card account number or the expiration date on any electronically printed receipt provided to the cardholder. This provision does not apply to transactions where the sole means of recording the credit card number is by handwriting or by an imprint or copy of the credit card.

Applicability and Conclusion

These new proposed TILA amendments relating to credit cards would apply to financial and other types of institutions such as retailers and any other commercial entity. Amendments under the Fair Credit Reporting Act relating to fraud alerts and credit reports affect consumer-reporting agencies. Credit reporting agencies are not limited to financial institutions, but are defined broadly to include any person which, for fees or on other cooperative nonprofit bases, regularly assembles or evaluates consumer credit information or other consumer information for the purpose of furnishing consumer reports to third parties and which uses means of interstate commerce to prepare or furnish consumer reports.

Fair Credit Reporting Act (15 U.S.C. § 1681) FRRS 6-1550

Purpose

The purpose of the Fair Credit Reporting Act is to require consumer reporting agencies to adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy and proper utilization of such information in accordance with the requirements of this title.

The Act is designed to regulate the consumer reporting industry, to place disclosure obligations on users of consumer reports, and to ensure fair, timely, and accurate reporting of credit information. It also restricts the use of reports on consumers, and in certain situation, requires the deletion of obsolete information.

Applicability

The Fair Credit Reporting Act applies to those who use Consumer Credit Reports and Consumer Reporting Agencies. A Consumer Reporting Agency is defined as any person who, for money, dues or on a cooperative nonprofit basis regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

The Act applies to banks that are Consumer Reporting Agencies and that are users of the information. A bank is considered a consumer-reporting agency if it regularly furnishes information about a consumer to, for example, other creditors, correspondents, holding companies or affiliates. A bank is not required to report information on its own transactions or experiences with a consumer and a bank does not become a CRA if it furnishes information from outside sources to another party involved in the same transaction. (See FRRS 6-1584.)

Conclusion

The Fair Credit Reporting Act applies to any entity that uses a Consumer Credit Report or is, by definition, a Consumer Reporting Agency. [Banks are likely to be subject to the Act as credit grantors, dealer paper purchasers, credit card issuers and employers. In general, the Act does not apply to commercial transactions.] (See FRRS 6-1578.)

Fair Debt Collection Practices Act (15 U.S.C. 1692) FRRS 6-1675

Purpose

The purpose of the Fair Debt Collection practices Act is to eliminate abusive debt collection practices by debt collectors, to insure that the debt collectors who comply are not competitively disadvantaged and to promote consistent state action to protect consumers against debt collection abuses.

Applicability

The Act applies to debt collectors. A debt collector is defined, generally, as any person who uses any instrumentality of interstate commerce or the mails in any business the principal purpose of which is the collection of any debts or who regularly collects or attempts to collect, directly or indirectly, debts owed or due or asserted to be owed or due another.

The Act applies to banks that regularly collect debts for other unrelated institutions, including collections under reciprocal service agreements.

FRRS 6-1703: *COVERAGE (*§ 803)

The act is applicable only to a person or institution that regularly collects or attempts to collect, directly or indirectly, consumer debts asserted to be *owed to another person or institution. C*onsumer debt is that debt incurred by an individual primarily for personal, family, or household purposes. Debts incurred for business or agricultural purposes are not covered. The following are not covered by the act:

- officers or employees of a bank who collect, in the bank's name, debts owed to the bank
- attorneys-at-law collecting debts on behalf of the bank
- legal process servers

FRRS 6-1704: *BANK AS A DEBT COLLECTOR*

The act is applicable to banks that regularly collect debts for other unrelated institutions, including collections under reciprocal service agreements. Typically under such an arrangement, a bank solicits the help of another bank in collecting a defaulted debt of a consumer who has relocated. A bank would also be subject to the requirements of the act if it uses a name other than its own in its collection efforts.

A bank is *not* a debt collector subject to the act when it—

- collects debts due another only in isolated instances;
- collects, in the bank's own name, debts owed to the bank;
- collects a debt that it originated and sells even though it services the debt, for example, mortgages and student loans;
- collects a debt not in default when obtained;
- collects a debt obtained as security for a commercial credit transaction involving the bank;
- collects a debt incidental to a bona fide fiduciary relationship or escrow arrangement, for example, debt held in the bank's trust department; or

- collects a debt for another person to whom it is related by common ownership or corporate control, as long as it does so *only* for those persons to whom it is so related. *However*, if the bank regularly collects defaulted debts owed a nonaffiliate person, the bank will become a debt collector for those defaulted debts as well as for defaulted debts of affiliated entities, but not for its own debts.

Conclusion

The provisions of the Fair Debt Collection Practices Act apply to any entity that acts as a debt collector as defined by the Act and may include financial institutions.

Expedited Funds Availability Act (12 U.S.C. § 4001 *et seq.) and* Regulation CC (12 C.F.R 229)

Purpose

The purpose of this law is to limit the amount of time banks may hold depositors' funds. Regulation CC implements the Expedited Funds Availability Act. The law and regulation contain outside time limits for banks to make funds deposited into transaction accounts available for withdrawal by an account holder (and related rules). Subpart C of the regulation contains rules designed to expedite the collection and return of checks.

Applicability

The availability rules are applicable to depository financial institutions (but not edge and agreement corporations). The collection and return rules in Subpart C of Regulation CC are applicable to depository financial institutions and "any person engaged in the business of banking, as well as a Federal Reserve Bank, a Federal Home Loan Bank, and a state or unit of general local government to the extent that the state or unit of general local government acts as a payment bank." (12 U.S.C. § 4002, 12 C.F.R § 229.2(e)). The Board's commentary indicates that this section intends that all checks will be covered by the same rules for forward collection and return (even if the availability rules do not apply).

Conclusion

The funds availability provisions are applicable to depository financial institutions. The collection rules apply to all entities engaged in bank collection activities.

Electronic Fund Transfer Act (15 U.S.C. § 1693 *et seq.) and* Regulation E (12 C.F.R Part 205)

Purpose

The purpose of this Act is to provide a basic framework that establishes the rights, liabilities and responsibilities of participants in electronic fund transfer systems. The primary objective is the provision of individual consumer rights. (15 U.S.C. § 1693, 12 C.F.R § 2051).

Applicability

The EFT Act and Regulation E are generally applicable to "financial institutions that debit or credit a consumer's account" as the result of an electronic fund transfer (including point of sale transfers, ATM transfers, direct deposit or withdrawal of funds, debit card transactions). However, the definition of "financial institution" is broad and includes traditional depository institutions and any other person that directly or indirectly holds an account belonging to a consumer or that issues an access device (card, PIN, etc.) and agrees with a consumer to provide EFT Services. (15 U.S.C. § 1693(a)(18), 12 C.F.R. § 205.2(i)). For example, the Board's Commentary indicates that a debit card or other access device that accesses a securities or commodities account, such as a money market mutual fund, is covered under the Act and Regulation.

In addition, the EFT Act and Regulation contain four sections that specifically apply to "a person." Three of these provisions relate to preauthorized transfers from an account (requiring a written authorization notice of transfers in varying amounts and prohibiting certain practices). (12 C.F.R. § 205.10(b)(d) and (e)). The last section, which applies to any person, requires retention of records for a specified period. (12 C.F.R. § 205.13).

Conclusion

Generally, this law applies to financial institutions that electronically debit or credit a consumer's account. Four provisions apply to other entities as well.

****NOTE:** **[*The following regulation applies to NON-BANK entities.*]**

Uniform Money Services Act

Background and Purpose

In 2000, the National Conference of Commissioners on Uniform State Laws (the body that approves changes to the *Uniform Commercial Code* and other uniform state laws), approved the Uniform Money Services Act. This Act is a safety and soundness law that creates licensing requirements for various types of money services businesses, including money transmissions and sales of payment instruments (money orders, traveler's checks, stored value, and check cashing).

Applicability

This law is directed at the proliferation of non-bank companies now providing money services _ indeed banks (and the U. S. Government and postal service) are specifically exempted. The law also provides for reporting record keeping and examinations by a state regulator. A number of states have statutes covering some or all of this subject that predate passage of this uniform act. For example, Illinois has had a law that regulates money transmitters since 1995. It has since been amended to include text very similar to the uniform law. (205 ILCS 657/1 *et seq.*)

Conclusion

This law, by its terms, does not apply to banks, but rather covers non-banks.

References

ABA Banking Journal. November 2002. "Debit on Trial." Pages 31-36.

Bank for International Settlements, Basel Committee on Banking Supervision. February 2003. "Sound Practices for the Management and Supervision of Operational Risk." Basel Committee Publications No. 96.

Bank for International Settlements, Basel Committee on Payment and Settlement Systems. March 2003. "Policy Issues for Central Banks in Retail Payments." Bank for International Settlements Press & Communications, Pages 32-33.

Bank of England. November 2000. "Oversight of Payment Systems." www.bankofengland.co.uk.

Bayot, Jennifer. May 2003. "Settlement Is Seen As Changing Ways Consumers Use Debit Cards." The New York Times.

BNA Banking Report. March 2003. "Rep. Frank Appoints Rep. Hooley to Lead Democratic ID Theft Panel." BNA Banking Report No. 9, Page 383.

Boettger, Faith. September 2002. "Risk Management of Outsourced Technologies." BITS. Financial Services Roundtable.

Boston Consulting Report. 2003. "The Payments Puzzle – Putting the Pieces Together." BCG Global Payments Report.

Bradford, Terri, Matt Davies and Stuart E. Winer. December 2002. "Nonbanks in the Payments System." Federal Reserve Bank of Kansas City Working Paper Series (WP02-02).

Business Week Online. February 2003. "Online Extra: Perilous Currents in the Offshore Shift." www.businessweek.com…t/magazine/content/03_05/b3818051.html.

Celent. March 2003. "Banks' Payments-Driven Revenues: Why Banks Need Payments Czars." http://www.celent.net/Pressreleases/20030227/PaymentsEmail.html.

Chakravorti, Sujit and Emery Kobor. 2002. "Why Invest in Payment Innovations?" Federal Reserve Bank of Chicago Working Paper.

Cournoyer, Susan, Bruce Caldwell, Tony Adams, Ron Silliman and Allie Young. January 2003. "IBM Ends Year With On-Demand Bank in Banking." Gartner Dataquest Alert, (ITSV-WW-DA-0179).

DeYoung, Robert, Mark J. Flannery, William W. Lang and Sorin M. Sorescu. "The Informational Advantage of Specialized Monitors: The Case of Bank Examiners." Federal Reserve Bank of Chicago Working Paper (1998-4).

Federal Deposit Insurance Corporation. December 2002. "QBP – Stats At A Glance." http://www.fdic.gov/statistical/stats/2002dec/industry.pdf.

Ferguson, Jr., Roger W. February 2003. Statement before the Subcommittee on Domestic and International Monetary Policy, Trade and Technology Committee on Financial Service, House of Representatives.

Flannery, Mark J., 1998. "Modernizing Financial Regulation (Again)." Paper presented at a conference on Financial Modernization and Regulation, Federal Reserve Bank of San Francisco.

Gillis, Arthur. December 2002. "Should You Outsource? It Depends." American Banker.

Global Concepts. "2003 Update: Trends in the Payments System." Presentation to the Internet Forum, (2/28/03).

Goodfriend, Marvin S. 1989. "Money, Credit, Banking and Payment System Policy, in the U.S. Payments System: Efficiency Risk and the Role of the Federal Reserve." Kluwer Academic Press, edited by D. Humphrey.

Herring, Richard J. and Anthony M. Santomero. May 1999. "What Is Optimal Financial Regulation?" Wharton Financial Institutions Center Working Paper.

Hollingsworth, Donald and Alan Rodack. January 2003. "Response for Comment on Corporate Check Conversion/Truncation." http://www.afponline.org/Information_Center/Government_Relations_Comment/clnacha013103/clnacha013103.html.

Horvitz, Paul M. "Financial Disclosure: Is More Always Better?" Journal of Retail Banking Services (Winter 1996).

Kellogg, Paul. 2003. "Evolving Operational Risk Management for Retail Payments." Federal Reserve Bank of Chicago Working Paper.

Kuttner, Kenneth N. and James J. McAndrews. December 2001. "Personal On-Line Payments." Federal Reserve Bank of New York Economic Policy Review.

Kuykendall, Lavonne and W.A. Lee. February 2003. "Intermediary Risk? Card Hack Puts ISO's in the Hot Seat." American Banker, Vol. CLXVII, Page 1.

Lemos, Robert. February 2003. "Slammer Attacks May Become Way of Life for Net." CNET News.com. http://news.com.com/2009-1001-983540.html.

McAndrews, James J. July 1999. "E-Money and Payment System Risks." Contemporary Economic Policy, Vol. 17, No. 3, Pages 348-357.

McAndrews, James J. and Simon M. Potter. November 2002. "Liquidity Effects of the Events of September 11, 2001." Federal Reserve Bank of New York Economic Policy Review.

Mester, Loretta J. 2000. "The Changing Nature of the Payments System: Should New Players Mean New Rules?" Federal Reserve Bank of Philadelphia Business Review (March/April), Pages 3-26.

National Credit Union Administration. Statistics for Federally Insured Credit Unions. http://www.ncua.gov/ref/statistics.html.

NYCE. March 2003. Annual Report. http://www.nyce.net/about_NYCE_annual.html.

O'Harrow Jr., Robert and Ariana Eunjung Cha. January 2003. "Virus Exposes Perils of the Web – Latest Computer Bug Shows Firms May Be Vulnerable in Linking to the Internet." The Washington Post .

Office of Inspector General, Board of Governors of the Federal Reserve System. October 2002. Report on the Failure of the Oakwood Deposit Company.

Pulse. http:www.pulse-eft./default.asp.

Rice, Tara. 2003. "The Importance of Payments-Driven Revenues to Franchise Value and in Estimating Bank Performance." Federal Reserve Bank of Chicago Working Paper.

Rice, Tara and Kristin Stanton. 2003. "Estimating the Volume of Payments-Driven Revenues." Federal Reserve Bank of Chicago Working Paper.

Roberds, William. 1998. "The Impact of Fraud on New Methods of Retail Payments." Federal Reserve Bank of Atlanta Economic Review (First Quarter), Pages 42-52.

Scott, Jr., David F., William G. Jens, Jr. and Raymond E. Spudeck. "The Secrecy of CAMELS." The Bankers Magazine (September/October 1991a).

Scott, Jr., David F., William G. Jens, Jr. and Raymond E. Spudeck. "Give Public Access to Taxpayer-Funded Secret Bank Ratings System." Challenge (November/December 1991b).

Siegel-Bernard, Tara and Riva Richmond. February 2003. "Hackers Steal 8M Credit Card Account Numbers." Dow Jones Newswires.

Star Financial Institutions. About Star. http://www.star-systems.com/about-fi.html.

U.S. General Accounting Office. March 2002. " Identity Theft: Prevalence and Cost Appear to be Growing." Report to Congressional Requestors (GAO-02-363).

U.S. General Accounting Office. February 2003. "Potential Terrorist Attacks: Additional Actions Need to Better Prepare Critical Financial Market Participants." Report to the Committee on Financial Services, House of Representatives (GAO-03-414).

Visa. http://www.usa.visa.com/personal/aboutvisa/who/who_we_are_corporate_profile.html.