POLICY STUDIES

Evolving Operational Risk Management for Retail Payments

Paul Kellogg

Emerging Payments Occasional Papers Series
2003-1E

FEDERAL RESERVE BANK
OF CHICAGO

Evolving Operational Risk Management for Retail Payments

Paul Kellogg

Abstract

Payment systems are an integral component of banking that is undergoing material change. Industry trends and discussions with key banking personnel highlighted four issues that are top concerns for banks engaged in emerging payments: changing delivery channels and safeguards, fraud, vendor oversight, and operational risk measurement and reporting. While risk management practices are evolving to meet current and emerging risks, bank management should increase their effort to make sure the overall risk is reported to senior management and Directorates.

Supervisory Examiner, Federal Reserve Bank of Chicago, paul.e.kellogg@chi.frb.org. The author thanks the interviewees within the sample for their insightful responses, and would also like to thank Margaret Beutel, Bob Chakravorti, Denise Duffy, Cathy Lemieux, Fred Miller, Paul Neff, Tara Rice and Ken Swenson 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.

I. Introduction

The payments industry has undergone significant change over the past several decades. The volume in debit card, credit card and ACH nearly doubled between 1995 and 2000. The share of noncash retail payments made by check has fallen from 77 percent in 1995 to 59 percent in 2000 according to Federal Reserve data. Retail payments products are an important business line for banks. Estimated income earned in 2001 on traditional checking products at regional banks was approximately six percent of total revenue (Rice, 2003). When other sources of payment revenue are included, such as ATM fees and payments-related credit card revenue, the percentage increases to twenty percent for regional banks.

This shift from paper to electronic payments changes the operational risk profile of banks because it represents a change in the business processes associated with retail payments. Traditional check systems are paper-based, batch systems that focus on securing the transfer of physical documents. Electronic systems focus on transferring electronic information, often over open architecture networks[1], and are moving toward real-time[2] processing. One should also note that check truncation and electronic check presentment is moving check processing to a more "electronic" type of processing system.

Evidence points to increasing fraud and criminal activity in retail payments systems. Carnegie-Mellon's CERT Coordination Center reports that verified incidents of compromised computer security have surged since 2000. Fraudulent transactions

[1] In this context, open architecture networks reflects open architecture, which is a computer architecture whose details are fully made public so that other manufacturers can make clones and compatible accessories; and, open source software, whose source is published so that a variety of people can add contributions. Significant examples of open source software include the Linux operating system and Apache web server. Knowledge derived from open architecture and systems can also be used to exploit or disable its controls.

accounted for only 0.1 percent of the volume of non-Internet transactions but 2.1 percent of online volume. Approximately 76 percent of all Suspicious Activity Reports (SARs) filed between 1996 and 2001 were related to payments fraud[3]. Over the same time period the total volume of SARs increased nearly four-fold. The American Bankers Association reported in its 2000 survey of bankers that total direct check-fraud losses in commercial bank accounts was $679 million in 1999, a 33 percent increase over losses in 1997. The Federal Trade Commission reported receiving 160,000 complaints about identity theft in 2002. The average amount of time spent by victims to regain their financial health was 175 hours. Furthermore, these cases dragged on for an average of two years, with many cases taking more than four years to be resolved (Givens, 2000). Celent estimates that US financial institutions will lose in excess of $8 billion over a four year period, ending in 2004, due to identity theft. (Celent, 2001).

Increasingly, banks are only handling a portion of the payments system components. Banks are relying on outsourcers, nonbank partners, and joint ventures to provide a full array of payments services to their customers. Prudential Securities estimates that financial services companies will spend $130 billion on information technology services next year and increase that amount by an annual rate of 12 percent. They estimate outsourcing accounts for 35 percent of information technology spending.

The growing importance of electronic payments, combined with the increasing vulnerabilities of electronic networks, the growth in payments fraud and the increasing participation of nonbanks in the payments system, represents a shift in the operational risk

[2] The processing of transactions on the computer as they occur, rather than batching them for processing at a later time. It is, therefore, more challenging to detect and prevent unauthorized transactions before it is applied to an account balance.

profile of banks. This project investigates how banks are dealing with this shift. The first section provides background information. The second section reports the results and the final section summarizes the findings.

II. Evolution of Operational Risk Management

Banks are in the business of managing risk. Their assessment of risk drives their product pricing decisions. Errors in their risk assessment will lead to losses that can, over time, impact the viability of the organization. The work done by both the industry and bank supervisors has focused increasing attention to the accurate estimation of total risk on an enterprise-wide basis. Considerable work has been done on refining the estimation of credit and market risk. As these measures become more precise, however, it is important to recognize that the assessment of other risks needs to keep pace.

The definition of operations risk has evolved over time. The Basel Committee on Banking Supervision, an international group of banking supervisors, defines operational risk as, "the risk of losses resulting from inadequate or failed internal processes, people and systems or from external events."[4] This is the definition that is currently being used by bank supervisors. In his testimony before the House Committee on Financial Services, Vice Chairman Roger W. Ferguson Jr. of the Federal Reserve's Board of Governors included the following in his examples of operational risk: rogue traders, fraud and forgery, settlement failures, inappropriate sales practices, poor accounting and lapses of control (Ferguson, 2000). Dow (2000) identified four principal causes of well-known episodes of financial failure in the US and Europe in the 1980s and 1990s. Of the 19 cases

[3] The SAR Activity Review, *Trends, Tips & Issues*, Issue 4, Published under the auspices of the Bank Secrecy Act Advisory Group, Department of the Treasury, August 2002.
[4] Basel Committee on Banking Supervision, Consultative Paper 3, April 2003.

listed, Ferguson's examples of operational risk are listed by Dow as the cause of 18 of the various financial disturbances. For instance, Barings' failure due to a rogue trader[5] and the US Savings and Loan failure[6] due to management's focus on profitability to the extent that excessive risks were taken to enhance short-term profitability (ignoring internal controls and poor accounting). Earlier definitions of operations risk were narrower and tended to focus on failure of software, hardware and security controls. The current definition expands this from a technology focus to include all internal processes and management oversight and the mitigation of these risks.

Recent research on risk inherent in emerging payments have highlighted the importance of operational risk (Bradford, Davies and Winer, 2002; Mesiter, 2000; Bank of England 2000; McAndrews, 1999 and Roberds, 1998). According to McAndrews (1999), "It is not, however, conventional credit, liquidity, and settlement risks that pose novel threats to the smooth operation of the payment and banking systems from the introduction and widespread acceptance of e-money. Rather, the threat arises principally from the uncertainty regarding fraud, legal and operational risks to the systems."[7] Bradford, Davies and Winer (2002) delineate the complex interdependencies between banks and nonbanks

[5] Trader Nick Leeson was supposed to be exploiting low-risk arbitrage opportunities that would leverage price differences in similar equity derivatives on the Singapore Money Exchange (Simex) and the Osaka exchange. In fact, he was taking much riskier positions by buying and selling different amounts of the contracts on the two exchanges or buying and selling contracts of different types. Because Leeson was given control over both the trading and back office functions, he was able to circumvent the internal controls that would have escalated the unauthorized activity to executive management. As Leeson's losses mounted, he increased his trades. However, after an earthquake in Japan caused the Nikkei Index to drop sharply, the losses increased rapidly, with Leeson's positions going more than $1 billion into the red. This was too much for the bank to sustain; in March of 1995, it was purchased by the Dutch bank ING for just one British pound sterling. (ERisk, 2000)

[6] In February 1989, President George Bush announced a program to rescue the stricken Savings & Loan industry. Between 1986 and 1995, the underwriting of US thrifts by the financial industry and the US taxpayer cost approximately $153 billion. One of the many lessons learned is that rapid growth into new lines of business signals the need for tighter risk management and financial controls (Jameson, 2002).

[7] James J. McAndrews, "E-Money and Payment System Risks," Contemporary Economic Policy, Vol. 17, No. 3, July 1999. pg.348

participating in the payments system. "Even though nonbanks are rarely involved in the direct transfer of funds, they are heavily involved in the transfer of payments-related information. As technological innovations in payments systems continue, the risk of operational failures impacting the flow of payments increases."[8] Bradford, Davies and Winer (2002) also identify operational risk issues as important areas for further research to enhance policymakers understanding of the changing risk profile of banks and nonbanks involved in the payments system. Appendix III provides more detail on how supervisors evaluate this risk. The Bank of England (2000) identified concentration in the use of third-party infrastructure suppliers or common reliance on a particular hardware or software as examples of common dependencies where an operational failure could impact the integrity of the entire payments system. Historically, operational risk has been considered idiosyncratic, but the interconnections between banks and nonbanks increase the potential for a systemic impact, as operational malfunctions in one organization may be transmitted throughout an entire system of users. While it is understood that network effects have benefits that should be considered, such as standardization, these benefits have to be weighed against the single sources of failure caused by a limited number of vendors supporting the majority of a market.

III. Managing Operational Risk

The Basel Committee on Banking Supervision[9] defines crucial elements of an effective operational risk management framework as:

[8] James J. McAndrews, "E-Money and Payment System Risks," Contemporary Economic Policy, Vol. 17, No. 3, July 1999. pg.348

[9] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, February 2003. The Basel Committee on Banking Supervision is commonly associated with global banking. However, it is important to point out that representatives from the Comptroller of the

1. Clear strategies and oversight by the board of directors and senior management.

2. A strong internal control[10] culture (including, among other things, clear lines of responsibility, independent audit validation, and segregation of duties).

3. Effective internal reporting and contingency planning.

Within the context of this framework, explicit roles are set forth for the banks and its supervisor. The role of the bank is twofold: (1) develop an appropriate risk management framework; and, (2) demonstrate effective risk management through the explicit identification, assessment, monitoring and mitigation/control of operational risk. Assurance for the bank performance falls upon the supervisor, whose role is to require that regulated institutions have an effective operational risk framework in place, and to verify that the institution is in compliance with the polices and practices defined by the framework.

A short example of an operational framework is provided in the following narrative, with a more detailed example is provided in Appendix II. In this example, key performance indicators (i.e. metrics with a focus towards production) are relatively mature. However, to effectively report upon the key risk drivers desired by the board, the key performance indicators have to be refined and augmented following a corporate standard before they can be converted into Key Risk Indicators ("KRIs"). Initially, KRIs would target risks within each line of business. For example, effective KRIs would speak to the

---

Currency (which regulates national banks in the United States) and the FDIC (which insures banks in the United States) sit on the committee, which is chaired by Mr. Roger Cole, of the Federal Reserve Board.

[10] For the purposes of this paper, internal control is defined as a process effected by a bank's Directorate, management and other personnel designed to provide reasonable assurance regarding the achievement of objectives in reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

overall risk and risk management practices for payments and settlement functions within each of the business lines, such as Corporate Finance, Trading/Sales, Retail Banking, and Commercial Banking. Even though different measures may be used due to the differences within each of the lines of business, the measures should share the same objectives:

- Determining the level of inherent risk;
- Monitoring the effectiveness of the risk management practices that are controlling/mitigating material risks;
- Determining whether the residual risk (the remaining risk after controls have been applied against the inherent risk) is improving, stable or eroding over time.

When advancing to the next level of sophistication, the KRIs need to be refined and normalized to provide a holistic view of payments and settlement across the entire banking institution. Ideally, a payments and settlement report to the risk committee would identify concentrations of risk and where controls for payments and settlement are stressed within the institution. With a few more refinements, executive management and the board should be able to determine if their business strategies were resulting in unintended stress points within payments and settlement. Ultimately, operational-risk executive-reporting should more clearly identify cause and effect, help management to work within their risk appetite, and target higher risk areas that may require a repricing of products, an exit strategy, or a shoring up of controls.

The benefit of the Basel guideline is that it helps management and bank supervisors develop a more uniform approach to identify, assess, monitor and control/mitigate operational risk. While the success or failure of management practices for credit, market,

and liquidity risk are tied to financial reporting, the cause and effect for operational risk are currently less clear. By the time an adverse operational condition reveals itself in financial reports, the costs for corrective action can be extraordinary. The Barings Bank and Allied Irish[11] incidents are two high profile examples that received global attention.

Absent clear reporting, bank directors rely on executive officers to evaluate the overall health of operational risk. Where reports are provided, they generally require explanation from executive management due to the lack of standardization or clarity in reporting. In some cases, a shift in operational risk may be so subtle between periods of time that it may exceed the Directorate's risk threshold undetected. Without historical bank data, operational risk lacks context; and without that context, it can be misvalued.

A sample of industry articles and guidelines suggests operational risk management practices are evolving in the manner suggested by Basel. For example, the International Swaps and Derivatives Association, Inc. has released guidance, "to bring a structured approach to the assessment of qualitative factors in operational risk management and reflect the need for an objective, internationally applicable approach to assessing operational risk."[12] A McKinsey survey (2002, number 4) of 200 directors of large corporations on corporate governance found that most directors are not confident that they understand the full magnitude of a firm's risks. At Risk Management Association's

[11] On February 6, 2002, Allied Irish Banks - Ireland's second-biggest bank – revealed that it was investigating an apparent currency fraud at its Baltimore-based subsidiary, Allfirst, perpetrated by a trader named John Rusnak. The AIB board of directors commissioned an independent report into what had gone wrong. Written by Eugene Ludwig, a former US Comptroller of the Currency, the report concluded that Rusnak had systematically falsified bank records and documents, and been able to circumvent the "weak control environment" at Allfirst's treasury. Estimates of the total losses to AIB/Allfirst are around $691 million. One of the many lessons learned is that risk management architecture is crucial - The Ludwig report concluded that risk management structure and practices within Allfirst's currency trading operations were seriously flawed. As described in an Erisk commentary earlier in 2002, the operational risks that this implies can quickly transform the typically large market risk exposures incurred in a proprietary trading environment into hard losses (McNee, 2002).

(RMA) Operational Risk Forum participants noted that obtaining clean, meaningful, and timely data across business unit and product lines and communicating the benefits of the program, such as improved productivity and quality, as well as loss reduction to top management were two major challenges. In 2002, RMA and First Manhattan Consulting Group conducted a survey of 30 international financial institutions that produced similar findings. Banks within this sample are experiencing similar challenges.

IV. Survey Findings

To gain insight into the banking industry's thoughts on this issue, representatives from a variety of banks in the Midwest that provided standard retail payments products and utilized multiple payment channels were interviewed. The respondents' input, combined with general industry trends, provides insights into the status and challenges of operational risk for retail payments. The questions were designed to determine what operational risks payment activities pose to their banking organizations, and how they control those risks.

For the purposes of this project, Large Banking organizations (LB) are defined as financial institutions with consolidated assets greater than $10 billion. Regional Banking organizations (RB) have consolidated assets less than $10 billion.

An "x" in the response column indicates that a majority of those interviewed fell into that given category.

[12] ISDA – International Swaps and Derivatives Association, Inc., *Operational Risk Regulatory Approach Discussion Paper*, September 2000

Question 1

What products and services do you offer?		
	LB	RB
Check	X	X
Credit Card	X	X
Electronic Banking	X	X
Electronic Payment	X	X
ATM	X	X
Debit Card	X	X
Point of Sale	X	X
Cash Management	X	X
Electronic Bill Payment & Presentment	X	X

The first question was asked to ensure that the sample shared most of the retail payment products. The table illustrates that a majority of the payment products are offered by most of the sample.

Question 2

What key measures are used to manage operational risk?		
	LB	RB
Key Performance Indicators	X	X
Key Risk Indicators	X	X
Service Level Agreements	X	X
Breaches in Risk Trigger Thresholds	X	X
Business Metrics	X	X
Fraud and Operational Loss Data	X	X
Concentration of Audit Findings	X	X
Reconcilement Control Trend Data	X	X
Other	X	

The second question determines the degree of evolution regarding operational risk metrics (measures) for the sample. A broad set of operational metrics will better identify, measure, and monitor operational risk than metrics solely devoted to an operation's production – such as "down-time" metrics, for example.

Respondents indicate that both LBs and RBs have key measures in place to capture a broad spectrum of risks associated with payments. Comments from LBs evidenced a higher evolution of these measures because large commercial banks process a majority of

the checks processed by financial institutions (23.6 billion transactions out of the 42 billion processed for the year 2000), with the Midwest region processing the largest number of checks, per capita (Gerdes and Walton II, 2002).

RBs also indicated they use a suite of key measures to identify operational risk. However, they seemed less confident in their ability to measure and monitor operational risk on a timely basis. Some detection measures were more advanced than others, such as money laundering detection systems required by BSA[13] and the systems designed to flag entities identified by OFAC.[14] Advances in this area will help banks understand the full loss exposure, or collective vulnerability, related to the release of new products, service outages and lapses in internal controls. The RBs and LBs were researching surveillance software to better identify operational risks, such as fraud, within and across the payment systems. Smaller banks in the sample had fewer key measures in place.

Question 3

Which key controls are used to manage operational risk?		
	LB	RB
Risk Mapping	X	X
Enterprise-wide Change Control	X	X
Internal Control Self-Assessments	X	X
Audits	X	X
Incident Cause Analysis	X	X
Reconcilement Control	X	X
Loss Reporting	X	X
Thresholds Set Within Payments Applications	X	X
Other	X	X

The third question indicates the degree of progress banks have made on key control metrics for operational risk. While payments processing has historically been subject to

[13] The Bank Secrecy Act (BSA) requires financial institutions to establish anti-money laundering programs.
[14] The Office of Foreign Assets Control (OFAC) is a department of the U.S. Department of Treasury. It enforces economic and trade sanctions against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC

rigorous production control, including an assessment of the related credit risk, other factors relating to operational risk may need to be captured to fully determine aggregate risk. This level of control rigor is a sound practice, and is an extension of the Federal Reserve's 1995 supervisory policy statement on sound risk management processes (Federal Reserve SR 95-45, 1995). The policy defines operational risk as a distinct risk, and suggests sound risk-management process including the following:

- Active board and senior management oversight;
- Adequate policies, procedures, and limits;
- Adequate risk measurement and monitoring, and
- Management information systems and comprehensive internal controls.

Survey responses show a concerted effort to more comprehensively control operational risks specific to payments. The LBs and RBs were deploying internal control self-assessments, audit findings, centralized reconcilement reporting, and were perfecting operational loss reporting to monitor the adequacy of their controls within payments systems. Risk thresholds were being set and monitored to mitigate operational losses on an ongoing basis. Enterprise-wide change control and incident-cause analysis were being used to reduce disruptions to payments systems resulting from ill-timed programming changes and recurring operational issues. Risk-mapping techniques were being used to heighten the accountability of executives responsible for executing operational risk management processes. Defining accountability is particularly important, as many of the processes relating to payments processing are threaded throughout the lines of business and support units.

---

acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction.

Smaller banks used audit to assess compliance with operational risk frameworks. Their reliance on data processing vendors for core banking products lessened the value of enterprise-wide change control and incident cause analysis. Nevertheless, management did state that the tools available from vendors were difficult to use, at best, or somewhat lacking, at worst; and vendors, in general, were slow to respond to requests.

Question 4

What is/are the key reporting system(s) used?		
	LB	RB
Anecdotal conclusions rather than conclusions supported with empirical data		X
Exception reporting at the production line level, but not consolidated at an executive level		X
Exception reporting is consolidated at an executive committee, but reporting remains in a business silo	X	X
Exception reporting is consolidated at an executive committee, and reporting crosses business silos to provide a holistic perspective	X	
Audit committee	X	X
Audit reports	X	X
GL attestations by management	X	X
Self assessment results	X	X
Customer complaints	X	X
Help desk escalation procedures and problem log reporting	X	X
Operational loss and fraud reporting to executive or board committee	X	X

This question reveals how well the collection of operational risks were reported up through the organization. Where risks can be directly attributed to a given business line, these distinctions often become blurred or overlooked in consolidated reporting formats. Accordingly, Nick Viner, Vice President and Director of Boston Consulting Group stated that, “Though 85% of banks consider payment processing a strategic source of income, only 30% have a method in place to monitor which channels are generating payments and

which channels are being used."[15] Even though the focus of the American Banker article was payments driven revenue, the statement is a good barometer regarding an institution's ability to measure the collective risk that each payment channel (e.g. ATM network) or product (e.g. checking account) brings to the institution.

The same challenges[16] in reporting profitability impede optimal reporting of risk. To be successful, executive reporting of operational must satisfy a number of objectives. Optimal executive reporting should be timely, relevant, and accurate. It should also measure the institution's progress in meeting its goals for operational risk, including the capability to produce forecasts using various scenarios (Federal Reserve SR 95-45, 1995). Also, to remain competitive within the payments business, banks must re-align their executive reporting processes to clearly identify where the best opportunities lie (Global Payments, 2003). Therefore, before asking the sample a question about what operational risks payment activities pose to their organizations, and how they control those risks, it is prudent to understand how the risks are reported within the organization. Better risk reporting systems will generally result in better responses regarding risk.

Responses indicate that key systems for reporting the collective operational risk are less mature than the key measures and controls used to control/mitigate those risks. Reporting systems are fragmented. While each line of business has key reports to manage operational risks within their direct control, the associated operational risks, such as concentration of audit issues, self-assessment results for the entire payments process, disaster recovery vulnerability and readiness, and fraud losses, for example, may follow

[15] Bill Wade, *Wachovia Unit's Goal: Centralize Payment Biz*, American Banker, March 4, 2003
[16] Impediments in risk reporting may include differing reporting systems, payments supporting multiple business units, complex payments products provided by complicated organizations structures

separate reporting lines. In some cases, the reporting lines may formally, or informally, reconnect at an executive level in an attempt to communicate the collective risk.

All in the sample felt challenged with efficiently reporting the enterprise-wide operational risk to executive management and the board. This is consistent with the industry. The LBs have more resources at hand, but also have more complex products and more complicated organizational structures. The RBs are less complex, but have fewer resources to advance reporting. At the smaller banks reporting is more informal.

While this may be acceptable in the near term, the growing expectation is that there should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk. One would expect to see more improved reporting of operational risk to achieve this end.

Question 5

What material risks or events are impacting the risk profile or risk management of payments systems, and how are you addressing these issues?		
	LB	RB
Material decrease in check volume contributed to the decision to outsource check processing. Didn't want to invest in item capture hardware and software upgrades that may not be fully utilized.	X	
Material increase in check fraud, but advances in automated detection systems have reduced actual losses. So even though attempted check fraud continues to climb, successful attempts have flattened over time.	X	X
Material increase in check fraud, but advances in manual detection processes have reduced actual losses. So even though attempted check fraud continues to climb, successful attempts have flattened over time.		X
Movement of payments from paper to electronic payments. Particularly as business customers use ACH more like a demand deposit account. Volume and rate of movement seem to be increasing. Controls for legacy payments applications are application-centric rather than customer-centric, which makes them more challenging to apply to customers using both payment products. Also, seasoned controls for demand accounts are not always included in an ACH application's suite of controls. Bank management is working with their vendors and in-house development staff to address these issues.	X	X
The longer return policy for ACH (60 days) makes ACH more vulnerable to fraud. Working through industry channels to make ACH rules, such as return policy, more like those for demand deposits.	X	X

Controls provided by service providers and vendors of payments applications to mitigate payments fraud are somewhat ungainly and do not seem to be advancing as fast as the tools used by criminals to exploit payments. Purchasing additional software specifically designed for controlling payments fraud seems to be gaining favor as a control solution.	X	X
Other payments fraud such as check kiting, counterfeit checks, and large ATM deposits. Purchasing additional software specifically designed for controlling payments fraud across the different payment products seems to be gaining favor as a control solution.	X	X
Increasing dependence on key vendors, but risk is mitigated through more rigorous vendor management processes.	X	X
Increasing dependence on key vendors. Attempt to mitigate risk through representation on vendor users groups. However, the vendor appears to be less responsive than bank management would like them to be.		X
Business customer creating ACH transactions without an understanding of NACHA[17] rules. Training programs have been launched to help business customers comply with NACHA rules.		X
The demand by business customers for Internet-based funds management systems will result in higher-value transactions being sent through the public network. This risk is mitigated though rigorous security protocols, which they manage in-house.	X	X
The demand by business customers for Internet-based funds management systems will result in higher value transactions being sent through the public network. This risk seems to be mitigated though rigorous security protocols, which they outsource.		X

Question 6

What is the biggest challenge with your payments risk assessment processes and how are you addressing this challenge?		
	LB	RB
Movement of payments from paper to electronic payments systems. The volume of change and the rate of change seem to be increasing. Issues include managing the differences in law with respect to ACH vs. DDA; lacking a physical document, encoding errors at the truncation end can be more difficult to resolve; and emerging issues with ACH bulk returns. Analysis is underway to address these issues.	X	X
Early identification of possible fraud items. Volume of suspects and fraudulent transactions continue to grow. Purchasing additional software specifically designed for controlling payments fraud seems to be gaining favor as a control solution.	X	X
Setting thresholds for ACH activity with respect to ACH credit originators (e.g. payroll deposits). This is more a credit risk, but operational controls in the system are needed to maintain the caps. They try to use customer financial data as a control, but it is difficult to get financial information on ACH credit originators that do not have a lending relationship with the bank.		X
Finding the time and resources to appropriately measure, assess and manage the risk. Will continue to work with staff and investigate automated tools to improve these areas.		X

Responses up to this point indicate that the organizations in the sample are using sound practices to capture and monitor risk within the business units that use payments

[17] ACH is a nationwide electronic payments system used by a large number of depository institutions and corporations.

systems. Therefore, responses regarding material risks represent organizations with fundamental operational risk-management controls already in place within their lines of business[18]. In addition to understanding the material risks faced by the sample, it is also important to understand the material challenges. Question 6 helps illuminate systemic challenges within the payments system that may transcend the specific bank, and require regulatory intervention.

The findings can generally be grouped into four categories: the shift of payments from paper to electronic transactions; operational control challenges within payments processing; the dependence on outsourcers; and Internet-based funds management systems desired by business customers.

Increased fraud attempts are being mitigated through manual and automated systems. However, controls specific to check fraud are not as proven, or even available, within ACH. As payments move from checking to ACH, the standard safeguards for check will have to be re-implemented on ACH processing platforms.

Controls included within the standard payments processing applications are becoming less efficient, while, at the same time, more business customers are converting to electronic payments. Many in the sample are looking at supplementary software solutions, which are specifically designed to detect fraud across payment systems. This seems to suggest that the fraud controls currently available within legacy systems, such as check processing and ACH processing applications, may be at the end of their lifecycle. More nimble and efficient detection and reporting systems are desired. However, since ACH may be considered less profitable than check processing (Celent, 2003), management may

be less motivated to invest in enhanced ACH controls, which may be costly. Also, if ACH's inherent risk was determined using an old business model, ACH may be viewed as a less risky payment conduit than it currently may be. Other operational challenges, such as the differing return policies between check and ACH, the absence of physical documents for research and adjustment, and advancing fraud detection systems within outsourced systems, were common issues noted.

With respect to outsourced systems, many in the sample noted an increased dependence on key vendors providing payments processing applications and processes. The LBs seemed less vulnerable to their key vendors because they had increased their vendor management processes to maintain optimal influence and control. The RBs seemed less able to influence their vendors, because they represented a limited amount of the vendor's customer base. Many RBs leveraged user groups to create the critical mass needed for change. Smaller banks seem to have even less influence over their vendor's control structure and business strategies. Interestingly, only 15% of the top 100 banks outsource, compared to 32% of the medium sized banks, and 44% of community banks.[19] The largest share of customers, by volume, is the group with the least influence over the operational control and business strategies of the vendor. For example, many of the smaller institutions find validating the adequacy of a vendor's security controls particularly challenging due to disclosure issues and the lack of affordable audit resources. They do not have the audit resources of an LB to perform targeted audits at the vendor. While external audits of a vendor are helpful, the targeted nature of the audit may exclude the payments product or channel the serviced bank wanted to validate. Therefore, existing

[18] Basel Committee on Banking Supervision, *Working Paper on the Regulatory Treatment of Operational Risk*, Appendix A, September 2001, for examples of lines of business.

supervisory programs such as Multi-regional Data Processing Servicers (see Appendix II for Details) seems to be a contributing factor to vendor management, in addition to a bank's participation in user's groups, and its own vendor management programs.

The increasing appetite of business customers who desired Internet-based funds management systems was also a growing concern. Additionally, it seems that ACH origination software bundled into PC-based business applications has created a surge in the business customer's use of electronic payments.

This creates stress from two perspectives. Higher-value transactions will be moving through the Internet, which becomes an attractive target for criminals. At the same time, the transactions may be subject to less rigorous controls than a business checking account, because ACH was not originally designed to be a substitute for a business checking account.

Question 7

Have you experienced material fraud losses through your Internet Banking products?		
	LB	RB
No	X	X

Question 8

Have your customers been exposed to identity theft through your Internet Banking products?		
	LB	RB
No	X	X

Question 9

Is fraud resulting from your customer's identity and account information being used to open an unauthorized account at another institution tracked at your institution?		
	LB	RB
No	X	X

[19] M. Arthur Gillis, Should *You Outsource? That depends,* American Banker, December 20th 2002

Questions 7 through 9 focus on the Internet banking platform because of its inherent security risks. Fraud and attacks experienced within electronic retail-payment products have been higher than expected (CERT 2002). The Federal Trade Commission (FTC), which now tracks Internet Related Fraud Complaints, revealed that for 2002, losses relating to Internet fraud represented about a third of overall fraud complaints received (Consumer Sentinel, 2003). It was therefore important to gauge the sample's vulnerability with respect to Internet Banking platforms.

Reponses to the questions regarding material risks (question 5) and challenges specific to the payments system (question 6) touched on concerns regarding the Internet delivery system. This seemed to be more of a concern to regional banking organizations than large banking organizations, as the large banking organizations had more control over and a better understanding of the security controls (e.g. firewalls) used to mitigate this risk.

Identity theft is a specific concern of the Federal Reserve System (Federal Reserve SR 01-11, 2001). As noted in the graphs provided in Appendix I, the adoption rate for Internet delivery (Figure 1) and the rate of identify thefts over the Internet (Figure 2) are rather steep. When factoring in the amount of time it takes to detect identity fraud (figure 3), the rate of identity theft over the Internet may be even steeper. Also, the indirect costs (loss + prevention expenses) relating to identity theft (Figure 4) are already material (34% annual compounded growth rate), and will, in all likelihood, continue to rise at a remarkable rate.

As expected, all respondents considered the Internet banking platform to be high-risk, but none had experienced any material losses. However, none could state with confidence that their Internet banking systems had never been "hacked" for the purposes of

identity theft. Nonetheless, it could be difficult to determine if a hacker had taken customer account data. Particularly, since the objective of identity theft is to steal account information from one bank for the purposes of committing the fraud at another bank.

Similar challenges affect the tracking of identity theft. Regardless of the source of customer's stolen information, whether from the customer, a data processing servicer, the customer's bank, or the institution targeted for fraud – it is difficult to detect the fraudulent information's actual source when the fraud is detected. Regulatory surveillance, such as Suspicious Activity Reporting that was designed to identify trends in bank fraud, has yet to be augmented to capture this type of data. Clearly, improved forensics and tracking systems will be required to better address this issue.

Question 10

How is vendor management factored into the payments process?		
	LB	RB
Management realizes their dependency on vendors within their retail payments process and is increasing vendor management rigor to better address this. To exact more control over their vendors, key performance indicators and actionable key risk indicators have been used to more precisely define the service level agreement between the bank and servicer. Failure to comply with a service level agreement allows bank management to send in one of their representatives to resolve the problem.		X
The institution manages its vendors via contracts and service level agreements that are subject to ongoing review.	X	X
Vendor management is not formally tied into the operational risk management process. However, management is open to the possibility of standardizing their vendor relationship management process with GLBA requirements and then linking both to the operational risk management process.		X
A high reliance is placed on third party reviews and regulatory reports such as MDPS reviews.		X
Vendors are managed across the enterprise, rather than in business silos. Reviews of information security and disaster recovery readiness is completed during the due diligence process and on an ongoing basis (for material vendors). Material vendors are subject to annual audits to ensure security administration and contingency provisions are properly addressed. In some cases, an attestation process had been put in place that requires attestations of compliance be completed to ensure that the vendor's information security and disaster recovery readiness complies with the bank's guidelines.	X	

Responses to previous questions indicate a growing dependence on vendors for payments processing and an increasing trend toward outsourcing. The 1999 Gramm-Leach-Bliley Act heightened regulatory expectations for customer privacy (Regulation P), and the safeguarding of customer information (Federal Reserve SR 01-15, 2001). In addition, the PATRIOT ACT is raising expectations regarding the surveillance of payment systems and anti money-laundering programs (Federal Reserve SR 01-29, 2001). Finally, the September 11, 2001 terrorist attacks have heightened expectations regarding the resiliency of the financial system (i.e. business continuity).[20] It is bank management's responsibly to ensure these guidelines are complied with, even if the bank's processing has been outsourced to a vendor.

When a bank outsources its processing to third party vendor, the bank is still accountable for the internal controls relating to that product (FFIEC, 2000). Regulatory guidelines require institutions to ensure that controls over outsourced information and transaction processing activities are equivalent to those that would be implemented if the activity were conducted internally (Federal Reserve SR 00-04, 2004).

LBs indicated that their vendor management programs successfully mitigated this risk, as they performed due diligence reviews during the vendor selection process. Internal control and operational risk management protocols are then incorporated into the vendor contracts, and ongoing monitoring of vendors ensures that the risks are properly controlled/mitigated.

[20]Joint Press Release, Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Securities and Exchange Commission, New York State Banking Department *Regulators Issue Draft White Paper on Sound Practices To Strengthen the Resilience of the U.S. Financial System*, dated August 30th, 2002

While some of the RBs had standardized their vendor management process by tying vendor contracts to specific control objectives, the majority seemed to use a less formal process to manage their vendors and relied more heavily on "relationship management." It seems that the RB monitoring process was directed more towards production service level agreements, than regulatory compliance with GLBA, for example. In some cases, RB management indicated a heavy reliance on regulatory examinations of data processing vendors to assess compliance with sound internal controls. While bank management is encouraged to use regulatory oversight to supplement its own vendor management routines, it is not meant to replace to validation routines, such as third party audits and other measures. It seems management within the RB group may need to advance their vendor management programs to meet growing regulatory expectations within this area.

Question 11

In management's opinion, is there an effective link between payment-system operational-risk and the other risks monitored by the bank?		
	LB	RB
More effort is needed. While OFAC requirements seem to be covered, more work is needed to ensure compliance with BSA and the PATRIOT ACT specific to ACH transactions.		X
Corporate audit has overall responsibility for monitoring corporate risk and controls. Senior executives participate as part of the corporate risk review committee process.	X	
As operational risk is primarily owned at the business level, any coordination or link between other factors would most likely be coordinated at the executive risk committee level.		X
Effective links are established through various risk committees.	X	X
There is not an effective link between operational risk and other risks within retail payments monitored by the bank. However, the benefits of creating such a link do not currently justify the cost.	X	

Question 11 is an extension of Question 10 regarding the risks associated with vendor management. As noted in the guidance, management must ensure that controls over outsourced information and transaction processing activities are equivalent to those that

would be implemented if the activity were conducted internally. This assumes that the internal processes used by the bank meet minimum regulatory guidelines.

Responses by the sample reflect different levels of governance rigor. Although management desires better reporting of consolidated risk,[21] it has difficulty creating a consolidated picture due to lack of resources, lack of automated tools, and timing issues regarding the availability of data. Management may have to accelerate efforts currently underway to provide timely, accurate and relevant data specific to the collective risks that payment systems bring to the organization. While informal processes may address current expectations, regulators, along with Directorates, have a growing appetite for stronger empirical data to support assessments of the material operational risks facing the financial institution.

Question 12

What material initiatives do you have planned for payments in the near future?		
	LB	RB
Web-based funds management system for business customers.		X
Bring check processing in-house to exploit imaging-based products and reduce dependence on outside vendors.		X
None	X	

Since change impacts risk, it is important to know if material change is expected within payments in the upcoming year. While there were a number of internal projects impacting payments over the last few years, changes to payment systems seem to have slowed down. The entire sample was focused on improving operations at hand, rather than preparing for material shifts in operations. Nonetheless, the shift from paper to electronic

[21] Consolidated risk is the total degree of non-compliance of internal control specific to payment systems. For the purposes of this paper, internal control is defined as a process effected by a bank's Directorate, Management and other personnel designed to provide reasonable assurance regarding the achievement of

payments was noted as a common theme. The growing appetite of business customers for Internet-centric payments-management systems was a common theme among the RBs. Many in the sample want advances in control guidelines specific to ACH, and were somewhat concerned about the move of business customer transactions from check to ACH. Particularly, since ACH was not originally designed to process high-value transactions.

Question 13

Is payment systems risk factored into the Merger & Acquisition (M&A) due diligence process?		
	LB	RB
Yes – generally		X
Yes. Factors for consideration include balancing controls and reconcilement reporting; service level agreements both internal and external; contingency plans and contracts; fraud review systems; write-off history and third party contracts	X	
No		X

The questions up to this point have considered operational risk management of the institution's payments processing environment, including its outsourced relationships. This question was asked to determine how the sample addressed operational risk specific to payments when considering institutions for acquisition.

While all the LBs indicated that their M&A due diligence included an assessment of operational risk specific to payments, the RBs were less clear regarding how they specifically included a payments assessment in their M&A. In some cases, the smaller institutions indicated that their M&A procedures do not include an operational risk assessment specific to payments.

objectives in reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

Question 14

Has the payment risk management process been validated by self-assessments, and if so, did it receive a favorable rating, and if not, what were the issues?		
	LB	RB
Management of these areas routinely prepares a risk self-assessment, and has not identified any significant issues for resolution.	X	
No		X
No; however internal self-assessments done at the business-line level have indicated some items worthy of follow-up actions and/or issues to be addressed during strategic planning.		X

This question relates to the sound practice that an operational risk management framework be subject to effective and comprehensive internal audit.[22] Responses indicate that while audit is involved in assessing pieces of the framework, the framework itself has not been subject to a comprehensive audit. Most in the sample were waiting for their operational risk framework to mature over the next year before conducting an audit of the framework. Overall, it seems that the audit departments were actively overseeing management's projects to design and implement an operational risk framework, rather than supplying an independent assessment of the framework.

V. Conclusions

The purpose of this study was to determine what operational risks retail-payment activities pose to banking organizations, and how they control those risks. Results indicate that there are four key risks: Changing delivery channels and safeguards, fraud, vendor oversight, and operational risk measurement and reporting.

A. Changing Delivery Channels

The migration of business checks to ACH and Internet delivery channels was an issue raised by the bankers surveyed. Proven controls for check processing do not easily

transfer to ACH processing. For example, positive pay controls, (e.g. only pay on check numbers x through y) are not readily available in an ACH processing application. Since ACH debits lack a physical document, they are more difficult to research, which can delay fraud detection. Most of the respondents are reviewing third-party software products to buttress current controls within payments applications to provide a more customer-centric, as opposed to application-centric, perspective of risk.

The growing use of the Internet by business customers to manage and originate payment products is also a concern. Particularly since larger account balances available through a public network are an attractive target to criminals. The Internet's vulnerability to identity theft is also a concern. While none in the sample had experienced a material financial loss or identity theft through the Internet delivery channel, all recognized that the very nature of identity theft makes it difficult to detect. Particularly since the information is generally stolen from one bank, and then used to create fraudulent loans at another bank. While the respondents are considering better ways to detect and track identity theft, the detection and remediation systems may require a collective effort among banks to be effective.

B. Fraud

Concern about fraud prevention was a common theme across a majority of the sample. Respondents were concerned that the advances in fraud detection keep pace with the criminal element that is becoming more sophisticated. Even though most of the sample's fraud experiences have stabilized over the last couple of years, the number of fraud ***attempts*** continues to rise. Respondents did note an increase in fraud within business

[22] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of*

customer accounts. This is a particular concern in cases where business customers are using ACH more like a business checking account.

C. Vendor Oversight

The increasing risk within the payments system, coupled with the increasing dependency on fewer payments processors, emphasizes the need for more rigorous vendor management programs within banks. While the LBs have standardized their due diligence processes during the vendor selection and contract negotiation processes, the procedures seem to become less formal with smaller banks. The same can be said for the sample's ongoing oversight of vendors. Smaller banks have less influence over a vendor's internal control process. They also have less opportunity to validate the adequacy of a vendor's internal-controls. While external audits of service providers are helpful, the audit focus may be so precise that it may exclude the validation of some of the controls within payments products used by smaller banks. Vendors and the banking industry are still trying to find the best way to confirm the adequacy of a vendor's control rigor, without jeopardizing the vendor's internal controls. For example, overly precise disclosures of a vendor's controls could be used by criminals to circumvent those controls. However, the absence of a vendor's internal-control disclosure makes it difficult for bank management to evaluate the adequacy of the vendor's control rigor.

D. Operational Risk Measurement and Reporting

Operational risk management for retail payments is evolving along three fronts:

1. Self-assessments, which require business units to attest to their compliance with an operational risk framework;

Operational Risk, Principle 2.

2. Key performance and risk indicators, which report on the overall health of the payments processes on an ongoing basis; and
3. Loss reporting, which can be used to validate the success of management risk control. For example, a declining trend in losses may indicate risk management effectiveness.

Ideally, all three should be used in tandem, as each serves as an indicator for separate risk dimensions. The self-assessments show a business unit's point-in-time compliance with the framework, the key indicators show a more timely risk profile, and the operational loss-reporting provides validation regarding the success of the control mechanisms.

Responses indicate that while the sample's operational risk measures and controls for payments system are fundamentally sound, executive reporting of the collective risk is evolving. LBs are further along in the development of operational risk metrics, while RBs are in the implementation stage.

The entire sample recognized the benefit of consolidated reporting to the executive officers and directorate, but they all find this a challenge. Key reporting systems are still somewhat fragmented. Management within the smaller institutions indicated that tools to monitor the collective operational risk across payments systems were difficult to use, at best, or somewhat lacking, at worst. For LBs, the complex payment products threaded throughout the lines of business, and the complicated organization structures, make it difficult to produce consolidated reports which are timely, accurate and relevant. Even though the RBs offer less complex products and have a more traditional organizational structure, they lack the resources to purchase and implement holistic reporting tools. To mitigate this risk, management uses executive committees, whose members represent the material business and support units, to collectively determine the consolidated risk profile

facing the organization. Many in the sample desired more effective reporting of consolidated operational-risk at the executive level, and were launching initiatives to achieve that objective.

Overall, while risk management practices are evolving to meet current and emerging risks, more work is needed to effectively report the overall risk to senior management and the Directorate. Uniform operational risk management reporting to the Directorate and regulators could result in better internal controls, enhance regulatory supervision, and reduce regulatory burden on the institution.

Finally, the banks surveyed were not planning major initiatives in the payments area. Their focus was on improving current operations. The shift from paper to electronic delivery channels was expected to continue to evolve. Banks in this sample were focused on customer-centric, rather than application-centric, payments solutions.

References

Bank for International Settlements, Basel Committee on Banking Supervision. September 2001. "Regulatory Treatment of Operational Risk." Working Paper, Appendix A.

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.

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation. July 1999. Assessing Capital Adequacy in Relation to Risk at Large Banking Organizations and Others with Complex Risk Profiles. Supervisory Letter SR99-18.

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation. April 2001. "Identity Theft and Pretext Calling". Supervisory Policy Working Paper 01-11.

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation. September 1995. Inspections of Management Information Systems. Supervisory Letter 95-45.

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation. February 2000. Outsourcing of Information and Transaction Processing. Supervisory Letter 00-04.

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulations. November 1995. Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies. Supervisory Letter SR95-51.

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulations. May 2001. Standards for Safeguarding Customer Information. Supervisory Letter 01-15.

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulations. November 2001. The USA Patriot Act and the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. Supervisory Letter 01-29.

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).

References - continued

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

CERT Centers Software Engineering Institute. August 2002. "Cyber Security Threats to the Financial Industry." FFIEC Presentation.

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

Consumer Sentinel. January 2003. Internet Related Fraud Complaints. Federal Trade Commission Report.

ERisk Report. October 2002. "What Your Board Needs to Know About Risk." Vol. 1, No. 10.

Erisk. 2000. "Case Study: Barings" www.erisk.com

Federal Financial Institutions Examination Council. November 2000. "Risk Management of Outsourced Technology Services."

Federal Reserve System. July 2002. Retail Payments Research Project. http://www.frbservices.org/Key-Initiatives/pdf/RetailPaymentsResearchProject.pdf

Federal Trade Commission. 2001. "Figures and Trends on Identity Theft in Illinois." Identity Theft Victim Complaint Data, Washington DC.

Gerdes, Geoffrey R. and Jack K. Walton II. August 2002. "The Use of Checks and Other Noncash Payment Instruments in the United States." Federal Reserve Bulletin, Vol. 88, No. 8.

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

Givens, Beth. July 2000. "Identity Theft: How It Happens, Its Impact on Victims and Legislative Solutions." Written testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information. Privacy Rights Clearinghouse. www.privacyrights.org/ar/id_theft.htm.

Global Payments. 2003. "The Payments Puzzle, Putting the Pieces Together." Boston Consulting Group.

Group of 10. January 2001. Report on Consolidation in the Financial Sector.

References - continued

Jameson, Rob, August 2002. "Case Study: US Savings & Loan Crisis" ERisk. www.erisk.com

Ledford, Steve. August 2002. "E-Commerce Issues Within the Ever Changing Landscape." The Global Concepts Internet Forum. www.global-concepts.com/.

Lee, Sang. September 4, 2001. "Identity Theft: Impact on the Financial Services Industry." Celent Communications

Moore, Ariana-Michele. July 2002. "Theft: Protecting the Customer – Protecting the Institution." Celent Communications.

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

McNee, Alan, April 2002. "Case Study: Allied Irish Banks" ERisk. www.erisk.com

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.

Raft International PLC. June 2002. Emerging Trends in Operational Risk Within the Financial Services Industry. http://www.raftinternational.com/products/oprisk/oprisk.htm.

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, 1998), Pages 42-52.

U.S. Department of Justice. February 2003. FBI Dismantles Fraud and Money Laundering Ring Exceeding 4 Million in Five States. FBI National Press Office.

U.S. General Accounting Office. March 2002. "Identity Theft: Prevalence and Cost Appear to be Growing." Report to Congressional Requestors (GAO-02-363), Pg. 43.

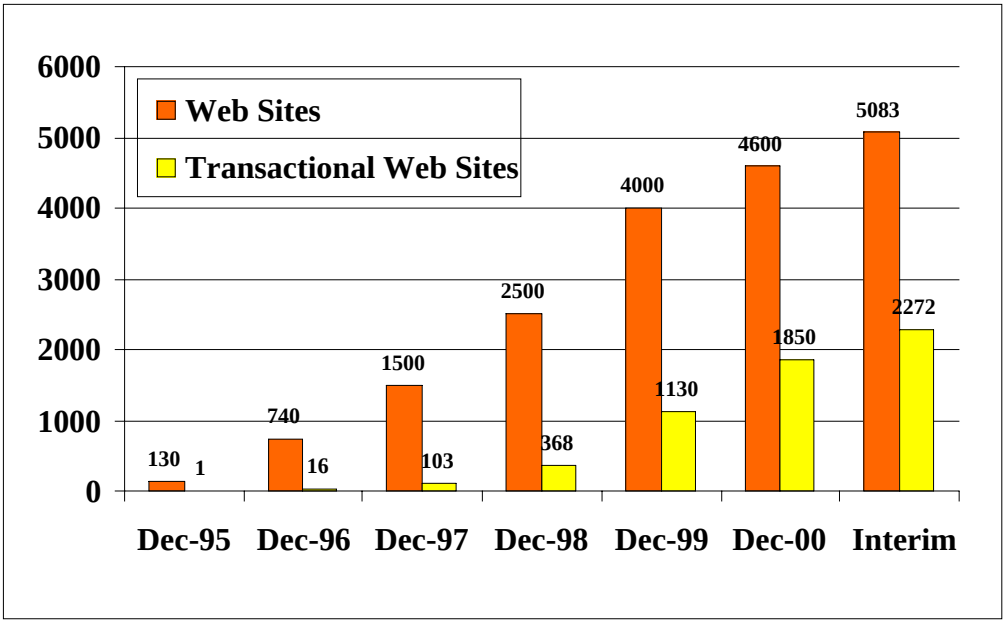
USA Today. February 2003. PNC Cancels Check Cards Following Hacker Incident. Associated Press.

Wade, Bill. March 2003. "Wachovia Unit's Goal: Centralize Payment Biz." American Banker .

Appendix I

Figure 1

Growth Trends of Web Sites for U.S.Banks & Thrifts (as of June 2001)

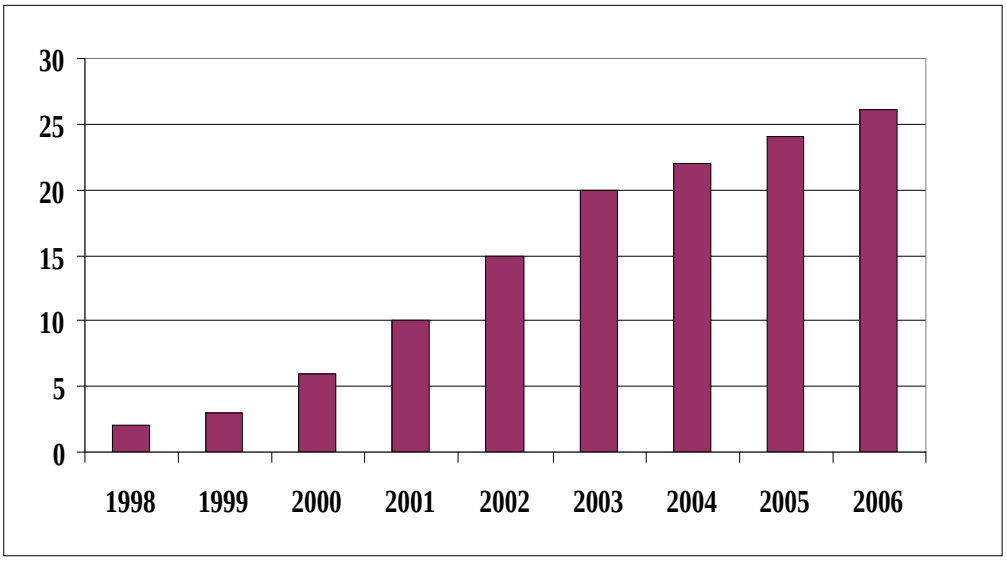


52% of all banks & thrifts have a web site
23% of all banks & thrifts have a transactional web site

Source: FDIC

Figure 2

Est. % of ID Theft Occurring On the Internet

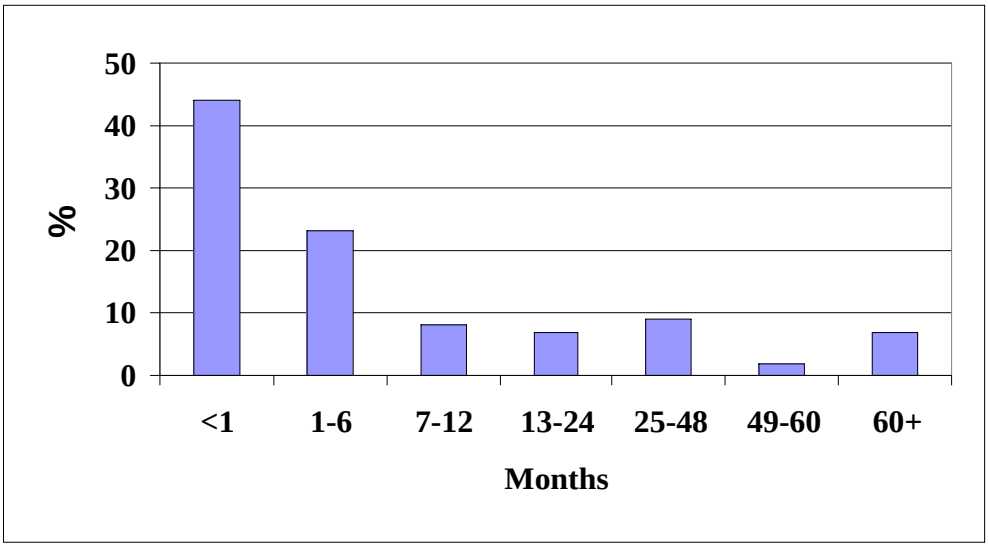


Source: Celent

Appendix III - continued

Figure 3

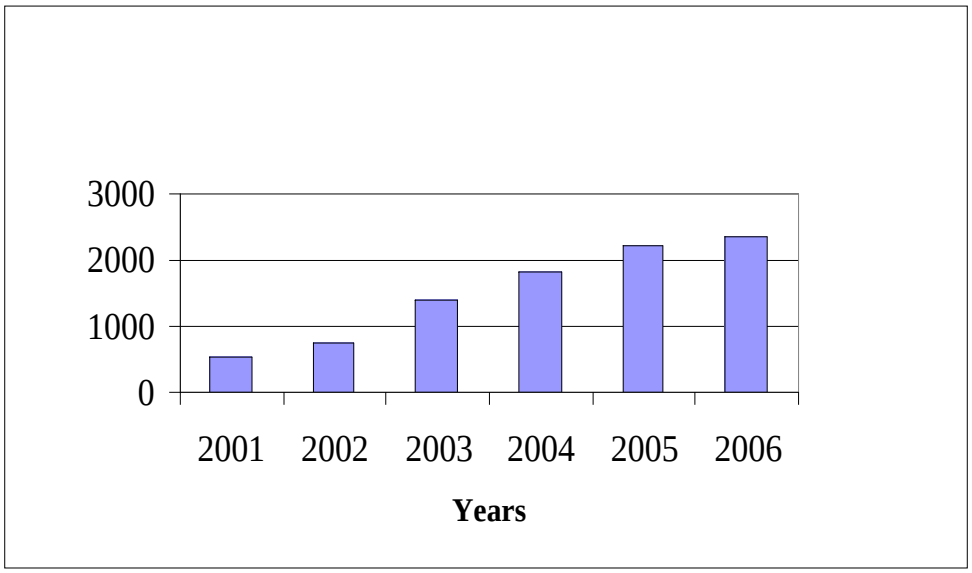
Lag Time In ID Theft Discovery



Source: FTC

Figure 4

Indirect Costs Relating to ID Theft (In Millions)



Source: Celent

Appendix II

Regulatory Supervisory Program – Retail Payments

Supervision and regulation of payments systems comprises on five elements.

1. Information Technology (IT) examinations of the financial institutions conducted by members of the Federal Financial Institutions Examination Council (FFIEC) [23] (e.g. banks, thrifts and credit unions).

2. Targeted examinations of payments products (e.g. ACH).

3. Targeted examinations of payments channels (e.g. ATMs & Internet Banking).

4. IT examinations of Multi-Regional Data Processing Servicers (MDPS) supporting regulated financial institutions.

5. Vendors who provide processing applications for a material number of financial institutions are subject to examination under the Shared Application Software Review program (SASR).

MDPS interagency IT examinations provide a single examination report for the servicer's management and board of directors. Findings noted during the examination are also made available to its serviced institutions by their primary regulator. The program facilitates better communication among regulatory agencies, servicer management, and the serviced financial-institutions. Generally, the total assets serviced by MDPS organizations are more than $20 billion. Additionally, these organizations meet two criteria:

1. Provide major applications for a large number of financial institutions that are regulated by more than one agency;

2. Have a number of data centers located in different geographic regions.

[23] The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and to make recommendations to promote uniformity in the supervision of financial institutions.

The SASR Program was established in 1990 by the FFIEC. IT examiners evaluate the control structure of major software packages used by a wide segment of financial institutions. The scope of the SASR program covers: "turnkey systems"[24] (which, generally, include an integrated mix of both software and hardware), stand-alone custom software (which runs on a commercially standard hardware configuration), and integrated packages. Selection criteria include purchased software to process high-risk applications. These applications include wire transfer, securities transfer, loans, deposits, and general ledger.

The scope of IT examinations are determined by the Uniform Rating System for Information Technology (URSIT).[25] The URSIT rating is based on a risk evaluation of four critical components: Audit, Management, Development and Acquisition, and Support and Delivery (AMDS). Examiners evaluate the functions identified within each component to assess an institution's ability to identify, measure, monitor and control/mitigate information technology risks. Each organization examined for IT is assigned a composite rating based on a scale of "1" through ''5'', with ''1'' representing the highest rating, and least degree of concern. The affect of the associated risks (such as credit, operational, market, reputation, strategic, liquidity, interest rate, and compliance with law and regulatory guidelines) are considered for each of the IT rating components. Additionally, results from targeted examinations of Wholesale Electronic Funds Transfers

[24] Turnkey System "A computer system that is ready to perform a particular task with no further preparation. ("just tun the key and it does it") A turnkey system is sold as a complete package from a single vendor. By contrast, most computer systems are assembled step-by-step by users who obtain hardware and software from various suppliers." *Dictionary of Computer and Internet Terms*, Seventh Edition, Barron's Business Guides.
[25] On January 13, 1999, the Federal Financial Institutions Examination Council (FFIEC) adopted a revised Uniform Rating System for Information Technology (URSIT). The FFIEC published the revised rating system in the Federal Register on January 20, 1999 (64 FR 3109) and is to be used in information technology examinations of all banks and data processing service providers subject to regulatory supervision. Refer to

(EFT) (such as Fedwire[26], CHIPS[27] and SWIFT[28]), Retail EFT (ATM&POS[29]), ACH[30], and FedLine[31] would be factored into the IT rating.

Risk management practices vary considerably among financial institutions and service bureaus depending on their size and sophistication, the nature and complexity of their business activities and their risk profile. Accordingly, the FFIEC recognizes that for less complex information systems, detailed, or highly formalized systems and controls are not required for an organization to receive the higher composite and component ratings.

Federal Reserve SR 98-9 *Uniform Rating System for Information Technology*, Attachment 1 at http://www.federalreserve.gov/boarddocs/SRLETTERS/1999/SR9908.HTM for details.

[26] Fedwire is the Federal Reserve System's nationwide electronic funds and securities transfer network. Fedwire links the 12 Federal Reserve Banks with a large number of depository institutions that maintain reserve or clearing accounts with the Federal Reserve.

[27] The Clearing House Interbank Payment System (CHIPS) is a funds transfer network owned and operated by the New York Clearing House Association (NYCHA) to deliver and receive U.S. dollar payments between banks, domestic and foreign, that have offices located in New York City.

[28] Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a nonprofit cooperative of member banks serving as a worldwide interbank telecommunications network, based in Brussels, Belgium. Unlike EFT systems, SWIFT only provides instructions to move funds.

[29] A POS system transaction is defined as an electronic transfer of funds from a customer's checking or savings account to a merchant's account to pay for goods or services. Transactions are initiated from POS terminals located in department stores, supermarkets, gasoline stations, and other retail outlets. In an electronic POS system, a customer pays for purchases using a plastic card (e.g., ATM card or debit card). The store clerk enters the payment information into the POS terminal and the customer verifies the transaction by entering a PIN. This results in an automatic debit to the customer's account and credits the merchant.

[30] The ACH payments mechanism was developed in the early 1970s as an electronic substitute for paper based payments. Today, the ACH is a nationwide electronic payments system used by a large number of depository institutions and corporations. ACH rules and regulations are established by the National Automated Clearing House Association (NACHA) and the local ACH associations, and are incorporated by reference in the Federal Reserve Bank's ACH operating circulars.

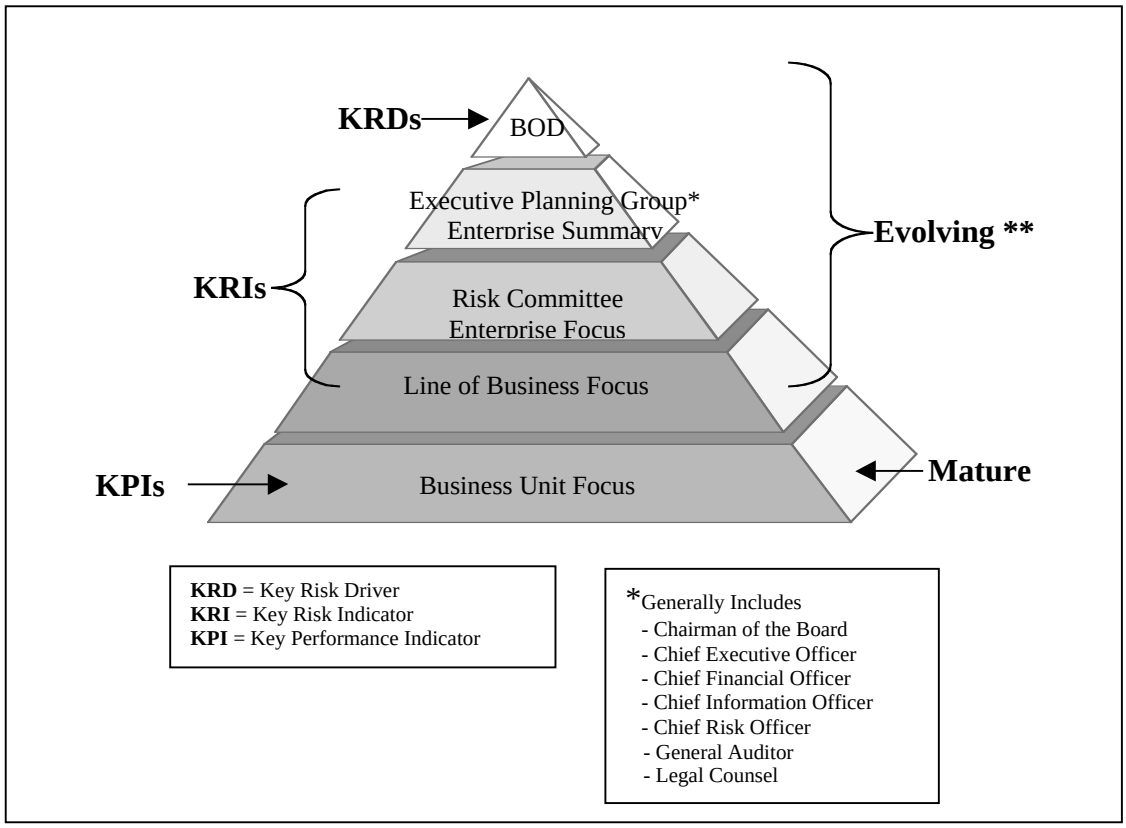
[31] Fedline is the Federal Reserve System's electronic funds and securities transfer system developed for low volume of transfers. Fedline terminals link each Federal Reserve with a large number of depository institutions that maintain reserve or clearing accounts with the Federal Reserve.

Appendix III

Operational Risk-Management Framework – Sound Practices

The operational risk framework is illustrated in Figure 5 as a pyramid of five levels. The pyramid is a helpful illustration, as it helps show how risk is managed from a bottom-up and a top-down perspective. The operational risk framework is derived from supervisory guidance from the Board of Governors of the Federal Reserve System and the Basel Committee on Banking Supervision.

Figure 5 "Operational Risk Framework"



** In a Raft study of emerging trends in operational risk within financial services, they noted that only 3.8% of those who monitor key risk indicators on an ongoing basis in a centralized consolidated manner have done so for more than 2 years.[32]

[32] Raft, *Emerging Trends in Operational Risk with the Financial Services Industry*, pg. 10, June 2002

Throughout this section, the terminology of key performance indicators, key risk indicators, and key risk drivers are provided to bring context to the operational risk framework. Institutions may use a variety of naming conventions to define each of these categories. For example, measures provided by the sample included the following

- Key Performance Measures (production focused),
- Key Risk Indicators (breach of trigger),
- Service Level Agreements (vendor),
- Concentration of Audit Findings (all areas)
- Reconcilement Control Data (exception reporting)
- Trends in Operational Loss Data (fraud), and
- Incident (unintended result) and Resolution (degree of impact and time to fix) Measures.

Nevertheless, it is the conceptual framework, rather than specific definitions, that forms the basis for this discussion.

At the base of the pyramid are the business units. The business units are generally a collection of departments that support a given line of business within a bank. For example, business units supporting a credit card line of business could include a business unit that creates the credit cards, another business unit that mails the credit cards, and yet another business unit that posts the credit card payments. Each of these business units is focused on fulfilling its mission by following a predefined set of procedures. Many of the business missions are production-based (e.g. "post *x* number of customer payments within *y* period of time, but with an error rate < *z*").

These procedures are often converted into Key Performance Indicators (KPIs) to help verify that the department is operating as intended. KPIs often differ from business unit to business unit, but they share a common objective – to determine whether critical business processes are operating as intended.

At the second level of the pyramid are the lines of business. It is not unusual to see larger banks define themselves by lines of business such as retail banking, commercial banking, investment management, and credit card.[33] Each line of business focuses on perfecting its products and processes and managing the attendant risks. With respect to operational risk, this process has not been supported by consistent and timely empirical data. Rather, risk management at this level consists of talented individuals using their collective experiences to govern pockets of operational risk warranting their attention.

Key Risk Indicators (KRIs) help each line of business understand the composite risk of their respective business units. The lines of business assume a broader risk perspective than the business units. Simply stated, a KRI represents a measurement for a situation that may require corrective action. That situation basically represents a "manifestation of risk" that exceeds management's risk appetite, or represents a situation where the return on risk-reward has materially diminished. Corrective action could be anything from shoring up internal controls to altering business strategies. In some cases KPIs feed into KRIs to determine weak links within the line of business's processing chain. This information is supplemented with additional KRIs, such as concentrations of audit issues, increases in the value and volume of fraud, or other operational losses, or

[33] Basel Committee on Banking Supervision, *Working Paper on the Regulatory Treatment of Operational Risk*, dated September 2001, Annex 2, Business Line/Event Types Classification uses this classification.

habitual business continuity problems, for example. To be truly effective, KRIs should be able to answer the following questions:

1. How well are business units adhering to the operational risk framework? Self-assessments completed by each of the business units regarding their compliance with the operational risk framework, buttressed with internal audit reviews of framework compliance, help answer this question.

2. What are the material risk issues that need to be addressed? The key performance indicators, along with profit and loss reporting, help illuminate these issues.
3. How well are control mechanisms working? Declining trends in operational loss are used to help validate the success of the risk management framework.

Nonetheless, it is important to emphasize that at this level management for each business line is charged with more precisely identifying, assessing, monitoring and controlling/mitigating the collective operational risk specific to that particular line of business.

At the third level of the pyramid is the Risk Committee. Banks have long recognized the value of managing aggregate credit and market risk at an executive committee level. Banks are now expanding the scope of this committee to explicitly address operational risk in the committee charter, along with credit, market, and other risks.

While each line of business may be very focused at managing these risks within their respective lines, the executive committee assumes a broader perspective to better understand the collective risk that all the lines of business bring to the enterprise. The challenge with creating meaningful KRIs at this level is that the operational risks within each line of business may be difficult to compare and contrast across business lines. Nonetheless, the committee can still develop a sound understanding of the collective

operational risk if management follows a standard risk framework for reporting the line of business risk to the Executive Committee. The framework should address the following questions:

1. What are the material operational risks within each line of business and what key indicators best identify the level of inherent risk?

2. How effective are the risk mitigation practices specific to those risks, and what key indicators best identify successful risk mitigation practices?

3. What is the level of composite risk, and is the trend improving, stable or eroding? Why is the trend moving in its given direction, and what significant events are affecting the trend?

With this type of information, the committee can more precisely identify, assess, monitor and control/mitigate the collective operational risk represented collectively by all the lines of business.

At the fourth level of the pyramid is the executive planning group. At this level of the pyramid that management can address material operational risks that transcend a given line of business. For example, habitual operational issues within the data processing department result in a business strategy to outsource certain components of in-house computer processing operations. Material increases in fraud may result in a decision to exit certain markets or products. Habitual and material reconcilement issues may result in a buttressing of internal controls. Or, a strategy to ramp up payment activities (ATM, POS, credit card), while at the same time launching a material marketing campaign for on-line banking, may cause unintended stress on the teleprocessing networks and help-desk functions. In each of these examples, the executive planning group would represent an enterprise-wide perspective and have the authority to make the necessary changes.

At the top of the pyramid is the Board of Directors. Sound practices dictate that the Board should be aware of the major aspects of the bank's operational risk and that those risks should be managed as a distinct risk category.[34] While senior management is responsible for implementing an operational risk framework, it is the board's responsibility to ensure that the framework is subject to effective and comprehensive internal audit.[35] Internal audit should ***not*** be directly responsible for operational risk management.[36] However, while sound practices suggest that operational risk management reside outside of internal audit, independent validation of the framework is the ultimate objective. Ultimately, it is the board of directors' responsibility to approve the risk appetite for the financial institution.[37] That appetite roughly translates to the Key Risk Drivers (KRDs) that management is expected to operate within. It is expected that the board will eventually have its own monitoring system (i.e., KRIs) to help ensure that their KRDs are being complied with.

Overall, the framework governed by the board of directors, and implemented by management, should demonstrate effective risk management through the explicit identification, assessment, monitoring and control/mitigation of operational risk.

Use of the framework should help to more clearly identify cause and effect between risk and return, help management to work within this risk appetite, and target higher risk areas that may require a remediation strategy such as re-pricing of products, an exit strategy, or a shoring up of controls.

---

[34] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, dated February 2003, Principle 1
[35] Basel Committee on Banking Supervision, Principle 2
[36] Basel Committee on Banking Supervision, Principle 2
[37] Basel Committee on Banking Supervision, Principle 1, Paragraph 14