



A newsletter published by the Supervision, Regulation & Credit Department for the institutions that it supervises.

IN THIS ISSUE

SVP Observations	1
Alternate Delivery Channels: Why Should You Care?	2
Maintaining Sound Compliance Programs In an Era of Electronic Delivery	6

SVP Observations On... Credit Risk in the Current Economic Expansion

by Michael E. Collins

The nature of banking entails taking a wide array of risks, the most prominent of which is credit risk. As history has shown, serious banking problems have arisen from the failure of banking organizations to avoid or recognize undue credit risk and to create reserves sufficient to absorb risk. The length of the current economic expansion, now in its 89th month, coupled with fierce competition for loans, has led to evidence of complacency in credit standards and aggressive pricing without full regard to credit risk. An overly aggressive response to credit demand has traditionally been a prescription for future problems at banking organizations, adversely impacting their ability to manage through a sectoral or macro downturn or respond appropriately to changing business conditions. A 1997 joint review of credit portfolio management by Robert Morris Associates and First Manhattan Consulting Group disclosed that most banks suffered substantial credit losses in the early 1990's as a result of their decisions during the late 1980's as to which loans to underwrite and which to hold in their portfolio. They noted that banks that have had better credit success than their peers have produced significantly higher and more stable returns to their shareholders.

continued on page 5

Please Route To:

- _____
- _____
- _____
- _____

Y2K

SNEAK A PEEK!

Y2K

Pssst...Do you want to know what to expect from the examiners when you receive your Phase II Year 2000 assessment? To get a copy of the FFIEC Year 2000 Workprogram, visit FFIEC's website at www.ffiec.gov/wp4web.htm

Haven't taken up surfing yet? Then call the FDIC at 1-800-276-6003 and ask for FIL 98-72 with attachments.

Alternate Delivery Channels: Why Should You Care?

by Cynthia L. Course, Sr. Credit Policy Specialist

Alternative delivery channels for banking products and services—channels such as telephone banking, PC banking, and Internet banking—are just for large banks, right? There is no need for a community bank to be concerned about these high-cost technology investments, is there? Wrong, and wrong. Most industry analysts agree that even community bankers should consider investments in technology or risk losing customers to larger competitors. In this article, we will look at three technologies that are receiving increased attention: telephone banking, PC banking, and Internet banking, and will explore the five elements of information technology identified by the federal banking regulators.

Telephone Banking

One may not think that “telephone banking” represents the leading edge in technology. After all, the telephone is an old and relatively simple device, particularly compared to computers. However, a bank can reach almost 100 percent of its customers through the telephone; this cannot be said for other technologies. Furthermore, telephone banking is no longer the stereotypical room filled with customer service representatives. Today, between 20 and 25 percent of total capital investment in technology by U.S. banks is being directed into telephone banking systems. These expenditures can be generally categorized as investments in voice response technology, call centers, or a combination of the two.

Voice response units (VRUs) allow a customer to obtain account information and perform basic transactions, e.g., transfers between accounts and predefined bill payments, without bank employee involvement. Although most VRUs give the caller the option to speak directly with an employee, on a national average, 66 percent of calls are completely handled without human involvement. One of the elements in a successful VRU, one where human in-

tervention is not the immediate selection of choice, is offering a rich menu—allowing customers to perform as many transactions as possible on the telephone. A second element is frontloading important options for the caller, and allowing customers who are familiar with the VRU system to preselect options without listening to the full menu.

Call centers, on the other hand, fulfill the customer’s need to speak to a live person and to get answers to more complex questions that cannot be handled by the VRU. However, call centers have evolved far beyond customer service representatives answering customer’s queries. Call centers now utilize emerging technology such as computer telephony integration (CTI), automatic number identification, and database software designed to capture all of a customer’s interactions with a bank. This allows call center staff to not only answer a customer’s questions but to sell products that specifically target the customer’s perceived needs. Some banks are hiring college graduates to staff their call centers, as the positions

evolve from question-answerers to problem-solvers and marketers.

PC Banking

Many banks have offered their customers some variation of PC banking for the better part of the past decade. Traditionally, large banks delivered PC banking through a proprietary system, with a direct dial-in link from the customer to the bank. These systems are often referred to as “closed systems,” with a central authority (generally the bank) overseeing the content of and access to the network.

Because of the high cost of developing proprietary software, this delivery channel was slow to catch on with smaller banks. In addition, due to the high cost of the early generations of personal com-

Even community bankers should consider investments in technology or risk losing customers to larger competitors.

puters, the general bank customer was not interested in PC banking. Recently, the cost of personal computers has fallen dramatically, and third party vendors have developed PC banking applications that can be tailored to fit almost any bank's legacy system. The lower cost and increased availability, coupled with the security of a closed system, indicate that we probably have not seen the end of proprietary PC banking.

Internet Banking

How many U.S. banks are on the Internet? Unfortunately, being on the Internet is not like holding a bank charter. As the Internet is an "open system," there is no single organization that tracks the number of banks (or other businesses, for that matter) that have web sites. RJE Communications Inc. numbered the banks with a web presence at 1,695 as of August 12, 1998 ('www.bankweb.com');* however, their number includes "banks" such as the "Federal Reserve Bank of _____" and the "Federal Home Loan Bank of _____." Various other sources ('www.moneypage.com', 'www.mybank.com', and 'www.bankstudies.uncc.edu', to name a few) list the banks that they have identified with a web site, generally sorted by state.*

The Third Federal Reserve District is not immune from the proliferation of web sites. Forty percent of the state member banks in the District have established web sites. These banks range in asset size from \$70 million to \$7 billion.

Why have all of these banks decided to establish a presence on the World Wide Web? While many individuals do use the Internet for entertainment, surveys have shown that the vast majority uses it for research. In fact, a Netsmart Research Inc. survey of 1,001 men and women who are on-line at least one hour per week found that 48 percent of the users first go to the Internet when they are considering a major financial decision. What they are looking for is information—information on products and services, pricing on products and services, and availability of products and services.

The Third District state member banks on the Internet are using their web sites primarily for marketing and communication purposes. These nontransactional web sites can be developed for well under \$10,000, with most of the cost related to site design. Along with the lower cost, marketing and

communication sites may have lower risks. However, it is important to remember that risk is not eliminated on these sites. As discussed in John Field's accompanying article, compliance risk is ever present on web sites. Reputation risk also exists, particularly if information on the web site is stale, if the site is maliciously altered by a hacker and not promptly detected and corrected, if the site is frequently unavailable or slow, or if e-mail messages from customers are not returned promptly.

Many espouse that Internet banking is the wave of the future. Without agreeing or disagreeing with these pundits, it would appear that true Internet banking is currently more of a ripple and not yet a wave. According to *Online Banking Report*, there were 196 true Internet banks in the United States at the end of July 1998, providing account balance and transaction detail to retail customers over the Internet. One of those institutions is a state member bank in the Third District.

As noted above, the Internet is an open system, with no single organization providing or monitoring content and security. Many financial institutions and many individuals believe that the security of the Internet is still too weak to allow safe and confidential transactions. Others believe that security is adequate to protect the integrity of both systems and communications. Regardless of your personal beliefs, it is unarguable that Internet banking poses risks that do not exist with Internet marketing or with in-branch, in-person banking.

What's Next?

All of this sounds interesting. So, where do you go from here? First, resist the impulse to become a lemming. Do not blindly follow either the competitor across the street or the competitor across the country off the technology cliff. The first step in determining if alternate delivery channels are for you is to determine how they would help the bank fulfill its mission, goals, and objectives. This leads to considering the first information technology element—Management Processes.

Information Technology Elements

In April 1998, the Board of Governors of the Federal Reserve System issued SR 98-9, *Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations*. This SR

Letter provides risk-focused examination guidance on assessing the risks inherent in information technology. To provide a framework for assessing information technology risks, the Board identified five information technology elements—Management Processes, Architecture, Integrity, Security, and Availability. Examiners will use these elements to analyze the organization’s approach to information technology at the corporate level or at a functional business level. However, examiners will not be assessing these risks in a vacuum. The way that an organization manages its information technology risk will be incorporated into the overall assessment of the six business risks—Operational, Credit, Market, Liquidity, Legal, and Reputational risk.

Management Processes encompass planning, investment, development, execution, and staffing of information technology from a corporate-wide and business-specific perspective. In previous guidance, this was referred to as “organization” or “strategic” risk. Examiners will determine whether the technology strategy for the organization or business unit is consistent with the organization’s overall mission and objectives. They will also determine whether the technology function has effective management processes that will allow it to successfully implement the technology strategy.

In developing the technology strategy, institutions should ensure that the system will meet both current and long-term organizational objectives. This is the **Architecture** element, which, in the past, has also been referred to as “infrastructure” risk. This element includes the hardware, software, and communications systems that allow the system to perform as designed. In assessing the architecture element, examiners will consider the hardware’s capability to run the software, the compatibility and integration of systems with other systems and sources of data, the ability to upgrade, and the adequacy of controls.

Systems may be architecturally sound, but they may not possess **Integrity**, the third information technology element. Integrity refers to the ability of the system to deliver information to the end-

user that is reliable, accurate, and complete. Examiners will review the organization’s policies for and results of information system audits and independent application reviews to determine the structure for ensuring the integrity of information. They will also review the reliability, accuracy, and completeness of information produced by the system.

The fourth information technology element is **Security**, which should be self-explanatory. It is important to remember, however, that security in this sense is all-encompassing, referring to both physical and logical controls that prevent unauthorized access, modification, destruction, or disclosure of information assets during their creation, transmission, processing, maintenance, or storage. Examiners will review security controls to ensure that they are commensurate with the potential for and risk of security breaches from both internal and external sources.

The final information technology element is **Availability**, which attempts to answer the question of whether information is available to end-users on a consistent and timely basis. Here, examiners will be concerned with the availability of information from primary and secondary sources, and the ability of back-up systems, as defined in the institution’s contingency plan, to mitigate business disruption.

Information Technology Elements

- **Management Processes**
- **Architecture**
- **Integrity**
- **Security**
- **Availability**

Final Thoughts on IT Elements

All of these information technology elements exist in institutions that do not use electronic delivery channels for information or products and services. Therefore, management should already be familiar with the terminology and concepts. However, management must fully and continually consider all of these elements when planning, developing, executing, and monitoring electronic delivery channels.

Additional information on these five elements, including how they integrate with the six business risks, can be found in SR Letter 98-9 *Assessment of Information Technology in the Risk-Focused Framework for the Supervision of Community Banks and Large Complex Banking Organizations*. This SR Letter is available at the Board of Governors web site at ‘www.bog.frb.fed.us/boarddocs/SRLETTERS/.’

Alternatively, you should always feel free to call your bank regulator with any questions. Finally, always remember that it is better to resolve issues and questions before the fact rather than during an examination or inspection.

*These websites, which are not affiliated with or authorized by the Federal Reserve System, contain information that may be helpful to you. The Federal Reserve, however, has no control over the information contained therein and cannot guarantee its accuracy. ■

SVP Observations On... Credit Risk in the Current Economic Expansion

continued from page 1

The combination of changing market dynamics, new business opportunities, and new ways to manage portfolio risks has spurred some banks to increase corporate leveraged lending, promote high loan-to-value or sub-prime lending, and loosen credit standards. Other trends include deterioration in protective covenants, extended maturities, increased loan syndications with shortened turn-around times, and competition from new players with different credit cultures, such as investment banks. Moreover, in many cases, bankers and borrowers have yet to quantify the cash flow and credit impact of the year 2000 on corporate and small business borrowers.

Second quarter corporate financial results have already depicted a large number of firms reporting earnings below expectations. Furthermore, the Asian economic crises and increased volatility in equity markets may lead to a lessening of confidence and reduced asset values. This heightens the impact of high risk lending practices, given that many new products and models to manage loan portfolio risk are not market tested. Consequently, bankers must monitor changing financial conditions of their borrowers closely.

Against this backdrop, for some time bank regulators and some trade groups have been sending cautionary signals to the industry in an effort to avoid the magnitude of lending problems here-to-fore associated with the savings and loan crises. As expected, with a rising level of business bankruptcy filings, continued high consumer charge-offs, and diminishing margins from high risk lending, bank supervisors are focusing expanded scrutiny on the adequacy of loan loss reserves. Federal Reserve examiners are also likely to increase their focus on the

adequacy of internal risk rating systems and any migration trends within the "pass" grades as part of their evaluation of credit risk management at large banking organizations.

In a recent survey of several hundred loans, the Federal Reserve found that banks lowered rates on loans in the past two years and are requiring less financial information from borrowers than in the past. Only 20 percent to 30 percent of the loans reviewed included formal projections of the borrower's future performance. An appraisal of credit reviews from examinations of banking organizations conducted in 1998 by this Reserve Bank disclosed that in roughly 53% of the examinations, credit risk was increasing, while the quality of credit risk management was only improving modestly. The OCC has also stepped up supervision of bank lending practices, providing information directly to bank directors on risky lending practices or specific loans. The Federal Reserve warns that, if carried too far, easing lending standards can undermine a bank's financial health, particularly if the economy weakens or the extraordinary performance of business profits or cash flow does not persist.

Given the current market dynamics, banking organizations should reassess their competitive strategy to ensure a profitable and sustainable position and a high level of business performance throughout the economic cycle. A bank's business or credit risk management process is one of its most important assets. Managed prudently, it can create long-term value, allowing banking organizations to support economic growth, serve their communities, and provide an optimum return to shareholders. ■

Maintaining Sound Compliance Programs In An Era Of Electronic Delivery

by John D. Fields, Team Manager

The public's confidence that the deposit and loan information at their bank is both accurate and confidential is one of the cornerstones upon which the banking industry has been built and thrives. This confidence generally remained unshaken in the era of documentation, identification, and examination. However, rapidly evolving changes in electronic technology and commerce have affected both bank product lines and their delivery channels. "Orders to pay," which were traditionally processed in documentary form as checks, are now processed in bits and bytes. Loan applications, which in the past entailed a trip to the bank, can be processed and approved without the customer's feet ever crossing the bank's threshold.

As a result of these efforts and innovations, a mutual system of trust has been established by which banks continue to refine and improve their procedures for consumer compliance, file management, and information retention. To assist in this endeavor, on July 15, 1998 the Federal Financial Institutions Examination Council (FFIEC) issued *Guidance on Electronic Financial Services and Consumer Compliance*, providing guidance on the consumer regulatory implications of emerging electronic banking technologies.

The guidance letter contains two sections: The Compliance Regulatory Environment and The Role of Consumer Compliance in Developing and Implementing Electronic Services. Each of these sections is discussed in more detail below.

It should be noted that this guidance is not "Official Staff Commentary" and does not shield institutions that comply with it from civil liability for violations under the various statutes addressed. Furthermore, as the electronic delivery of products and services continues to evolve, additional explicit guidance may be issued by the regulatory agencies.

Compliance Regulatory Environment

This section summarizes the provisions of the federal consumer protection laws and regulations that address electronic financial services, whether explicitly or implicitly. Included with this guidance are examples of the practical application of existing consumer laws and regulations. This section also references a matrix entitled "Compliance Issues Involving Electronic Services," which is attached to the guidance. This matrix identifies some of the principal compliance issues that should be considered by financial institutions when developing and implementing electronic delivery systems.

The guidance letter assesses how compliance activities under various consumer regulations—such as the Equal Credit Opportunity Act, the Consumer Leasing Act, the Home Mortgage Disclosure

Act, the Electronic Funds Transfer Act, and the advertising of non-deposit investment products—may be affected by emerging technologies. Following are excerpts from this guidance that highlight some of the factors that should be considered when developing electronic product delivery systems. You should refer to the full text of the guidance, which can be found at 'www.ffiec.gov/press.htm', for additional information.

Regulation Z – Truth in Lending: Advertising Requirements. The compliance officer or management should review advertisements for loan products before they are placed on the Internet to determine if they conform to the advertising disclosure requirements of sections 226.16 (open-end credit) and 226.24 (closed-end credit).

For example, if electronic advertisements for consumer loans contain certain "triggering terms," additional disclosures must be made. The list of such triggering terms includes, but is not limited to, the

Banks must consider compliance issues when developing and implementing electronic delivery systems.

amount of any finance charge, the number of payments or period of repayment, and the amount of any payment.

Some financial institutions have placed “loan calculators” on websites to allow prospective borrowers to determine monthly payment amounts for mortgage or consumer loans. Bank management must ensure that such calculation tools comply with the applicable provisions of the regulation.

Fair Housing Act. If a bank advertises loans for purchasing, constructing, improving, repairing, or maintaining a dwelling, the advertisement must contain a facsimile of the Equal Housing Lender logo-type, as prescribed by the regulation, or written text that indicates that the bank is an “equal housing lender.”

Regulation DD – Truth in Savings: Advertising Requirements. Management should review advertisements that directly or indirectly promote the availability of deposit accounts on a website to determine if they comply with section 230.8 of the regulation. If an advertisement states the annual percentage yield (APY) for a deposit product, the following information, to the extent applicable, must be stated clearly and conspicuously:

- If variable rate, a statement that the rate may change after the account is opened.
- The time period that the APY is offered or a statement that the APY is accurate as of a specified date.
- The minimum balance, if any, required to obtain the advertised APY.
- The minimum opening deposit, if any, required to open the account, if greater than the minimum balance necessary to obtain the advertised APY.
- A statement that fees, if any, could reduce the earnings on the account.
- Features of time accounts, including the term, early withdrawal penalties, and required interest payouts.

General Considerations. In addition to ensuring that advertisements meet the accuracy and completeness requirements of the various consumer regulations, banks should develop internal guidelines and procedures to retain documentation of the dates that the advertisements were online. Additionally, bank policies related to information dissemination, security, and confidentiality should be periodically revised.

The Role of Consumer Compliance in Developing and Implementing Electronic Services

The second section of the guidance discusses the importance of involving the compliance officer in the design, development, implementation, and monitoring of electronic banking operations. The compliance officer should develop procedures to minimize compliance risk and to consider the implications of consumer regulations as a component of the institution's overall online banking business or technology program.

Further Regulatory Considerations

Ensuring continued compliance with consumer-related laws and regulations is certainly important. However, bankers active on the Internet must also be aware of operating regulations and public policy considerations that may affect their activities. Two areas that have received increased attention are the display of logos or notices and the disclosure of privacy policies on web sites.

Logos or Notices. The FDIC considers every insured depository institution's home page on the Internet to be an advertisement. Therefore, financial institutions subject to section 328.3 of the Federal Deposit Insurance Act should display the official advertising statement on their home page, unless subject to one of the exceptions contained in that section. Any subsidiary page that contains an advertisement should also display the official advertising statement, unless one of the exceptions applies. In addition, Internet or other sites through which an application can be made on-line may be considered “places of business” under HUD's rules prescribing lobby notices

Disclosure of Privacy Policy. As noted above, the privacy of consumer personal information is an important element of public trust and confidence in depository institutions. Just as the advent of electronic banking has led to new means of collecting and communicating consumer information, it has also led to increased consumer concerns about privacy. Information can be collected on-line through visible means, including applications, transactions, forms, questionnaires, and through undisclosed means, such as “cookies.” As the Internet is an open system, third parties may inadvertently gain access to this sensitive information.

Both the Federal Trade Commission and the FDIC surveyed bank Web sites in 1998, focusing on information collection practices and privacy notifica-

tion. Both agencies concluded that self-regulation efforts to protect the privacy of consumer information were ineffective. For example, the FTC survey revealed that 97 percent of the financial sector Web sites reviewed collected personal information, but only 16 percent provided notice of their information practices.

Information on consumer privacy and the Internet has been published by many government agencies and trade organizations. However, the federal regulatory agencies are currently reluctant to prescribe specific practices for privacy policy notification for Internet banking. Bank management may want to refer to the FDIC's Financial Institutions Letter 86-98, *Online Privacy of Consumer Personal Information*, dated August 17, 1998 for additional guidance in this area.

In Conclusion

Most industry analysts expect that electronic product delivery in financial institutions will continue to expand with increases in customer acceptance and the development of additional and innovative delivery systems. Traditional terminology used in the banking environment, such as "business days" and "written documents" will have to be redefined, due to the constant availability of the Internet and other technological advances. Anticipating these accelerating events, the banking industry should take a proactive stance in information systems management, audit techniques, and compliance risk management procedures related to electronic delivery. Bank management and compliance professionals must be prepared to interpret both existing and new consumer legislation in light of these changes, and must develop and implement effective internal policies that address the privacy and security of customer information.

If, after reviewing existing guidance, you still have questions concerning the application of specific consumer regulations to electronic delivery channels, you should speak with your primary banking regulator directly. At the Federal Reserve Bank of Philadelphia, you can call John Fields, Team Manager, at (215) 574-6044. ■

NEXT ISSUE

Subprime Lending

Insurance Activities

Personal Trust Services

Editor.....Cynthia L. Course

SRC Insights is published quarterly and is distributed to institutions supervised by the Federal Reserve Bank of Philadelphia. The current issue and immediately prior issue of SRC Insights are available at the Federal Reserve Bank of Philadelphia's web site at www.phil.frb.org. Suggestions, comments, and requests for back issues are welcome in writing, by telephone ((215) 574-3760), or by e-mail (Cynthia.Course@phil.frb.org). Please address all correspondence to: Cynthia L. Course, Federal Reserve Bank of Philadelphia, SRC - 7th Floor, Ten Independence Mall, Philadelphia, PA 19106-1574.