



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

IN THIS ISSUE

SVP Commentary	1
Introducing Integrated Information Technology Supervision	2
Reducing the Burden: New CRA and Compliance Examination Frequency for Small Banks	4
Internet Banking Examinations: Practical Guidelines	6

SVP Commentary on... Predatory Lending

by Michael E. Collins

The economic expansion of the 1990s, advances in risk management techniques, and heightened attention to CRA resulting from mega-mergers all contributed to the significant growth in lending to low- and moderate-income borrowers in the 1990s. In addition, lenders began to realize that loans to marginally qualified people could be very profitable if a high enough rate were charged to cover the risks. A significant portion of this lending appears to be in the so-called subprime lending market. This type of lending allowed many low- and moderate-income borrowers to attain the dream of home ownership, which they may not have been able to achieve had they been subject to conventional lending terms. Unfortunately, a portion of this lending may also be considered “predatory.”

Predatory Lending vs. Subprime Lending

Predatory lending, a phrase that inflames passions among legislators, regulators, lenders, and the borrowing public, is receiving increasing attention in the new millennium. However, predatory lending is difficult to define and predatory loans are difficult to identify because they carry many of the same characteristics as suitable loans. The June 20, 2000 joint paper released by the Department of Treasury (“Treasury”) and the Department of Housing and Urban Development (“HUD”) described a predatory lending situation as one where:

“the party that initiates the loan often provides misinformation, manipulates the borrower through aggressive sales tactics, and/or takes advantage of the borrower’s lack of information about the loan terms and their consequences. The results are onerous terms and conditions that the borrower often cannot repay...”

This definition of predatory lending focuses on “information” and “knowledge,” two of the distinguishing elements between subprime lending and predatory lending. Subprime lending generally refers to lending to borrowers who do not qualify for “prime” rates, hence the term “subprime.” These borrowers may have no credit histories, blemished credit histories, or higher debt levels, making them riskier than prime borrowers. Subprime lenders increase informed borrowers’ access to credit, and price loans according to the risk of the borrower.

continued on page 8

Please Route To:

- _____
- _____
- _____
- _____

Introducing Integrated Information Technology Supervision

by Cynthia L. Course, Senior Financial Specialist

Information technology (IT) has become an integral component of bank operations, greatly affecting a bank's financial condition and operational performance. Once a term used to describe only mainframe and back office operations, IT in banking has expanded to encompass distributed processing systems and end-user computers. It has also moved from the realms of transaction processing and financial reporting to transaction initiation, telecommunication, and decision-making.

SR 98-9, *Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations*, broadly defines information technology as "a business resource that is the combination of computers (hardware and software), telecommunications, and information." By this definition, it is clear that information technology affects all of the risks associated with banking today.

Consequently, bank management, auditors, and bank supervisors are concerned with ensuring the quality, reliability, and integrity of banks' and third-party providers' IT systems and the information generated therefrom. Bank supervisors have also realized that examiners can no longer assess information technology operations and risks separate from the overall safety and soundness examination.

Outsourcing IT Activities

As technology moved beyond item processing, as the pace of IT change accelerated, and as the business of banking became more complex, depository institutions began to look toward third parties to provide IT services. Today, many banking organizations outsource all or a part of their information and transaction processing services.

The reasons cited for outsourcing are varied, but generally revolve around cost savings, enhanced service, and lack of in-house expertise. However, while reaping the benefits of lower costs and improved service, the reduced control over outsourced activities also exposes the institution to additional risks.

The Bank Service Company Act permits the federal banking agencies to examine "service providers," those entities that provide information or transaction processing services to insured depository institutions. However, this examination authority in no way relieves a depository institution of its responsibility to maintain appropriate oversight of its vendors and service providers.

The Federal Reserve has developed examination procedures to assess an institution's controls over outsourced activities at service providers. Guidance on these procedures can be found in SR 00-4,

Outsourcing of Information and Transaction Processing, and in section 4060 of the Federal Reserve's *Commercial Bank Examination Manual*.¹ As noted in SR 00-4, the Federal Reserve expects 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. Bank

Controls over outsourced information and activities should be equivalent to those implemented for internal information and activities.

¹ See SR 00-4, *Outsourcing of Information and Transaction Processing*, at <www.federalreserve.gov/boarddocs/SRLETTERS/2000/SR0004.HTM> and *Commercial Bank Examination Manual* at <www.federalreserve.gov/boarddocs/supmanual/default.htm#cbem>. See also the *FFIEC Information Systems Examination Handbook*, which is available for order or download at <www.ffiec.gov/handbook.htm>.

management and the Board must understand the risks inherent in the use of service providers for core processing functions, and the risks associated with selection of the chosen service provider in particular. Consequently, bank management must conduct a risk assessment of the IT activities it proposes to outsource, and must conduct sufficient due diligence to satisfy itself of the service provider's competence and stability, both financially and operationally. As highlighted in the box below, SR 00-4 delineates eight areas that a depository institution must consider when overseeing a domestic service provider. Outsourcing to a service provider located outside the United States presents additional risks that must be considered, including adequate oversight and compliance and information access.

IT Rating Systems

In April 1999, the FFIEC adopted a revised Uniform Rating System for Information Technology (URSIT).² The revised URSIT replaced the Information Systems rating system used by examiners since 1978, and reflected the changing nature of technology and the shift in supervisory approaches from primarily transaction-based supervision to risk-focused supervision.

Today, examiners use URSIT to assess the information technology risks at financial institutions and service providers. The URSIT rating is based on a risk evaluation of four components—Audit, Management, Development and Acquisition, and Support and Delivery. Consistent with risk-focused supervision, in assessing each component examiners focus on the quality of risk management processes to identify, measure, monitor, and control information technology risks. The overall assessment of information technology risk, the composite URSIT rating, is used to identify those banks and service providers that

warrant special supervisory attention. Historically, the URSIT rating has also been factored into the Management component in CAMELS.

Integrated Examinations

Even as the revised URSIT rating system was being developed, the federal bank regulators were working on integrating the safety and soundness and IT examination functions. To facilitate this integration, one of the modifications to the URSIT rating system aligned the rating definitions to bring them in line with the Uniform Financial Institution Rating System (UFIRS), or CAMELS, definitions.

Completing its integration initiative just after the Y2K rollover, the Federal Reserve System issued SR 00-3, *Information Technology Examination Frequency*, on February 29, 2000.³ SR 00-3 eliminated the separate

examination frequency guidelines for information technology examinations, and required that all safety and soundness examinations conducted by the Federal Reserve System include an assessment and evaluation of information technology risks and risk management. This assessment must be conducted whether the information technology activities are conducted in-house or are outsourced.

All institutions, whether conducting IT activities in-

house or outsourcing, will experience some changes. First, the IT examination cycle will now coincide with the safety and soundness examination. The first day letter for the integrated information technology and safety and soundness examination will include IT-related questions, allowing examiners to determine the required IT examination scope before going on-site. At the conclusion of the integrated examination, examiners will issue one report, as-

Considerations in Outsourcing Arrangements

- Risk assessment
- Selection of service provider
- Contracts
- Policies, procedures, and controls
- Ongoing monitoring
- Information access
- Audit
- Contingency plans

² See SR 99-8, *Uniform Rating System for Information Technology*, at <www.federalreserve.gov/boarddocs/SRLETTERS/1999/SR9908.HTM>.

³ See SR 00-3, *Information Technology Examination Frequency*, at <www.federalreserve.gov/boarddocs/SRLETTERS/2000/SR0003.HTM>.

Reducing the Burden: New CRA and Compliance Examination Frequency for Small Banks

by Connie Wallgren, Team Manager

The Gramm-Leach-Bliley Act (the “Act”) changed the frequency of Community Reinvestment Act (CRA) examinations for banks with assets of less than \$250 million that have either a Satisfactory or Outstanding CRA rating by placing the frequency at four and five years, respectively. In the past, examiners conducted CRA examinations simultaneously with compliance examinations, and the Federal Reserve frequency guidelines mandated an interval between compliance examinations of no more than three years. Consequently, the Board of Governors (the “Board”) needed to reevaluate the System’s existing examination frequency schedule.

On July 28, 2000, the Board adopted a revised CRA and Consumer Compliance Examination Frequency Policy for banks with assets of less than \$250 million, placing both examinations on the same frequency schedule for most banks. Also included as part of the revised policy are new “Small Bank Monitoring Procedures.” Examiners will use these procedures during monitoring activities at the midpoint of the interval between combined full risk-focused compliance and CRA examinations. The new policy is effective immediately.

Examination Frequency for Small Banks

The new frequency guidelines are based on three factors—the size of the bank, the bank’s CRA rating, and the bank’s compliance rating. Consumer compliance and CRA examinations for a bank with less than \$250 million

in assets, with a *Satisfactory* CRA rating, and with a compliance rating of either 1 or 2 will be conducted every 48 months. The consumer compliance and CRA examinations for a bank with less than \$250 million in assets, with an *Outstanding* CRA rating, and with a compliance rating of either 1 or 2 will be conducted every 60 months.

If a small bank has a Satisfactory or Outstanding CRA rating, but has a compliance rating of 3, 4, or 5, the frequency of the consumer compliance examination will not be extended. Consumer compliance examinations for these institutions will continue to be conducted at a 12-month interval, in accordance with present Board policy. However, the frequency of the CRA examination will be extended, to 48 months for a small bank with a *Satisfactory* CRA rating and to 60 months for a small bank with an *Outstanding* CRA rating.

The table below summarizes the provisions of the Act and the new examination frequency guidelines. It also clarifies the examination frequency for those small banks that are not eligible for the extended CRA examination frequency due to a less-than-satisfactory CRA rating.

When Does a Small Bank Become a Large Bank?

Examiners will continue to conduct CRA and compliance examinations of banks with assets of \$250 million or more according to present Board policy, every

Examination Frequency for Banks < \$250 million in Assets

CRA Rating	Compliance Rating	
	1 or 2	3, 4, or 5
Outstanding	60 month joint exam	60 month CRA / 12 month Compliance
Satisfactory	48 month joint exam	48 month CRA / 12 month Compliance
Needs to Improve	12 month joint exam	
Substantial Noncompliance	12 month joint exam	

24 months. Consequently, a small bank will understandably be concerned with when it will be deemed a large bank.

State member banks with assets of less than \$250 million on December 31, 1999, and new state member banks whose assets are less than \$250 million on the date of membership are subject to the new CRA examination frequency provisions. A small bank will be deemed to be a large bank and no longer subject to the extended examination frequency once its total assets exceed \$250 million for two consecutive years. Asset size will be based on data reported on the bank's December 31 Report of Condition and Income (Call Report).

Small Bank Monitoring Procedures

The Federal Reserve System has developed a formal monitoring process to supplement the new examination frequency schedule for small banks. Examiners will perform formal monitoring activities at the midpoint of the examination cycle (24 months for banks with *Satisfactory* CRA ratings and 30 months for banks with *Outstanding* CRA ratings). These monitoring activities will focus on the regulations that examiners normally review during a consumer compliance examination, including those related to fair lending. The objective of the monitoring program is twofold:

- to evaluate the operational, structural, and environmental changes between examinations that could affect a bank's overall compliance risk assessment or compliance rating; and
- to determine whether at least a satisfactory compliance rating can continue to be justified at the

time of the monitoring event, or whether a more in-depth review or a full risk-focused consumer compliance examination should be conducted.

Information available at the Reserve Bank will support the basic monitoring activity. This information may be supplemented by telephone interviews, and perhaps the use of a customized questionnaire developed specifically for the institution under review. If sufficient information cannot be obtained through these methods, examiners will conduct an onsite visitation to make an accurate assessment of the bank's compliance posture.

If at the conclusion of the monitoring event the examiner determines that the institution has maintained a satisfactory compliance posture, the Reserve Bank will send a letter to senior management of the bank indicating the same. If the Reserve Bank determines that the monitoring activities, including the on-site visitation, cannot support a conclusion that the bank's compliance posture remains consistent with at least a satisfactory compliance rating, examiners will complete a full risk-focused consumer compliance examination, and a new compliance rating will be assigned.

Questions?

If you have any questions about the new examination frequency schedule for small banks, or would like additional information on this program, please contact Reed Raymond, Assistant Vice President, Consumer Compliance/CRA Examinations Unit at (215) 574-6483 (reed.raymond@phil.frb.org), or Connie Wallgren, Team Manager at (215) 574-6217 (connie.wallgren@phil.frb.org). ■

Do you have questions on Consumer Compliance and CRA issues?

Perhaps *SRC Insights* can resolve your quandary. Consumer Compliance and CRA staff have addressed the following topics in prior editions of *SRC Insights*:

Compliance Implications of Electronic Delivery Systems: Guidance is Coming	Q2 2000
Using Self-Evaluations to Streamline the Fair Lending Examination	Q1 2000
Ready or Not, New PMI Rules Are Here	Q4 1999
Who Needs Assessment Areas, Anyway?	Q3 1999
Federal Reserve Adopts New Interagency Fair Lending Procedures	Q1 1999
Maintaining Sound Compliance Programs in an Era of Electronic Delivery	Q3 1998
Flood Insurance	Q4 1997

Internet Banking Examinations: Practical Guidelines

by Saba Tesfaye, Senior Examiner

As the Internet becomes more prominent, a growing number of depository institutions is offering Internet banking services. According to a study by Online Banking Report (Table 1), the number of banks offering Internet banking increased exponentially in the past five years. In particular, the growth in electronic banking accelerated in 2000 as resources dedicated to Y2K were redirected to e-commerce initiatives. Internet banking is not just for the larger banks. A Grant Thornton survey of community banks revealed that 17 percent of the respondents already offer online banking, and another 47 percent plan to offer it by the end of 2000.

As the number of banks offering Internet banking increases, so does the number of households taking advantage of this new distribution channel. As illustrated in Table 2, several industry analysts agree that use of Internet banking by households will continue to grow exponentially. IDC now projects that within four years, 22.8 million households will bank online.

Regulatory Guidance Takes Various Forms

In response to the rapid growth and increased risks associated with Internet banking, the Federal Reserve has periodically issued guidance over the past several years. This guidance has taken various forms, and has included formal SR Letters, articles in prior editions of *SRC Insights*, and the recent series of Internet Banking Conferences held throughout the Third District. Continuing this pattern, this article provides guidance to the industry on what may be expected when the Federal Reserve examines an Internet banking operation at a state member bank.

The overarching objective of examinations of Internet banking activities is to (1) determine the adequacy of a bank's policies, procedures and internal controls, including audit coverage, related to Internet banking and (2) ensure that Internet banking risks are identified, controlled and monitored on an ongoing basis. The review of Internet banking operations is not a separate examination, but is conducted as part of the full scope safety and soundness examination of the banking organization.

As one would expect, the examiners' review of Internet banking will increase with the level of complexity of the systems and services offered. For example, a trans-

Table 1

	May 1995	May 2000
Financial Institutions with web banking	1	3,000
Financial Institutions with web sites	50	10,000
Web banking users	5,000	7 million
Total online banking users (US)	300,000	11 million
Total online bank web traffic (US)	100,000	18.8 million
Monthly credit apps submitted via web (US)	0	10,000

Source: Online Banking Report, June 16, 2000

Table 2
Projections for Household Banking Online (Millions)

	1999	2000
EMarketer	5.4	8.8
Piper Jaffray	6.1	9.5
Jupiter Communications	9.1	12.0
Dataquest	10.5	14.0
IDC	10.2	15.6

actional system, which permits the user to transfer funds between accounts, pay bills, and conduct other similar activities, will be subject to a more thorough examination review than an information-only system that allows the user to view information but that provides no account inquiry capability. However, since examinations are now risk-focused, the level and depth of the review depends on many factors, such as the level of Internet activity, the degree of outsourcing, and the significance of Internet banking activity to the bank.

Dissecting the Internet Banking Examination Process

Currently, the Internet banking examination process is divided into six areas—(1) Preliminary Review; (2) Policies, Procedures, and Risk Limits; (3) Internal Controls and Security; (4) Audit/Independent Review; (5) Vendors and Outsourcing; and (6) Board Oversight. Each of these areas could be the subject of an entire article. However, the following summary should provide a flavor of the elements that the examiners will consider when reviewing an Internet banking operation.

Preliminary Review. Before beginning the review, the examiner will gather enough information to determine the scope of the examination and the resources required to conduct the review. The examiner will focus on the bank's current and planned Internet banking activities, the bank's involvement in technology development and support, the significance of the bank's electronic banking activities, the level of board oversight, and the adequacy of the risk management process.

Policies, Procedures and Risk Limits. The examiner will review the bank's policies and procedures to determine if they address the risks associated with electronic banking, and are appropriate relative to the size of the bank and the nature and scope of its operations. Policies and procedures should, at the minimum, address issues related to the monitoring of third-party vendors, customer complaints, contingency planning in the event of a disruption, customer education, security, ongoing review of the web site, disclosures, and verification of customer identity.

Internal Controls and Security. Security measures and internal controls are crucial elements in an Internet banking strategy. While the Internet invites broad

opportunities to conduct business through the offering of products and services, its vast geographic realm and open architecture pose material security risks. Security concerns arise from unauthorized access, computer viruses, employee sabotage, loss of transaction information, and difficulties in identifying customers.

As part of this review area, the examiner will ensure that the following are addressed:

- Security evaluation, testing to review content, and stress testing to ensure system reliability and capacity prior to launching the Internet banking system;
- Management reviews of each electronic application for accuracy, confidentiality and integrity of data, system capacity and reliability, and adequacy of virus prevention tools and back-up systems;
- Procedures to monitor vendor systems for vulnerabilities, and implementation of related system patches or upgrades, as appropriate;
- Password administration and effective controls to ensure that only authorized employees have access to sensitive information and applications;
- Effective firewalls; and
- Adequate disaster recovery plans.

Audit/Independent Review. The scope of both the bank's internal and external audit programs should include Internet banking. Consequently, examiners will evaluate the adequacy, effectiveness, and efficiency of the audit coverage of Internet banking systems. For example, examiners will evaluate the audit department's involvement in the development and implementation of the Internet banking system, and its involvement in ongoing penetration testing and intrusion detection. Examiners will also determine whether the audit staff has the appropriate skills to audit Internet banking operations. When a bank outsources its internal audit of Internet banking activities, examiners will evaluate whether the scope of the outsourced audit is adequate.

SVP Commentary on... Predatory Lending

continued from page 1

Predatory lenders, however, take advantage of uninformed consumers. Typically, predatory lending practices involve fraud; harmful sales practices; and/or abusive or deceptive terms and conditions, including excessive fees and interest rates, hidden or undisclosed costs, unnecessary insurance, and deceptive use of balloon payments. However, not all loans exhibiting “unusual” or high-cost terms or conditions are predatory loans. Because predatory lending typically involves an uninformed consumer, each loan must be considered in the context in which it was made.

For example, not all loans that have high interest rates or fees, credit insurance, or balloon payments are predatory loans. Most of the time, these practices allow borrowers access to funds that may otherwise be unavailable. Consider the following:

- Allowing lenders to charge **high interest rates** may be desirable in matching relatively risky borrowers with appropriate lenders. Predatory lending occurs when the higher-than-prevailing interest rates are unrelated to the credit risk of the borrower.
- **Credit insurance** can serve a valid purpose. Mortgage credit insurance may improve credit availability to borrowers who cannot meet the minimum down payment requirements for conventional loans. Mortgage life insurance may also serve a valuable purpose to protect the home of a single wage earner family. However, an implication that single premium credit insurance is required, when in fact it is not required and is nonrefundable, may be indicative of predatory lending.
- **Balloon payments**, when used appropriately, may make it possible for young homeowners with increasing earnings potential to buy their first house, and match payments with their rising income stream. Balloon payments, when used inappropriately, may force a low-income or retired borrower to refinance a loan at even higher costs, continuing the cycle of high-cost refinancings.

Apart from outright fraud and harmful sales practices, predatory lending involves the abuse of lending practices, such as risk-based pricing, credit insurance, and balloon payments, which are generally desirable. For this reason, regulators and legislators are reluctant to outlaw practices that are effective most of the time.

1998 Joint Report of the Board and HUD

In July 1998, the Board of Governors of the Federal Reserve System (the “Board”) and HUD issued a joint report to Congress that included a detailed analysis of the problem of abusive practices in mortgage lending. The Board and HUD recommended a multifaceted approach that would curb predatory lending practices without unduly interfering with the flow of credit, creating unnecessary creditor burden, or narrowing consumers’ options in legitimate transactions. The recommended approach included a mix of legislative action, stronger enforcement of current laws, and nonregulatory strategies such as community outreach and consumer education. However, this report generally focused on reform of the Truth in Lending Act and the Real Estate Settlement Procedures Act. Recent initiatives have become more far-reaching.

Current Initiatives

Predatory lending takes advantage of a group of consumers who can least afford it—those living in low-income communities. Consequently, a wide range of groups is concerned about identifying and preventing predatory lending. It is not possible to list all of the initiatives here. However, the following summarizes some of the more visible initiatives currently underway.

Interagency Task Force on Predatory Lending. In the fall of 1999, the Board of Governors of the Federal Reserve System convened a nine-agency Interagency Task Force on Predatory Lending.¹ The aim of

¹ Participants include five agencies that regulate depository institutions (the Federal Reserve, the OCC, the FDIC, the OTS, and the NCUA), two that regulate housing (HUD and the Office of Federal Housing Enterprise Oversight), and two that regulate or prosecute deceptive trade practices (the Department of Justice and the Federal Trade Commission).

this group is to tighten enforcement of existing standards, to identify predatory practices that might be limited by tightened regulations or legislative changes, and to establish a coordinated attack on predatory practices.

National Task Force on Predatory Lending.

A HUD-Treasury Task Force, the National Task Force on Predatory Lending, was formed in March 2000 to collect information about predatory lending, provide data on the impacts of predatory practices, and make recommendations for legislative action to Congress. The HUD-Treasury Task Force held public hearings in April and May, and issued its report to Congress in June 2000.

FNMA Guidelines. In April 2000, FNMA established anti-predatory lending policies for the loans it purchases from lenders. In part, these policies address predatory practices such as “steering” customers toward more expensive and inappropriate loans, given their financial position; charging excessive fees; offering prepaid single premium credit life insurance; and assessing prepayment penalties. FNMA will not purchase loans from lenders that do not adhere to these policies, thereby reducing the liquidity and potentially the volume of the predatory lending market.

Hearings on the Home Ownership and Equity Protection Act of 1994 (HOEPA). In August and September 2000, the Board of Governors of the Federal Reserve System (the “Board”) held four public hearings on predatory lending practices in the home equity lending market. During these hearings, the Board invited comment on what approaches it might consider in exercising its regulatory authority under HOEPA. The Board also solicited written comment on approaches to dealing with predatory lending practices. The Board will give full weight to the oral and written comments as it reviews its regulatory authority under HOEPA and the Board’s Regulation Z, “Truth in Lending.”

Congressional Action. In addition to these regulatory studies, policies, and guidelines, Congress is considering legislative action to eliminate predatory lending practices. Congress is currently considering at least four bills related to predatory lending, two introduced in the House of Representatives and two introduced in the Senate. The House bills—H.R. 3901 “The Anti-Predatory Lending Act of 2000” and H.R. 4250 “Predatory Lending Consumer Protection Act of 2000”—have been re-

ferred to the Committee on Banking and Financial Services. The two Senate bills—S.2405 “Predatory Lending Deterrence Act” and S.2415 “Predatory Lending Consumer Protection Act of 2000”—have been referred to the Committee on Banking, Housing, and Urban Affairs.

State Action. The states have also begun to address predatory lending activities within their borders. In 1999, North Carolina adopted the “Predatory Lending Law,” which became effective July 2000. Many states are using this law as a model for proposed legislation and/or regulation. Some states, including New Jersey, focus on enforcing existing state laws that provide consumers with protection against some predatory lending practices.

However, state initiatives with perhaps the most potential focus on educating the public. When individuals understand the lending process and their rights and responsibilities as borrowers, they are less likely to sign agreements that are not in their best interests. Some states, including Indiana and New Jersey, are working with state education departments to ensure that basic financial education is an integral part of every student’s high school education. Other states, such as New York, are working with community groups, and hold outreach programs in the neighborhoods most likely to be victimized by predatory lending.

Banks and Predatory Lending

Nondepository institutions conduct the majority of subprime lending. In 1998, 239 subprime lenders reported data under the Home Mortgage Disclosure Act, and only 36 of those institutions were banks or subsidiaries of banks and savings and loans that were regulated by the federal banking regulators. Furthermore, most anecdotal reports and legal cases concerning predatory lending have involved subprime lenders. Considering the level of oversight by federal banking regulators, and the banking industry’s low level of participation in subprime lending, it is unlikely that a bank would become intentionally involved in predatory lending.

To avoid inadvertently becoming involved in predatory lending, bankers must perform due diligence on their third-party partners. Best practices may include:

- **Spotting predatory practices** – Bank staff must be able to identify potential predatory lending

practices, recognizing that there is a difference between acceptable subprime lending practices and unacceptable predatory lending practices.

- **Monitoring third-party partners** – A bank must monitor brokers, loan originators, and other sources from which it accepts credit applications. It must look carefully at the practices of loan originators to ensure that the originator does not condone or conduct predatory lending.
- **Monitoring subsidiaries and affiliates** – Today, banks have complex business structures, with subsidiaries and affiliates that operate geographically and functionally apart from headquarters. Many of these subsidiaries and affiliates operate

with nonbanking cultures. Banks should evaluate whether credit subsidiaries and affiliates that are producing high short-term profits and that resist scrutiny from the corporate compliance unit are involved in predatory lending.

The misdeeds of a small group of predatory lenders will have implications for the banking industry as a whole. Predatory lending is receiving scrutiny at the highest levels of federal and state government, and aggressive enforcement and even new legislation may be inevitable. I encourage you to be vigilant in your internal operations and in your dealings with third parties and customers to ensure that your organization does not inadvertently become a predatory lender. ■

Introducing Integrated Information Technology Supervision

continued from page 3

sessing IT and safety and soundness risks and providing comment on deficiencies, if necessary.

An institution that has in-house information technology processing or outsources only a small segment of its activities will experience few changes in the examination process. IT examiners will continue to conduct the IT assessments of these institutions, and the scope of the integrated examinations will be sufficient to allow the examiner to assign a composite URSIT rating. Based on the scope of the assessment, individual URSIT component ratings may be updated at the examiner's discretion.

An institution that outsources its core processing

functions (see box) may experience some changes in its examination process. Initially, IT examiners will assist

Characteristics of “Core Processing Functions”

- Applications that process portfolios representing a significant dollar amount of the institution's assets
- Applications that process a high dollar volume of transactions
- Functions that cannot be performed manually, and where tolerance to interruption is very low and cost of interruption is very high
- Applications that are vital to the successful continuance of a primary business activity

safety and soundness examiners in performing an assessment of the IT risks as part of the safety and soundness examination program, utilizing section 4060 of the *Commercial Bank Examination Manual*. Ultimately, safety and soundness examiners will receive Federal Reserve System training to conduct the IT risk assessment, and will consult with IT examiners when issues are identified. The IT assessment will focus on the adequacy of the institution's oversight of the service providers for its core processing functions. It will also include a

review of any significant in-house IT activities. Generally, examiners will not assign a URSIT rating when an institution outsources all or a significant portion of its core pro-

cessing functions; however, the assessment of IT activities will be reflected in the components of the CAMELS rating. The effect of the IT assessment may not be limited to the Management rating; depending on the examination findings, the IT assessment may affect financial risks and other ratings as well.

The Federal Reserve Bank of Philadelphia will implement the integrated supervision processes over the

course of 2000 during regularly scheduled safety and soundness examinations. For additional information on integrated supervision, you can visit any of the referenced web sites for SR letters and examination manuals. You can also discuss your questions with your institution's central point of contact at the Federal Reserve Bank of Philadelphia, or with the examiner-in-charge of the examination. Alternately, you can contact John V. Mendell, Manager, at 215-574-4139 (john.mendell@phil.frb.org). ■

Internet Banking Examinations: Practical Guidelines

continued from page 7

Vendors and Outsourcing. Banking organizations are increasingly relying on services provided by other entities to support a range of banking operations. While outsourcing helps banks manage data processing and personnel costs and provides resources that are not available internally, the reduced operational control over outsourced activities exposes the bank to additional risks. On February 29, 2000, the Federal Reserve System released SR Letter 00-4, *Outsourcing of Information and Transactional Processing*, which provides guidance in managing risks related to outsourced services.¹

In conducting this review, the examiner will determine if management has completed sufficient due diligence before engaging a vendor. The due diligence review should consider the financial strength, reputation, and viability of the vendor; the vendor's commitment to ongoing enhancements and security features of the product; and the ease of interface between the product and the bank's core processing system.

Management and legal counsel of the bank should review the terms and conditions of vendor contracts, and examiners will evaluate vendor contracts to ensure that they clearly define the responsibilities of both parties. Gen-

erally, these contracts should include provisions related to insurance, termination rights, disaster recovery capabilities, data and system ownership and access, performance clauses, liability for delayed or erroneous transactions, and institution access to internal and external audits, among others. The examiners will also determine if the bank has an appropriate vendor oversight program in place to monitor the vendor's financial condition and performance on an ongoing basis.

Board Oversight. Examiners, as well as customers and shareholders, expect the Board of Directors to provide adequate resources to protect the bank against operational and other risks. Consequently, the Board plays a critical role in providing effective oversight of the Internet banking product, from start to finish.

Before launching an Internet banking initiative, the Board and management should choose a product and technology that is consistent with the business objectives outlined in the bank's strategic plan. The Board should also consider whether adequate resources are available to identify, monitor, and control risks in the Internet banking business. Once a web site is operational, the Board should also approve any significant changes to the bank's web site.

During this review, the examiners will ensure that the bank has sufficient staff with technical expertise to operate and manage its online banking operations consis-

¹ See SR 00-4, *Outsourcing of Information and Transactional Processing*, at <www.federalreserve.gov/boarddocs/SRLETTERS/2000/SR0004.HTM>.

tent with the complexity of the system. The examiner will also ensure that the Board of Directors has approved each of the electronic banking services, based on a written plan that includes cost/benefit, risk, and financial impact analyses.

Conclusion

This article highlights only some of the major review areas, and it should not be considered all-inclusive. Bankers should expect to see additional guidance related to Internet banking as regulators continue to direct their efforts to keep abreast of the rapid changes in technological advancements and privacy issues in Internet banking. For additional information on the Federal Reserve Bank of Philadelphia's supervision of Internet banking, please contact Saba Tesfaye, Senior Examiner, at (215) 574-3487 (saba.tesfaye@phil.frb.org). ■

NEXT ISSUE

Consumer Compliance Update

Supervisory Implications of Subprime Lending

Editor.....Cynthia L. Course

SRC Insights is published quarterly and is distributed to institutions supervised by the Federal Reserve Bank of Philadelphia. The current and prior issues 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.