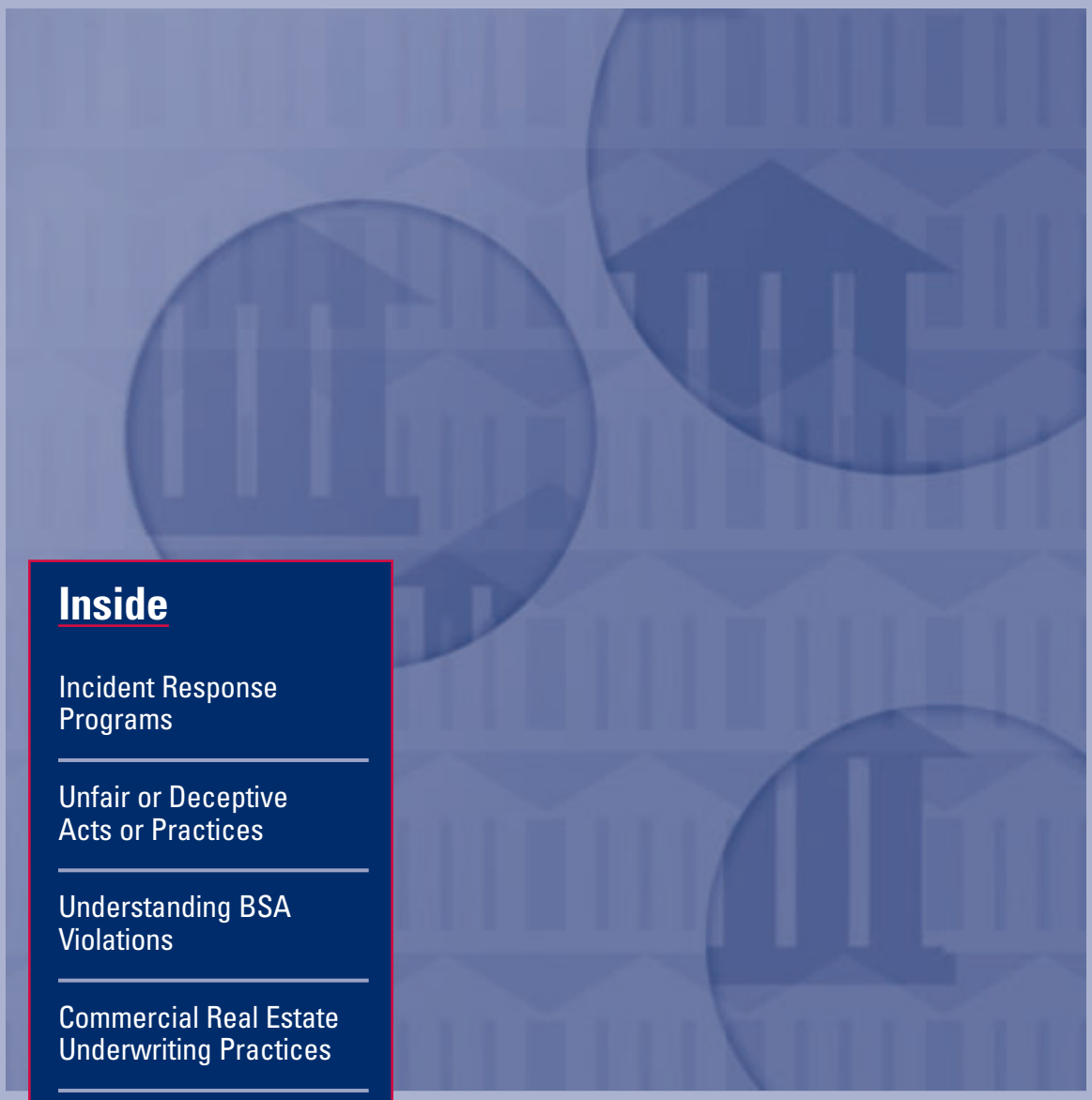
Supervisory Insights

Devoted to Advancing the Practice of Bank Supervision

Vol. 3, Issue 2 Winter 2006



Inside

FDIC

Supervisory Insights

Supervisory Insights is published by the Division of Supervision and Consumer Protection of the Federal Deposit Insurance Corporation to promote sound principles and best practices for bank supervision.

Sheila C. Bair
Chairman, FDIC

Sandra L. Thompson
Director, Division of Supervision and Consumer Protection

Supervisory Insights is available online by visiting the FDIC's website at www.fdic.gov. To provide comments or suggestions for future articles, to request permission to reprint individual articles, or to request print copies, send an e-mail to SupervisoryJournal@fdic.gov.

Issue at a Glance

Volume 3, Issue 2 Winter 2006

Articles

Regular Features

Letter from the Director

It used to be that banks spent more money on protecting the cash they held in their vaults than on anything else. The bars on the windows, security guards in the lobby, and armored cars were familiar signs of how important it was to protect the cash. These days, we know that another critical asset for a bank to protect is data.

Banks hold valuable data that, when compromised, allow criminals to steal an individual's identity and drain financial accounts. The potential for large financial gain has driven the demand by identity thieves for data. There are even secondary markets where thieves can purchase or trade data in mass quantities. There are people in the data theft industry whose "job" it is to obtain and aggregate as much data as they can. Others operate the elaborate black market operations where data can be bought and sold. And other participants are the actual end-users of the stolen information. Whether by manufacturing duplicate credit or debit cards, applying for credit in someone else's name, or using stolen online banking IDs and passwords to access someone's cash by originating transfers, the end-users are the criminals who actually convert the data into cash.

There are many reasons for banks to safeguard data. There are, of course, the regulatory requirements. In 2001, the Federal banking agencies implemented section 501(b) of the Gramm-Leach-Bliley Act by promulgating *Guidelines Establishing Standards for Safeguarding Customer Information.* The objectives of the guidelines and of the written information-security program they require are to (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. In addition, the guidelines require financial institutions to ensure that service providers with whom they contract implement a security program designed to meet the guidelines' objectives. Other laws, such as the Fair and Accurate Credit Transactions Act of 2003 and the USA PATRIOT Act, also require financial institutions to have in place strong policies and programs to safeguard customer data.

Another reason to protect customer data is to avoid financial losses to the bank. The costs associated with a data compromise can be great. They range from expensive insurance claims, to investigation and remediation costs, to the cost of providing free monitoring services for those affected. As important, however, banks need to safeguard data to protect against harm to their reputation and a loss of consumer confidence. If bank customers feel their bank cannot be trusted to protect their confidential information, they will go somewhere else. Although it has not yet happened to a financial institution, companies in other industries have gone out of business because of serious data breaches.

Everyone has a responsibility in safeguarding data. Financial institutions and their technology service providers have a legal duty to protect data, but consumers also have a responsibility to protect their own information. The FDIC has sponsored a number of symposiums around the country to educate consumers about the need to protect personal and confidential information from compromise. We advise consumers to always protect their Social Security number, credit card and debit card numbers, personal identification numbers, passwords, and other personal information. They should also protect their incoming and outgoing mail, properly discard any trash that contains personal or financial information, and keep a close watch on bank

account statements and credit card bills for any abnormalities.

The FDIC also has safeguards in place to protect our confidential data. As the steward of the deposit insurance fund and primary supervisor of more than 5,200 banks, the FDIC plays a vital role in maintaining confidence in the banking industry. In August, the FDIC issued updated procedures to examination staff as a reminder of the importance of safeguarding examination information—whether in paper, electronic, or other form. The updated procedures cover all documentation acquired or created in connection with a bank examination, such as reports of examination, examination work papers, bank information, and, especially, any sensitive bank customer information that may be gathered as part of a bank examination. The updated procedures (1) specify minimum standards for safeguarding examination information, including technical, physical, and administrative safeguards; (2) provide guidance for the implementation of an Information Security Incident Response Program with required procedures if an actual or suspected loss, theft, or unauthorized access of confidential or sensitive examination information is detected; and (3) incorporate recently issued guidance from the U. S. Office of Management and Budget requiring that security incidents involving personally identifiable information be reported within one hour after discovery.

The FDIC recognizes that even the best information security program may not prevent every incident. A critical feature of information security programs must be a plan for the bank to respond when incidents of unauthorized access to sensitive customer information maintained by the institution or its service providers occur. An incident response program provides a preplanned framework for dealing with the aftermath of a security breach or attack. In this issue of ***Supervisory Insights,*** "Incident Response Programs: Don't Get Caught Without One" highlights the importance of incident response programs and provides information on required content and best practices banks may consider when developing effective response programs.

We encourage our readers to continue to provide comments on articles, to ask follow-up questions, and to suggest topics for future issues. All comments, questions, and suggestions should be sent to SupervisoryJournal@fdic.gov.

Sandra L. Thompson
Director, Division of Supervision and Consumer Protection

Incident Response Programs: Don't Get Caught Without One

Everyone is familiar with the old adage "Time is money." In the Information Age, data may be just as good. Reports of data compromises and security breaches at organizations ranging from universities and retail companies to financial institutions and government agencies provide evidence of the ingenuity of Internet hackers, criminal organizations, and dishonest insiders obtaining and profiting from sensitive customer information. Whether a network security breach compromising millions of credit card accounts or a lost computer tape containing names, addresses, and Social Security numbers of thousands of individuals, a security incident can damage corporate reputations, cause financial losses, and enable identity theft.

Banks are increasingly becoming prime targets for attack because they hold valuable data that, when compromised, may lead to identity theft and financial loss. This environment places significant demands on a bank's information security program to identify and prevent vulnerabilities that could result in successful attacks on sensitive customer information held by the bank. The rapid adoption of the Internet as a delivery channel for electronic commerce coupled with prevalent and highly publicized vulnerabilities in popular hardware and software have presented serious security challenges to the banking industry. In this high-risk environment, it is very likely that a bank will, at some point, need to respond to security incidents affecting its customers.

To mitigate the negative effects of security breaches, organizations are finding it necessary to develop formal incident response programs (IRPs).[1] However, at a time when organizations need to be most prepared, many banks are finding it challenging to assemble an IRP that not only meets minimum requirements (as prescribed by Federal bank regulators), but also provides for an effective methodology to manage security incidents for the benefit of the bank and its customers. In response to these challenges, this article highlights the importance of IRPs to a bank's information security program and provides information on required content and best practices banks may consider when developing effective response programs.

The Importance of an Incident Response Program

A bank's ability to respond to security incidents in a planned and coordinated fashion is important to the success of its information security program. While IRPs are important for many reasons, three are highlighted in this article.

First, though incident prevention is important, focusing solely on prevention may not be enough to insulate a bank from the effects of a security breach. Despite the industry's efforts at identifying and correcting security vulnerabilities, every bank is susceptible to weaknesses such as improperly configured systems, software vulnerabilities, and zero-day exploits.[2] Compounding the problem is the difficulty an organization experiences in sustaining a "fully secured" posture. Over the long term, a large amount of resources (time, money, personnel, and expertise) is needed to maintain security commensurate with all potential vulnerabilities. Inevitably, an organization faces a point of diminishing returns whereby the extra resources

[1] In its simplest form, an IRP is an organized approach to addressing and managing the aftermath of a security breach or attack.

[2] A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

applied to incident prevention bring a lesser amount of security value. Even the best information security program may not identify every vulnerability and prevent every incident, so banks are best served by incorporating formal incident response planning to complement strong prevention measures. In the event management's efforts do not prevent all security incidents (for whatever reason), IRPs are necessary to reduce the sustained damage to the bank.

Second, regulatory agencies have recognized the value of IRPs and have mandated that certain incident response requirements be included in a bank's information security program. In March 2001, the FDIC, the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the Board of Governors of the Federal Reserve System (FRB) (collectively, the Federal bank regulatory agencies) jointly issued guidelines establishing standards for safeguarding customer information, as required by the Gramm-Leach-Bliley Act of 1999.[3] These standards require banks to adopt response programs as a security measure. In April 2005, the Federal bank regulatory agencies issued interpretive guidance regarding response programs.[4] This additional guidance describes IRPs and prescribes standard procedures that should be included in IRPs. In addition to Federal regulation in this area, at least 32 states have passed laws requiring that individuals be notified of a breach in the security of computerized personal information.[5] Therefore, the increased regulatory attention devoted to incident response has made the development of IRPs a legal necessity.

Finally, IRPs are in the best interests of the bank. A well-developed IRP that is integrated into an overall information security program strengthens the institution in a variety of ways. Perhaps most important, IRPs help the bank contain the damage resulting from a security breach and lessen its downstream effect. Timely and decisive action can also limit the harm to the bank's reputation, reduce negative publicity, and help the bank identify and remedy the underlying causes of the security incident so that mistakes are not destined to be repeated.

Elements of an Incident Response Program

Although the specific content of an IRP will differ among financial institutions, each IRP should revolve around the minimum procedural requirements prescribed by the Federal bank regulatory agencies. Beyond this fundamental content, however, strong financial institution management teams also incorporate industry best practices to further refine and enhance their IRP. In general, the overall comprehensiveness of an IRP should be commensurate with an institution's administrative, technical, and organizational complexity.

Minimum Requirements

The minimum required procedures addressed in the April 2005 interpretive guidance can be categorized into two

[3] Appendix B to Part 364 of the FDIC Rules and Regulations at www.fdic.gov/regulations/laws/rules/2000-8660.html#2000appendixbtopart364 and FDIC FIL-22-2001, Guidelines Establishing Standards for Safeguarding Customer Information, issued March 14, 2001. Also refer to 12 CFR 30, App. B (OCC); 12 CFR 208, App. D-2 and 12 CFR 225, App. F (FRB); and 12 CFR 570, App. B (OTS).

[4] FDIC FIL-27-2005, Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued April 1, 2005, www.fdic.gov/news/news/financial/2005/fil2705.html. Also refer to 12 CFR 30, App. B (OCC); 12 CFR 208, App. D-2 and 12 CFR 225, App. F (FRB); 12 CFR 364, App. B (FDIC); and 12 CFR 570, App. B (OTS).

[5] "State Security Breach Notification Laws (as of June 2006)," September 15, 2006, www.thecyberangel.com/StSecBrchNotifLaw.doc.

Incident Response Programs

continued from pg. 5

broad areas: "reaction" and "notification." In general, reaction procedures are the initial actions taken once a compromise has been identified. Notification procedures are relatively straightforward and involve communicating the details or events of the incident to interested parties; however, they may also involve some reporting requirements. Figure 1 lists the minimum required procedures of an IRP as discussed in the April 2005 interpretive guidance.

Reaction Procedures

Assessing security incidents and identifying the unauthorized access to or misuse of customer information essentially involve organizing and developing a documented risk assessment process for determining the nature and scope of the security event. The goal is to efficiently determine the scope and magnitude of the security incident and identify whether customer information has been compromised.

Containing and controlling the security incident involves preventing any further access to or misuse of customer information or customer information systems. As there are a variety of potential threats to customer information, organizations should anticipate the ones that are more likely to occur and develop response and containment procedures commensurate with the likelihood of and the potential damage from such threats. An institution's information security risk assessment can be useful in identifying some of these potential threats. The containment procedures developed should focus on responding to and minimizing potential damage from the threats identified. Not every incident can be anticipated, but institutions should at least develop containment procedures for reasonably foreseeable incidents.

Notification Procedures

An institution should notify its primary Federal regulator as soon as it becomes aware of the unauthorized access to or misuse of sensitive customer information or customer information systems. Notifying the regulatory agency will help it determine the potential for broader ramifications of the incident, especially if the incident involves a service provider, as well as assess the effectiveness of the institution's IRP.

Institutions should develop procedures for notifying law enforcement agencies and filing SARs in accordance with their primary Federal regulator's requirements.[6] Law enforcement agencies may serve as an additional resource in handling and documenting the incident. Institutions should also establish procedures for filing SARs in a timely manner

Figure 1

Minimum Requirements

Develop reaction procedures for

- assessing security incidents that have occurred;
- identifying the customer information and information systems that have been accessed or misused; and
- containing and controlling the security incident.

Establish notification procedures for

- the institution's primary Federal regulator;
- appropriate law enforcement agencies (and filing Suspicious Activity Reports [SARs], if necessary); and
- affected customers.

[6] An institution's obligation to file a SAR is specified in the regulations of its primary Federal regulator. Refer to 12 CFR 21.11 (OCC), 12 CFR 208.62 (FRB), 12 CFR 353 (FDIC), and 12 CFR 563.180 (OTS).

because regulations impose relatively quick filing deadlines. The SAR form[7] itself may serve as a resource in the reporting process, as it contains specific instructions and thresholds for when to file a report. The SAR form instructions also clarify what constitutes a "computer intrusion" for filing purposes. Defining procedures for notifying law enforcement agencies and filing SARs can streamline these notification and reporting requirements.

Institutions should also address customer notification procedures in their IRP. When an institution becomes aware of an incident involving unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to determine the likelihood that such information has been or will be misused. If the institution determines that sensitive customer information has been misused or that misuse of such information is reasonably possible, it should notify the affected customer(s) as soon as possible. Developing standardized procedures for notifying customers will assist in making timely and thorough notification. As a resource in developing these procedures, institutions should reference the April 2005 interpretive guidance, which specifically addresses when customer notification is necessary, the recommended content of the notification, and the acceptable forms of notification.

Best Practices—Going Beyond the Minimum

Each bank has the opportunity to go beyond the minimum requirements and incorporate industry best practices into its IRP. As each bank tailors its IRP to match its administrative, technical, and organizational complexity, it may find some of the following best practices relevant to its operating environment. The practices addressed below are not all inclusive, nor are they regulatory requirements. Rather, they are representative of some of the more effective practices and procedures some institutions have implemented. For organizational purposes, the best practices have been categorized into the various stages of incident response: preparation, detection, containment, recovery, and follow-up.

Preparation

Preparing for a potential security compromise of customer information is a proactive risk management practice. The overall effectiveness and efficiency of an organization's response is related to how well it has organized and prepared for potential incidents. Two of the more effective practices noted in many IRPs are addressed below.

- **Establish an incident response team.**

A key practice in preparing for a potential incident is establishing a team that is specifically responsible for responding to security incidents. Organizing a team that includes individuals from various departments or functions of the bank (such as operations, networking, lending, human resources, accounting, marketing, and audit) may better position the bank to respond to a given incident. Once the team is established, members can be assigned roles and responsibilities to ensure incident handling and reporting is comprehensive and efficient. A common responsibility that banks have assigned to the incident response team is developing a notification or call list, which includes contact information for employees, vendors, service providers, law enforcement, bank regulators, insurance companies, and other appropriate contacts. A comprehensive notification list can serve as a valuable resource when responding to an incident.

[7] See www.fincen.gov/reg_bsaforms.html.

Incident Response Programs

continued from pg. 7

■ **Define what constitutes an incident.**

An initial step in the development of a response program is to define what constitutes an incident. This step is important as it sharpens the organization's focus and delineates the types of events that would trigger the use of the IRP. Moreover, identifying potential security incidents can also make the possible threats seem more tangible, and thus better enable organizations to design specific incident-handling procedures for each identified threat.

Detection

The ability to detect that an incident is occurring or has occurred is an important component of the incident response process. This is considerably more important with respect to technical threats, since these can be more difficult to identify without the proper technical solutions in place. If an institution is not positioned to quickly identify incidents, the overall effectiveness of the IRP may be affected.[8] Following are two detection-related best practices included in some institutions' IRPs.

■ **Identify indicators of unauthorized system access.**

Most banks implement some form of technical solution, such as an intrusion detection system or a firewall, to assist in the identification of unauthorized system access. Activity reports from these and other technical solutions (such as network and application security reports) serve as inputs for the monitoring process and for the IRP in general. Identifying potential indicators of unauthorized system access within these activity or security reports can assist in the detection process.

■ **Involve legal counsel.**

Because many states have enacted laws governing notification requirements for customer information security compromises, institutions have found it prudent to involve the institution's legal counsel when a compromise of customer information has been detected. Legal guidance may also be warranted in properly documenting and handling the incident.

Containment

During the containment phase, the institution should generally implement its predefined procedures for responding to the specific incident (note that containment procedures are a required minimum component). Additional containment-related procedures some banks have successfully incorporated into their IRPs are discussed below.

■ **Establish notification escalation procedures.**

If senior management is not already part of the incident response team, banks may want to consider developing procedures for notifying these individuals when the situation warrants. Providing the appropriate executive staff

[8] Pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), the FDIC, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission, have jointly proposed (1) guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft, and (2) regulations requiring each financial institution and creditor to establish reasonable policies and procedures for implementing the guidelines. The notice of proposed rulemaking (NPR) also includes provisions requiring credit and debit card issuers to assess the validity of a request for a change of address under certain circumstances, and, pursuant to section 315 of the FACT Act, guidance regarding reasonable policies and procedures that a user of consumer reports must employ when such a user receives a notice of address discrepancy from a consumer reporting agency. The NPR was published on July 18, 2006, at 71 Fed. Reg. 40786, and the comment period ended on September 18, 2006. The agencies are reviewing the comments received in preparation for a final rule.

and senior department managers with information about how containment actions will affect business operations or systems and including these individuals in the decision-making process can help minimize undesirable business disruptions. Institutions that have experienced incidents have generally found that the management escalation process (and resultant communication flow) was not only beneficial during the containment phase, but also proved valuable during the later phases of the incident response process.

- **Document details, conversations, and actions.**

Retaining documentation is an important component of the incident response process. Documentation can come in a variety of forms, including technical reports generated, actions taken, costs incurred, notifications provided, and conversations held. This information may be useful to external consultants and law enforcement for investigative and legal purposes, as well as to senior management for filing potential insurance claims and for preparing an executive summary of the events for the board of directors or shareholders. In addition, documentation can assist management in responding to questions from its primary Federal regulator. It may be helpful during the incident response process to centralize this documentation for organizational purposes.

- **Organize a public relations program.**

Whether a bank is a local, national, or global firm, negative publicity about a security compromise is a distinct possibility. To address potential reputation risks associated with a given incident, some banks have organized public relations programs and designated specific points of contact to oversee the program. A well-defined public relations program can provide a specific avenue for open communications with both the media and the institution's customers.

Recovery

Recovering from an incident essentially involves restoring systems to a known good state or returning processes and procedures to a functional state. Some banks have incorporated the following best practices related to the recovery process in their IRPs.

- **Determine whether configurations or processes should be changed.**

If an institution is the subject of a security compromise, the goals in the recovery process are to eliminate the cause of the incident and ensure that the possibility of a repeat event is minimized. A key component of this process is determining whether system configurations or other processes should be changed. In the case of technical compromises, such as a successful network intrusion, the IRP can prompt management to update or modify system configurations to help prevent further incidents. Part of this process may include implementing an effective, ongoing patch management program, which can reduce exposure to identified technical vulnerabilities. In terms of non-technical compromises, the IRP can direct management to review operational procedures or processes and implement changes designed to prevent a repeat incident.

- **Test affected systems or procedures prior to implementation.**

Testing is an important function in the incident response process. It helps ensure that reconfigured systems, updated procedures, or new technologies implemented in response to an incident are fully effective and performing as expected. Testing can also identify whether any adjustments are necessary prior to implementing the updated system, process, or procedure.

Incident Response Programs

continued from pg. 9

Follow-up

During the follow-up process, an institution has the opportunity to regroup after the incident and strengthen its control structure by learning from the incident. A number of institutions have included the following best practice in their IRPs.

- **Conduct a "lessons-learned" meeting.**

Successful organizations can use the incident and build from the experience. Organizations can use a lessons-learned meeting to

- discuss whether affected controls or procedures need to be strengthened beyond what was implemented during the recovery phase;
- discuss whether significant problems were encountered during the incident response process and how they can be addressed;
- determine if updated written policies or procedures are needed for the customer information security risk assessment and information security program;
- determine if updated training is necessary regarding any new procedures or updated policies that have been implemented; and
- determine if the bank needs additional personnel or technical resources to be better prepared going forward.

The preceding best practices focused on the more common criteria that have been noted in actual IRPs, but some banks have developed other effective incident response practices. Examples of these additional practices are listed in Figure 2. Organizations may want to review these practices and determine if any would add value to their IRPs given their operating environments.

What the Future Holds

In addition to meeting regulatory requirements and addressing applicable industry best practices, several characteristics tend to differentiate banks. The most successful banks will find a way to integrate incident response planning into

Figure 2

Additional IRP Best Practices

- Test the incident response plan (via walk-through or tabletop exercises) to assess thoroughness.
- Implement notices on login screens for customer information systems to establish a basis for disciplinary or legal action.
- Develop an incident grading system that quantifies the severity of the incident, helps determine if the incident response plan needs to be activated, and specifies the extent of notification escalation.
- Provide periodic staff awareness training on recognizing potential indicators of unauthorized activity and reporting the incident through proper channels. Some institutions have established phone numbers and e-mail distribution lists for reporting possible incidents.
- Inform users about the status of any compromised system they may be using.
- Establish a list of possible consultants, in case the bank does not have the expertise to handle or investigate the specific incident (especially regarding technical compromises).
- Establish evidence-gathering and handling procedures aimed at preserving evidence of the incident and aiding in prosecution activities.

normal operations and business processes. Assimilation efforts may include expanding security awareness and training initiatives to reinforce incident response actions, revising business continuity plans to incorporate security incident responses, and implementing additional security monitoring systems and procedures to provide timely incident notification. Ultimately, the adequacy of a bank's IRP reflects on the condition of the information security program along with management's willingness and ability to manage information technology risks. In essence, incident response planning is a management process, the comprehensiveness and success of which provide insight into the quality and attentiveness of management. In this respect, the condition of a bank's IRP, and the results of examiner review of the incident response planning process, fit well within the objectives of the information technology examination as described in the Information Technology–Risk Management Program.[9]

An IRP is a critical component of a well-formed and effective information security program and has the potential to provide tangible value and benefit to a bank. Similar to the importance of a business continuity planning program as it relates to the threat of natural and man-made disasters, sound IRPs will be necessary to combat new and existing data security threats facing the banking community. Given the high value placed on the confidential customer information held within the financial services industry, coupled with the publicized success of known compromises, one can reasonably assume that criminals will continue to probe an organization's defenses in search of weak points. The need for response programs is real and has been recognized as such by not only state and Federal regulatory agencies (through passage of a variety of legal requirements), but by the banking industry itself. The challenges each bank faces are to develop a reasonable IRP providing protections for the bank *and* the consumer and to incorporate the IRP into a comprehensive, enterprise-wide information security program. The most successful banks will exceed regulatory requirements to leverage the IRP for business advantages and, in turn, improved protection for the banking industry as a whole.

Eric R. Morris
Information Technology Examiner, Chicago, IL

John J. Sosnowski II
Examiner, Indianapolis, IN

[9] The Information Technology–Risk Management Program (IT–RMP) is the approach for conducting information technology examinations at FDIC-supervised institutions, regardless of size and complexity. FIL 81-2005, Information Technology–Risk Management Program New Information Technology Examination Procedures, August 18, 2005, www.fdic.gov/news/news/financial/2005/fil8105.html.

Chasing the Asterisk: A Field Guide to Caveats, Exceptions, Material Misrepresentations, and Other Unfair or Deceptive Acts or Practices

Section 5 of the Federal Trade Commission (FTC) Act prohibits "unfair or deceptive practices in or affecting commerce."[1] Although enforced generally by the FTC against nonbank entities, the authority for enforcing Section 5 as it relates to FDIC-supervised institutions rests with the FDIC, pursuant to Section 8 of the Federal Deposit Insurance Act,[2] which permits the FDIC and the other Federal banking agencies to enforce "any law."

The prohibition against unfair and deceptive acts or practices (UDAPs) applies to all products and services offered by a financial institution, directly or indirectly. The prohibition applies to every stage and activity: from product development to the creation and rollout of the marketing campaign; from servicing and collections all the way through to the termination of the customer relationship.

Although the vast majority of FDIC-supervised institutions adhere to a high level of professional conduct, the FDIC has seen an increase in violations of Section 5 of the FTC Act. This may be the result of increased competition among financial institutions, along with a growing dependence on fee income and increased reliance on third parties. Expansion into the subprime market may be another factor, as well as the proliferation of products with complex structures and pricing. Examiners have identified various acts and practices that violate Section 5, including deceptive marketing and solicitations, misleading billing statements, and failure to adequately disclose material terms and conditions for both credit and deposit products.

Depending on the severity of their nature and scope, violations of the FTC Act may adversely affect an institution's compliance rating, as well as result in an enforcement action and restitution. Evidence of such violations may also cause a downgrade of an institution's Community Reinvestment Act (CRA) rating. Public knowledge that a financial institution engaged in unfair or deceptive acts or practices—from publication of a cease and desist order, a statement in the institution's public CRA Performance Evaluation, or reports in the media—may result in reputational harm to the institution, lawsuits, and financial damages. In light of these risks, failure to prevent or address potential UDAPs may, in turn, expose the institution to questions regarding the adequacy of its management and the safety and soundness of its operations.

This article provides insights into how examiners identify and address acts or practices that may violate the prohibition against UDAPs found in Section 5 of the FTC Act. Financial institutions can use this information to conduct assessments of their products and services and to develop a blueprint for avoiding Section 5 violations.

FDIC Enforcement of Section 5 of the FTC Act

A number of agencies have authority to combat UDAPs. While the FTC has broad authority to enforce the requirements of Section 5 of the FTC Act, banks and certain other businesses are exempted from the FTC's authority.[3] In a Financial Institution Letter (FIL) dated May 30, 2002,[4]

[1] 15 U.S.C. § 45(a).

[2] 12 U.S.C. § 1818(b).

[3] 15 U.S.C. § 45.

[4] FIL-57-2002, Guidance on Unfair or Deceptive Acts or Practices, May 30, 2002, www.fdic.gov/news/news/financial/2002/fil0257.html.

the FDIC confirmed the applicability of Section 5 of the FTC Act to state nonmember banks and their institution-affiliated parties, as well as the FDIC's intention to cite violations of this law and take appropriate action under Section 8 of the Federal Deposit Insurance Act[5] (FDI Act) when it discovers unfair or deceptive acts or practices.

On March 11, 2004, the FDIC with the Board of Governors of the Federal Reserve System (FRB) jointly issued guidance on UDAP (Joint Guidance) to state-chartered banks outlining the standards the FDIC and the FRB will consider when applying the prohibitions against UDAPs found in the FTC Act and providing advice on managing risks relating to UDAPs.[6]

In determining the appropriate response to a Section 5 violation, the FDIC consults with other state and federal agencies depending on the issue and their jurisdiction over the parties involved. Where necessary to address the UDAP and provide an appropriate remedy for consumers, the FDIC will also pursue a joint action with other government entities.[7]

Standards for Determining What Is Unfair or Deceptive

As stated in the Joint Guidance,[8] the standards for unfairness and deception are independent of each other. While a specific act or practice may be both unfair and deceptive, an act or practice is prohibited by the FTC Act if it is *either* unfair *or* deceptive.

To assist in determining whether a particular act or practice is unfair or deceptive, the FTC has issued policy statements on both unfairness and deception.[9] In most cases, Section 5 violations involve deception, although there have been a few instances where a particular act or practice, or the sum of a variety of acts and practices, have been found to be unfair.

Unfairness

An act or practice may be found to be unfair where it

(1) Causes or is likely to cause substantial injury to consumers, which

(2) Is not reasonably avoidable by consumers themselves, and

(3) Is not outweighed by countervailing benefits to consumers or to competition.

Public policy may also be considered in the analysis of whether a particular act or practice is unfair.

Deception

A three-part test is used to assess whether a representation, omission, or practice is deceptive:

(1) The representation, omission, or practice must mislead or be likely to mislead the consumer;

(2) The consumer's interpretation of the representation, omission, or practice must be reasonable under the circumstances. If a representation or practice is targeted to a particular group—for example, the elderly

[5] 12 U.S.C. § 1818(a).

[6] FIL-26-2004, Unfair or Deceptive Acts or Practices by State-Chartered Banks, March 11, 2004 (Joint Guidance), www.fdic.gov/news/news/financial/2004/fil2604.html.

[7] Ibid., footnote 6, page 1.

[8] Ibid., footnote 6, page 2.

[9] See FTC Policy Statement on Unfairness (December 17, 1980), www.ftc.gov/bcp/policystmt/ad-unfair.htm, and FTC Policy Statement on Deception (October 14, 1983), www.ftc.gov/bcp/policystmt/ad-decept.htm.

Chasing the Asterisk: A Field Guide

continued from pg. 13

Unfairness Based upon Lack of Utility

A bank advertised a credit card with no application or annual fees. However, consumers were charged a "refundable acceptance fee," which completely exhausted the available credit line. According to the terms of the card, this acceptance fee would be "refunded" in increments of $50 every three months, assuming the consumer paid the minimum amount due on a timely basis, making available an equal amount of credit. As opposed to an annual fee, a monthly maintenance charge of $10 was charged against the account, along with an interest rate of almost 20 percent against the outstanding balance.

The FDIC found that the "refundable acceptance fee" was nothing more than a bookkeeping entry used by the bank to create a balance upon which it could assess interest and other charges. At a minimum, consumers were paying $120 a year plus interest in exchange for the use of a credit line made available to them in $50 increments. Account activity reports showed little or no purchases or charges, only the assessment of monthly fees, interest, and other charges.

The card program was determined to be "unfair." The fees associated with the program made any benefit negligible, and the program was structured so that only a very small percentage of account holders would receive any initial or subsequent credit. Moreover, with no out-of-pocket money at risk and the limited utility of the card, a high delinquency rate was foreseeable. Within six months from the initial offering of the product, nearly 50 percent of all accounts opened were delinquent.

or troubled borrowers—its reasonableness must be evaluated from the vantage point of that group; *and,*

(3) The misleading representation, omission, or practice must be material.

A deceptive representation can be expressed, implied, or involve a material omission. The overall impression is key—written disclosures in the text or fine print in a footnote may be insufficient to correct a misleading headline.[10]

As can be seen from the examples in the text box above and on the facing page, and as stated in the Joint Guidance, whether an act or practice is unfair or deceptive depends upon a careful analysis of the facts and circumstances. In analyzing a particular act or practice, the FDIC is guided by the body of law and official interpretations for defining UDAPs developed by the courts and the FTC, as well as factually similar cases brought by other enforcement and regulatory agencies, including other federal bank regulatory agencies.[11]

Identifying UDAP Issues

UDAPs are not always apparent or easily discovered. In most instances, examiners may be unaware of any potential unfair or deceptive concerns prior to their examination of a bank. FDIC examiners may identify potential UDAPs during the course of an examination, through a consumer complaint, or through referrals from state or local agencies or consumer protection organizations. Reports of unfair or deceptive acts or practices in the media—print, TV, and the Internet—may trigger investigations.

The scope of an examination or investigation to determine whether an institution is engaging in UDAPs involves a review of the institution's products, services, target markets, operations, and compliance management systems and programs. Examiners first develop a risk profile for the institution using information about the institution's business lines, organizational structure, operations, and past supervisory performance. Then they investigate any identified high-risk areas, such as subprime lending and third-party relationships.

Identifying red flags and high-risk areas, and investigating them, is a key part of any UDAP review or investigation.

[10] FTC Policy Statement on Deception, p. 5, October 14, 1983, www.ftc.gov/bcp/policystmt/ad-decept.htm.

[11] Joint Guidance at page 2; FIL-57-2002, Guidance on Unfair or Deceptive Acts or Practices, May 30, 2002, www.fdic.gov/news/news/financial/2002/fil0257.html.

Deceptive Advertising and Billing

On one bank's home page was a large multicolored advertisement that prominently displayed a series of credit cards and a large blue ball. Alternately flashing across the ball, in bold white letters outlined in red, were the statements "NO COLLECTION CALLS*!" and "NO LATE FEES*!" Although each statement contained an asterisk, there were no explanatory notes on this page.

A consumer who clicked on the blue ball or one of the credit cards would be linked to an application page containing the online application form. At the top of this page, the statements "NO collection calls*" and "NO late fees*" again appeared as static text, along with the statement, "NO Nonsense." The phrases "NO COLLECTION CALLS*," "NO LATE FEES*," and "APPLY NOW!" appeared a second time on this page as flashing text in a red banner. The following text appeared in small print in the middle of the page, largely obscured by other promotional information:

> Late fees may apply and you may receive collection calls if payments are past due on your credit account and charges or fees incurred cause your credit account balance to exceed its credit line (over limit) or any portion of your credit line becomes unsecured . . .

If the consumer clicked the site on or near "APPLY NOW!" the online application moved from the middle to the top of the screen, covering over this qualification. If, instead of clicking "APPLY NOW!" the consumer clicked the "Important Terms and Conditions" link appearing at the top of the application page, they would be taken to another web page containing the general terms and conditions, again with the flashing statements "NO COLLECTION CALLS*," "NO LATE FEES*," and "APPLY NOW" appearing at the top of the page. In this instance, as with the original statements on the bank's home page, there were no qualifying disclosures.

The FDIC found the statements to be deceptive. The qualifications, printed in small text and largely obscured, contradicted the prominently advertised terms. Additionally, while the banner headlines appeared multiple times on each of the three pages, the qualifying language appeared only once, could easily be skipped, and was completely covered if the consumer clicked the link for the online application.

In a similar case, the bank sent out billing statements to its delinquent credit card account holders featuring a prominently placed message, located in a box in the center of the statement, advising the consumer that if they paid a specific sum, they could avoid additional fees and further collection efforts. Upon investigation, the examiners determined that the amount stated in the message box was the amount past due, not the larger minimum payment amount, and that payment of this amount would result in additional charges as well as continuation of the consumer's delinquent status.

Although the minimum amount due was stated elsewhere on the billing statement, the bank's practice was deceptive because it used an alternative amount in the message box to direct the consumer's attention away from the correct minimum payment amount necessary to restore their account to a current status. Moreover, despite the bank's explicit claims to the contrary, payment of the amount the bank specified in the message box would subject the consumer to what they were told they would avoid: additional fees and collection efforts.

The bank was directed to immediately terminate this practice and reimburse those consumers who incurred late charges and other fees as a result of this practice.

Red Flags That Could Warrant a UDAP Review

Consumer Complaints

Consumer complaints are often a key source of information on possible UDAPs.[12]

As part of the pre-examination process,[13] examiners are required to review consumer complaints. At the FDIC, complaints received regarding state nonmember banks are maintained in an automated database and are available directly to examiners. In addition to reviewing complaints received by the FDIC, on-site examinations always include a review of the complaints received by the institution and its procedures for addressing them.[14]

[12] For agencies that do not have authority to perform on-site examinations, such as the FTC or a state attorney general, consumer complaints often serve as the primary basis for their investigations.

[13] FDIC *Compliance Examination Handbook,* "Compliance Examinations—Pre-examination Planning," page II-3.1.

[14] Ibid., "Compliance Examinations—Analysis," page II-4.1.

Chasing the Asterisk: A Field Guide

continued from pg. 15

When reviewing complaints, examiners also look for trends: for example, how many of the same or similar type of complaints did the bank receive? While a large volume of complaints will frequently indicate an area of concern, the number of complaints received is not a determining factor in and of itself of whether there is a potential unfair or deceptive issue. A small number of complaints do not undermine the validity of the complaints or the seriousness of the allegations raised. If even a single complaint raises apparent valid concerns relative to a potential UDAP, the examiner may determine that a Section 5 review is warranted. Consequently, examiners focus on the issues raised in complaints, not just the number of complaints.

Because many consumers may not be aware that the FDIC and the other bank regulatory agencies have consumer protection offices responsible for investigating consumer complaints,[15] examiners may contact other entities more generally known to consumers as places to file a complaint. These include the Better Business Bureau, the FTC, and state agencies, such as a state banking department or an attorney general's office.

When reviewing complaints, examiners pay particular attention not only to the immediate concerns of the consumer, but the broader implications. Allegations or claims that may indicate possible UDAPs include

- Misleading or false statements,
- Missing disclosures or information,
- Undue or excessive fees,
- Inability to reach customer service, or
- Previously undisclosed charges.

Investigations by Other Federal or State Agencies

The FDIC gives serious attention to investigations initiated by other government agencies such as state banking departments or attorneys general offices. The regional offices are often notified directly by the investigating agency, although notice may first come from the target bank once it has learned it is under investigation.[16]

Where a state or other agency asserts that an FDIC-insured institution has violated state consumer protection law, the FDIC office in the Region, in consultation with the Washington office, reviews the allegations to determine if they involve potential UDAPs. Although such assertions may be based on state law, they nonetheless may also involve potential violations of Section 5 of the FTC Act.

Criticism of Institution, Product, or Service in the Media

Newspaper articles, radio programs, and television consumer reports can provide information on potential UDAP issues. For example, during the course of one bank examination, a local news station did a special report on a consumer's complaint of deceptive practices at the bank's mortgage subsidiary. This information further corroborated issues examiners noted in consumer complaints.

Internet searches for information on an institution or a particular product or service it offers (such as a credit card or other loan product) can be another source of information on possible UDAPs. There are many websites and blogs where consumers write about the problems they have

[15] Congress amended the FTC Act in 1975 to require that each of the bank regulatory agencies establish a division of consumer affairs to address complaints. See 15 U.S.C. § 57a.

[16] As part of the Compliance Information and Document Request (CIDR) sent to institutions prior to a compliance examination, financial institutions are asked whether they are subject to any investigation by a state or government entity or other legal action.

had with particular entities or products. These websites may be used by examiners to supplement information in the complaints received by the FDIC and state authorities.

High-Risk Areas Requiring Scrutiny for UDAPs

Subprime Products

Subprime lending, by its nature, involves the extension of credit to borrowers who may be among the more economically vulnerable or less financially sophisticated. While the presence of subprime products does not automatically equate to unfairness or deception, the complexity of many of these products and their pricing structure may raise Section 5 concerns.

Subprime products are sometimes specifically marketed to consumers with lower levels of financial sophistication, creating greater risk for Section 5 problems. *Products targeted to the elderly, recent immigrants, or a specific ethnic or racial group are also subject to scrutiny for Section 5 violations, as well as for violations of the Equal Credit Opportunity and Fair Housing Acts.*

Third-Party Relationships

The prohibitions against UDAPs found in the FTC Act apply to state-chartered banks, their subsidiaries and institution-affiliated parties, *and* third-party contractors.[17] Third-party relationships, both affiliated and unaffiliated, are one of the most common features in the Section 5 violations found by FDIC examiners.

Unaffiliated Third Parties

An unaffiliated third-party relationship could include a company that provides advertising services, issues credit cards through the bank, sells insurance, brokers loans, or purchases loans or receivables from the bank. Collection activity is another activity frequently conducted by unaffiliated third parties.

Examiners analyze all third-party relationships, affinity agreements, contracts, or partnerships in which the bank is involved or anticipates involvement. In particular, examiners focus on what functions the third party performs for the bank and the bank's oversight and monitoring of the relationship.

If the bank is involved with a third party that offers products or services that raise concerns about UDAP, such as subprime loans, examiners closely review the agreement between the bank

Analyzing Third-Party Relationships

In reviewing third-party arrangements, examiners consider

- The types of services or products provided by the third party and their potential for possible UDAP concerns;
- The due diligence conducted by the bank prior to entering into an agreement with the third party;
- The extent of the bank's oversight and monitoring of the third party; particularly whether the bank's oversight goes beyond "rubber-stamping" disclosures or solicitations produced by the third party; and
- Whether the bank reviews customer service and collection activity for compliance with Section 5.

Financial institutions also can consider these issues when assessing a potential or ongoing relationship with a third party.

[17] FIL-57-2002, Guidance on Unfair or Deceptive Acts or Practices, May 30, 2002, www.fdic.gov/news/news/financial/2002/fil0257.html

Chasing the Asterisk: A Field Guide

continued from pg. 17

and the third party to fully understand its scope and to identify important terms and conditions, such as indemnification clauses and limitations on liability, that may have an impact on the redress for consumers. Moreover, if the agreement provides for the performance of significant activities by the third party—such as marketing, loan processing, or collections—examiners may need to conduct an on-site visitation of the third party.

Affiliated Third Parties

Examiners will want to be apprised of all subsidiaries and affiliates and the types of products and services each offers. Other important factors in the examiner's analysis include

- Level of control and oversight the banks exert over the subsidiary;
- Types of reporting mechanisms in place;
- Origin of the relationship between the bank and the affiliated third party (i.e., was the subsidiary or affiliate "homegrown" or was it an independent entity purchased by the bank?).

Regarding the relationship between the bank and the affiliated third party, it can sometimes take a long time to implement bank policies and procedures and integrate a purchased subsidiary into the bank's organizational culture. Previously independent entities and independent vendors frequently have difficulty assimilating and conforming to the supervisory compliance structure of regulated institutions.

If weaknesses are seen in the oversight and controls of a bank subsidiary or affiliate, and the types of products or services the subsidiary or affiliate offers have the potential for possible unfair or deceptive practices, examiners may review related files, documents, disclosures, or information on-site at the offices of the subsidiary or affiliate instead of at the bank. As with any examination, examiners on-site observe how the subsidiary or affiliate operates, the business culture, and how well-versed employees dealing directly with consumers are with applicable laws and regulations.

Analyzing an Unfair or Deceptive Case

Section 5 of the FTC Act does not impose any specific requirements on banks.[18] The policies and procedures necessary to avoid engaging in unfair or deceptive activities will largely depend on an institution's business strategy, its target markets, its products and services, and its relationships with third parties.

The UDAP examination procedures cover various topics to assist examiners

Importance of Strong Oversight and Control

In some cases involving UDAP issues, the banks involved had affinity agreements with unaffiliated third-party providers to issue credit cards via a rent-a-BIN arrangement. In this type of arrangement, the financial institution permits a third party to use its Bank Identification Number (which is required to issue credit cards) to issue credit cards on its behalf. Generally, in rent-a-BIN relationships, the institution sells its credit card receivables to the third party, although the bank remains the issuer. In both small and large institutions involved in these arrangements, examiners have at times found a lack of oversight and control, resulting in unchecked UDAPs in connection with the subprime credit card product issued under the bank's name.

[18] FDIC *Compliance Examination Handbook,* "Abusive Practices—Federal Trade Commission Act," page VII-1.5.

in their review: product structure and terms, advertising and solicitation, repricing and change of terms, servicing and collections, and monitoring the conduct of third parties. A Section 5 analysis is not based upon a particular checklist, but is fact specific. The examination procedures provide, as guidelines, questions for examiners to consider when evaluating a particular act or practice, developed largely based upon past Section 5 violations. Whenever an examiner determines a product or practice is potentially unfair or deceptive, he or she will analyze it using the standards for unfairness and deception summarized in the examination procedures and discussed more fully in the Joint Guidance.

In addition to setting forth the standards for evaluating a potential Section 5 situation, the Joint Guidance addresses a number of other topics examiners consider when evaluating a product or practice. The Joint Guidance further discusses the interplay between the FTC Act and other laws, and cautions that even though a bank may be in technical compliance with other laws, such as the Truth in Lending or Truth in Savings Acts, a product or practice may still violate Section 5. For example, a bank's credit card advertisement may contain all the required Truth in Lending Act disclosures, but obscured or inadequately disclosed material limitations and restrictions could lead to a Section 5 violation.

In analyzing a product or service that raises unfairness or deception concerns, examiners will often look beyond the compliance aspects and evaluate the product or practice from a safety and soundness perspective. For example, high default and delinquency rates identified through profitability reports, aging and delinquency reports, or re-aging and negative amortization practices may raise questions about whether a product fulfills its various marketing promises—claims often based upon building or improving a borrower's credit. Account activity reports, with fees and interest broken out, may also raise questions. In several credit card products reviewed by FDIC examiners, the limited credit lines were largely exhausted by various account opening fees and other fees. As a result, there was no purchase or other normal credit activity because there was little or no available credit. Activity reports for deposit products, such as stored-value cards, are also often reviewed to assess consumer usage, access to account information, and the assessment of fees and other charges and their impact on the deposited balance.

Enforcement actions brought by the FDIC, other banking agencies, and the FTC on similar issues, and guidance issued by the FDIC and these agencies provide an important framework for analyzing potential Section 5 violations. State investigations and actions may also be useful in evaluating an unfairness or deception claim. The FDIC's examination procedures provide a reference section on cases and guidance on unfairness or deception issues relating to specific areas, such as mortgage and credit card lending, and servicing and collections.[19]

Given the dynamic nature of the market and the constant emergence of new products and practices that may raise unfairness or deception issues, it is important to remain alert to any new case law or guidance on a given topic.

Corrective Action

As with any violation of law or regulation, the response to a violation of the FTC Act will depend on a number of factors, including

- The nature of the violation;

[19] Ibid., page VII-1.7.

Chasing the Asterisk: A Field Guide

continued from pg. 19

- Whether it is a repeat violation or a variation of a previously cited violation;
- The harm, or potential harm, suffered by consumers;
- The number of parties affected; and
- The institution's overall compliance posture and history, both in general and with respect to UDAPs.

Significant violations not only may require discontinuance of the practice and reimbursement of consumers, but may also result in a downgrade of the bank's compliance (and possibly CRA[20]) rating as well as an enforcement action.

UDAP—a Priority at the FDIC

Unlike most consumer compliance laws and regulations, which tend to be prescriptive, Section 5 of the FTC Act is a broadly written law subject to interpretation. While Section 5 is specific in the criteria that must be met for an act or practice to be considered unfair or deceptive, determining whether any particular act or practice is unfair or deceptive requires a review of applicable law and judgment. In a dynamic market with constant new products and services emerging, it is critical that UDAP situations be evaluated with a national perspective. The FDIC recognizes the seriousness of violations involving UDAPs and the potential impact of such violations on consumers, the institution, and the community at large. Therefore, examiners are required to consult with both the regional and headquarters offices when they first identify a product or service that raises deception or unfairness concerns. Headquarters concurrence, which may include consultation with the FDIC's Legal Division and the FTC, must be obtained before a violation of the FTC Act may be cited in an examination report.

The FDIC has made identification of products and services with UDAP implications a key priority in its efforts to combat predatory lending practices. The significance and seriousness of these violations should not be underestimated: they are raised to the highest levels of the FDIC, and can adversely affect the institution's overall compliance, CRA, and safety and soundness ratings. Depending on their severity, violations may result in a costly formal enforcement action and restitution for

Corrective Action in the Case of Overdraft Protection and Erroneous ATM Disclosures

In several cases involving overdraft protection, examiners found that the bank provided only a single account balance at its ATMs reflecting the consumer's actual balance plus the amount of overdraft protection. If consumers did not have adequate information at the time of their ATM transaction to determine the amount of funds they had available, they could inadvertently overdraw their accounts and incur overdraft protection fees as well as other charges.

In some instances, the FDIC determined that this practice was deceptive based upon an omission of material information necessary for the consumer to consider in making an informed decision. The affected banks corrected the problem in different ways: some posted signs at ATMs that alerted customers that withdrawals might overdraw accounts and trigger fees; others took steps to ensure that ATMs showed actual account balances. The FDIC required banks to identify and reimburse all consumers who were charged overdraft protection and other fees as a result of the initial practice.

[20] 12 C.F.R. § 345.28(2).

consumers. These actions, in turn, may damage the institution's reputation, expose it to litigation risk, and result in substantial financial loss. Financial institutions should use this information and prior guidance on unfairness and deception issued by the FDIC and other agencies to educate their staffs on how to avoid UDAPs and to strengthen their compliance management system overall.

Deirdre Foley
Senior Policy Analyst
Washington, DC

Kara L. Ritchie
Review Examiner, Boston, MA

The authors acknowledge the assistance provided by the following FDIC staff in the preparation of this article: Todd L. Hendrickson, Field Office Supervisor (Compliance) and Denise R. Beiswanger, Senior Compliance Examiner, Sioux Falls Field Office; Greg Gore, Counsel, Richard Bogue, Counsel, and Hugo Zia, Counsel, Washington Office Legal Division; Mira Marshall, Senior Policy Analyst, Compliance Policy Section, Washington Office; and Patricia W. Farrell, Acting Field Office Supervisor (Compliance) and Robert M. Macrae, Field Office Supervisor (Compliance), Philadelphia Field Office.

Understanding BSA Violations[1]

The Bank Secrecy Act (BSA) and its implementing rules are not new; the BSA has been part of the bank examination process for more than three decades.[2] In recent years, a number of financial institutions have been assessed large civil money penalties for noncompliance with the BSA. While most insured financial institutions examined demonstrate an adequate system of BSA controls, these high profile cases highlight the importance of banks' efforts to ensure compliance with the BSA and its implementing rules. Nevertheless, where an institution falls short of these requirements, these shortfalls can result in violations of the BSA and the implementing rules being cited in Reports of Examination (ROE).

This article discusses the evolution of the BSA, including a brief overview of the USA PATRIOT Act (Patriot Act) changes. The article also discusses the types of BSA-related violations cited in examination reports, provides examples of best practices for maintaining a strong Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program, and clarifies the distinctions between a significant BSA program breakdown and technical problems in financial institutions.

Evolution of the BSA

The first Anti-Money Laundering (AML) statute, enacted in the U.S. in 1970, was titled *Currency and Foreign Transactions Reporting Act* and has become commonly known as the *"Bank Secrecy Act"* or *"BSA."* The BSA established basic recordkeeping and reporting requirements for private individuals, banks and other financial institutions. The complexity of the BSA expanded in subsequent years with legislative changes requiring banks to establish procedures to ensure BSA compliance. Provisions were also added establishing criminal liability against persons or banks that knowingly assist in money laundering or structuring or that avoid BSA reporting requirements.

The most sweeping changes in the BSA occurred shortly after the September 11, 2001, terrorist attacks with the passage of the Patriot Act in October 2001.[3] The Patriot Act criminalized the financing of terrorism and augmented the BSA by strengthening customer identification procedures; prohibiting financial institutions from engaging in business with foreign shell banks; requiring financial institutions to have due diligence procedures, and, in some cases, enhanced due diligence procedures for foreign correspondent and private banking accounts; and improving information sharing between financial institutions and the U.S. government. The Patriot Act and its implementing regulations also

- Expanded the AML program requirements to all financial institutions;
- Increased the civil and criminal penalties for money laundering;
- Provided the Secretary of the Treasury with the authority to impose

[1] This article reflects the FDIC's practices to date and is not intended to be a legal interpretation. Information is provided to assist banks in complying with the law but is subject to adjustment as examination practices are reviewed or refined.

[2] By regulation, authority to examine for BSA compliance has been delegated to the regulator of each category of financial institution (i.e., the banking regulators for banks, the Securities and Exchange Commission for broker-dealers), and to the IRS for institutions that do not have a primary regulator. 31 CFR 103.56(b). The first rules delegating this authority were finalized in 1972. *See* 37 FR 6912, April 5, 1972.

[3] Refer to the *Supervisory Insights,* From the Examiner's Desk… Summer 2004 edition for a discussion of the USA PATRIOT Act and new regulations affecting the industry. See www.fdic.gov/regulations/examinations/supervisory/insights/sisum04/sisum04.pdf.

"special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern";

- Facilitated records access and required banks to respond to regulatory requests for information within 120 hours; and
- Required the Federal banking agencies to consider a bank's AML record when reviewing bank mergers, acquisitions, and other applications for business combinations.

To ensure consistency in the BSA/AML examination process and provide guidance to the examination staff, the Federal banking agencies, the Financial Crimes Enforcement Network (FinCEN), and the Office of Foreign Assets Control released the *Federal Financial Institutions Examination Council's Bank Secrecy Act/Anti-Money Laundering Examination Manual* in June 2005. The manual was updated and re-released in July 2006.[4]

Required Elements of a BSA/AML Program

Federal law requires each financial institution to establish and maintain a BSA/AML compliance program. This program must provide for the following minimum requirements (also referred to as "pillars") as outlined in Part 326.8 of FDIC Rules and Regulations:

1) A system of internal controls to ensure ongoing compliance.
2) Independent testing of BSA compliance.
3) A specifically designated person or persons responsible for managing BSA compliance (i.e., BSA compliance officer).
4) Training for appropriate personnel.

In addition, the Patriot Act required banks to establish a customer identification program, which must include risk-based procedures that enable the institution to form a reasonable belief that it knows the true identity of its customers. Referred to as the "fifth pillar," this requirement was implemented in October 2003.

Examiners assess compliance in these areas during BSA/AML examinations. Relevant findings from transaction testing and recommendations to strengthen the bank's BSA/AML compliance program, including its policies, procedures, and processes, are reflected within the ROE, and are an integral part of the FDIC's risk management examination process. Examination findings may include violations of the BSA and the implementing rules. The next section takes a closer look at the different types of violations and discusses the significance of these types of violations in an overall BSA/AML program.

BSA-Related Violations

For state-chartered, nonmember banks supervised by the FDIC, applicable BSA-related violations include infractions of FDIC Rules and Regulations (12 CFR 326.8 and 12 CFR 353), as well as, the Department of Treasury Regulations (31 CFR 103). These regulations, in addition to other applicable legal requirements, are summarized as

> A body of statutes, regulations and administrative rulings, both Federal and State, is an element of the regulatory framework within which banks operate. Their underlying rationale is the protection of the general public (depositors, consumers, investors, creditors, etc.) by establishing boundaries and standards within which banking activities may be conducted.

[4] See FFIEC BSA/AML Examination Manual InfoBase, www.ffiec.gov/bsa_aml_infobase/default.htm.

Understanding BSA Violations

continued from pg. 23

The FDIC assigns a high priority to the detection and prompt correction of violations in its examination and supervisory programs.[5]

In general, there are three broad categories of violations that reflect noncompliance with BSA-related regulations:

(I) Lack of an effective overall compliance program,[6] or specified components of a program ("pillar");[7]

(II) Systemic and recurring noncompliance with the BSA and implementing regulations; and

(III) Isolated and technical noncompliance with the BSA.

Examiners document in the ROE instances of noncompliance with the BSA to develop and provide for the continued administration of a BSA/AML compliance program reasonably designed to assure and monitor compliance with the BSA. However, BSA compliance deficiencies range from isolated instances of noncompliance within an effective overall BSA/AML compliance program to serious weaknesses exposing the institution to an unacceptable level of risk for potential money laundering or other illicit financial activity. The distinction between these violations types is outlined below.

(I) Program Violations. Violations of the FDIC's BSA/AML program rule are cited when ***failure*** occurs in the overall BSA/AML program. BSA program violations must be supported by at least one pillar violation. Violations of individual pillars might, or might not, lead to the conclusion that the bank has suffered an overall BSA/AML program violation. A BSA/AML program failure exposes the institution to an unnecessarily high level of potential risk to money laundering or other illicit financial transactions. The first possible indication that a BSA program has failed is by the absence of one or more of the required pillars. For example, a bank might have a lengthy period when there is no designated BSA compliance officer, or may have failed to provide necessary training.

A BSA/AML program ***failure*** can also be demonstrated by significant noncompliance, on a recurring or systemic basis, with the primary elements of the BSA related to recordkeeping and reporting of critical financial information,[8] as outlined in the Department of Treasury Regulations 31 CFR 103. Generally, examination reports citing BSA/AML program failures would include violations that demonstrate noncompliance with one or more of the primary elements of the minimum financial recordkeeping or reporting requirements. These requirements include

- Reporting suspicious transactions by filing Suspicious Activity Reports (SARs) [31 CFR 103.18];[9]

[5] From the FDIC's *Risk Management Manual of Examination Policies* and applies to violations that may be cited for all types of examinations (e.g., Safety and Soundness, BSA, Information Technology).

[6] 12 CFR 326.8(b)(1) requires that each bank develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with recordkeeping and reporting requirements.

[7] 12 CFR 326.8(b)(2) and (c)(1) through (c)(4) require that a program specifically include: implementing a customer identification program; establishing system of internal controls; providing independent testing; designating a BSA Officer; and instituting a training program.

[8] The BSA, Titles I and II of Public Law 91-508, as amended, modified at 12 D.S.C. 1829b, 12 D.S.C. 1951-1959, and 31 D.S.C. 5311-5332, authorizes the Secretary of the Treasury, *inter alia,* to require financial institutions to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, to protect against international terrorism, and to implement counter-money laundering programs and compliance procedures. Regulations implementing Title II of the Bank Secrecy Act appear at 31 CFR 103.

[9] Part 353 of the FDIC Rules and Regulations parallels 31 CFR 103.18, related to suspicious activity reporting requirements.

- Implementing a program to obtain and verify customer identification [31 CFR 103.121];
- Establishing procedures for responding to information requests made by law enforcement through the FinCEN, in accordance with the process provided for in Section 314(a) of the Patriot Act [31 CFR 103.100];
- Reporting large cash transactions through accurate and timely Currency Transaction Report filings (CTRs) [31 CFR 103.22]; and/or
- Documenting purchases and sales of monetary instruments and incoming/outgoing wire transfers [31 CFR 103.29 and 31 CFR 103.33].

To affect corrective action when a BSA/AML program violation is cited, the FDIC will issue a cease and desist order as required under Section 8(s) of the *Federal Deposit Insurance Act.*

(II) Systemic and Recurring Violations. Regardless of whether a program failure which falls under Section 8(s) is found, an examiner could find systemic violations which relate to ineffective systems or controls to maintain necessary documentation or reporting of customers, accounts, or transactions, as required under various provisions of 31 CFR 103. Determining whether such violations are systemic may be influenced by the number of customers, accounts, or transactions affected; the importance of the unavailable or unrecorded information; the pervasive nature of noncompliance; the predominance of violations throughout the organization; and/or certain program elements that do not adequately provide for an effective system of reporting. Examples of violations that may result in systemic violations include

- Habitually late CTR filings across the organization;
- A significant number of CTRs or SARs with errors or omissions of critical data elements;
- Consistently failing to obtain critical customer identification information at account opening; and
- Systems and programs that do not allow for proper aggregation of multiple cash transactions for regulatory reporting purposes.

Systemic violations of the BSA represent significant noncompliance with financial recordkeeping and reporting requirements or reflect failures within one or more pillars of a BSA/AML program, if not the overall BSA/AML program.

(III) Isolated and Technical Violations. Isolated and technical violations are those limited instances of noncompliance with the financial recordkeeping or reporting requirements of the BSA that occur within an otherwise adequate system of policies, procedures, and processes. Despite the adequacy of the overall program, examiners may note minor violations regarding limited, isolated individual transactions and will focus ROE comments on critical missing or incorrectly reported information for those transactions. These types of violations do not generally result in significant concerns over management's administration of the overall BSA/AML program. Further, when such violations are correctable and management is willing and able to implement appropriate corrective steps, a formal supervisory response may not be warranted.

The Best Defense Is a Good Offense

The steps a bank should take to ensure compliance with the BSA and its implementing rules are documented extensively and are consistent with guidelines that existed before the implementation of the Patriot Act: *To avoid the most serious violations and the implications that can result when those violations are cited, banks must have a strong BSA/AML compliance program.*

Understanding BSA Violations

continued from pg. 25

Financial institutions should ensure they have a well-developed and documented risk assessment that accurately captures the risk exposures of their products, services, customers, and geographic locations. Exposures identified through the risk assessment should be addressed in policies and procedures making sure all identified risks are addressed. Monitoring programs should be in place to ensure account and transaction activity is consistent with expectations and to identify and report suspicious activity. A strong training program should ensure that appropriate personnel are familiar with regulatory requirements and bank policies. The compliance program should be subjected to a periodic independent test of BSA/AML controls to verify compliance with the financial institution's BSA/AML program. The test plan and its results should be reviewed by management to ensure corrective action is taken and the scope of testing meets the bank's requirements. Finally, the bank should have a qualified employee designated by the board of directors to oversee BSA functions and ensure that regulatory requirements and bank policies are being followed on a day-to-day basis.

Table

Best Practices for BSA/AML Compliance
1) Comprehensive Risk Assessment
2) Appropriate Policies and Procedures
3) Adequate Monitoring Programs
4) Strong Training Programs
5) Thorough Independent Testing
6) Qualified Employee Overseeing Day-to-Day Operations

While banks have long been required to have an appropriate BSA program, including policies, procedures, and processes in place to ensure BSA compliance, passage of the Patriot Act has resulted in a number of sweeping changes to the BSA. Understanding the main components of a strong BSA compliance program will help banks to appropriately implement these changes and future amendments.

For additional information on BSA/AML, refer to the Federal Financial Institutions Examination Council's (FFIEC's) BSA/AML InfoBase. (*See* http://www.ffiec.gov/bsa_aml_infobase/default.htm.) The InfoBase is intended to be a one-stop resource for BSA compliance. In addition to the FFIEC BSA/AML Examination Manual, the InfoBase includes, for example, a list of frequently asked questions, various forms needed for meeting BSA/AML compliance responsibilities, and links to the various BSA/AML laws and regulations.

Debra L. Novak
Chief, Anti-Money Laundering Section
Washington, D.C.

Charles W. Collier
Senior Program Analyst, Anti-Money Laundering Section
Washington, D.C.

From the Examiner's Desk . . . Examiners Report on Commercial Real Estate Underwriting Practices

This regular feature focuses on developments that affect the bank examination function. We welcome ideas for future columns. Readers are encouraged to e-mail suggestions to ***SupervisoryJournal@fdic.gov.***

Much has been written about the increase in commercial real estate (CRE) lending. The FDIC has published numerous articles over the last few years reporting increased levels of CRE and construction and development (C&D) loans as a percentage of total capital.[1] The Federal banking regulators[2] have each alerted their supervised financial institutions to the risks associated with this rapid growth and the potential erosion of prudent underwriting practices in the effort to capture market share. In 2004, an article in this journal discussed a CRE lending review program conducted in the FDIC's Atlanta Region, where a relatively high number of banks reported significant levels of CRE exposure.[3]

In this article, we take a closer look at CRE underwriting and loan administration practices, present recurring examination findings, and discuss best practices for managing CRE portfolios in the current environment. This informal review suggests that examiners are observing weaknesses in CRE underwriting and loan administration fairly frequently. A strong economy has thus far helped protect insured banks against the risks associated with CRE. Nevertheless, the FDIC is concerned about trends in the underwriting and management of CRE risks. Examiners are considering these issues in their assessments of banks' risk management practices.

FDIC-Supervised Banks Are Becoming Increasingly Reliant on CRE Lending

The writers' field examination experience, as well as information from other examiners, indicates that many of the institutions experiencing moderate to rapid growth in CRE lending see such loans as their particular market niche. Larger financial institutions and other market participants have gained pricing advantages over community banks in other areas of lending, particularly traditional residential mortgages, home equity lines of credit, and other consumer financing. In addition, the use of predictive credit scoring models for small and medium-sized business loans continues to gain wider acceptance among larger lenders and leasing companies. Community banks can, however, compete for CRE loans because of their knowledge of local markets and borrowers. This characteristic has enabled community banks to expand their share of the CRE market nationwide. Growth in CRE concentrations among FDIC-supervised banks is detailed in Table 1.

Examiners Report on CRE Underwriting

In an effort to identify changes in underwriting practices for CRE concentrations, we requested information on examination findings from each of the

[1] *FDIC Outlook,* Summer 2006; FDIC *Quarterly Banking Profile,* First Quarter 2006.

[2] Office of the Comptroller of the Currency; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of Thrift Supervision.

[3] Assessing Commercial Real Estate Portfolio Risk, *Supervisory Insights,* Vol. 1, Issue 1, Summer 2004, www.fdic.gov/regulations/examinations/supervisory/insights/sisum04/index.html.

From the Examiner's Desk . . .

continued from pg. 27

Table 1

Percentage of FDIC-Supervised Institutions with CRE Loans/Total Capital Ratios > 300% by FDIC Region

Region	June-00	June-01	June-02	June-03	June-04	June-05	June-06
San Francisco	42.0	46.8	51.8	54.1	55.2	60.0	59.8
Atlanta	21.9	28.6	35.7	40.4	44.1	47.6	50.9
Chicago	12.6	15.3	20.1	20.8	24.8	28.2	30.4
New York	10.5	12.1	17.7	19.2	21.7	24.8	27.6
Dallas	11.5	13.3	15.9	17.7	20.4	22.8	24.8
Kansas City	7.4	8.1	8.8	10.2	12.2	14.7	17.1

Note: Data from June 2000 through June 2006 Reports of Condition.

six FDIC Regional Offices. Examiners responded either with examples of individual institutions from recent examinations or with a synopsis of recurrent findings.

The most common deficiencies noted were of institutions failing to monitor their CRE portfolios properly and failing to comply with the requirements of Part 365 of the FDIC Rules and Regulations—Real Estate Lending Standards (see text box, Major Provisions of Part 365). Other areas of concern were the lack of effective oversight of construction projects, weak appraisal review programs, inadequate knowledge of lending markets, and poor loan structuring. While noting such deficiencies, examiners also reported many best practices that mitigate the risk.

CRE Monitoring and Management Information Systems Can Mitigate Risk

Examiners indicated that many institutions have increased their exposure to CRE lending without a formal monitoring system or adequate consideration of concentration risk. Some institutions did not know what percentage of their CRE portfolio was concentrated in more risky speculative C&D loans. Common deficiencies include

- Failure to consider or establish limits of exposure by type (e.g., condominium conversion, multifamily) or geographic market;
- Preparing reports of activity for senior management and the board of directors that do not provide sufficient

Major Provisions of Part 365—Real Estate Lending Standards[a]

- Written lending policies must establish
  - Diversification standards
  - Prudent underwriting standards that include clear and measurable loan-to-value limits
  - Loan administration procedures
  - Guidelines for monitoring loan policy compliance
- Market conditions must be monitored.
- Real estate lending policies should reflect consideration of the Interagency Guidelines for Real Estate Lending Policies (Appendix A to Part 365).

[a] Part 365 of the FDIC Rules and Regulations prescribes real estate lending standards to be used in a state nonmember bank's lending policies. See 12 CFR 365.2.

information to enable management to make informed decisions;

- Inadequate or nonexistent interest rate stress testing; and
- Failure to prepare timely or consistent concentrations reports.

This lack of oversight often caused examiners to cite contraventions of FDIC Rules and Regulations, specifically Appendix A to Part 365—Interagency Guidelines for Real Estate Lending Policies[4] at safety and soundness examinations. Examiners provided examples of institutions failing to monitor the loan portfolio appropriately for loan-to-value exceptions (see text box, Supervisory Loan-to-Value Limits). The following were common deficiencies:

- Failure to track exceptions;
- Failure to track the aggregate amount of loans in excess of loan-to-value limits;
- Originating numerous loans in excess of loan-to-value limits without documentation of credit factors that support the underwriting decision;
- Failure to consider commitment amounts when computing loan-to-value limits;
- Underwriting raw land loans in excess of prescribed loan-to-value limits based on "As Complete" appraised values; and
- Failure to provide timely and sufficiently complete reports to the board of directors as required by Part 365.

There were numerous reports of institutions whose aggregate amount of all loans in excess of the supervisory loan-to-value limits routinely exceeded 100 percent of total capital, in contravention of Appendix A of Part 365.[5] Several examiners reported that banks were granting extensions of credit of up to 75 percent of value to acquire raw land although the borrowers had no plans to develop this property in the near term. Certain institutions in high-growth areas had concentrations in excess of 150 percent of total capital for land development loans, but for purposes of measuring risk, internal monitoring did not differentiate

Supervisory Loan-to-Value Limits[a]

Institutions should establish their own internal loan-to-value limits for real estate loans. These internal limits should not exceed the following supervisory limits:

Loan category	Loan-to-value limit (percent)
Raw land	65
Land development	75
Construction:	
Commercial, multifamily,[b] and other nonresidential	80
1- to 4-family residential	85
Improved property	85
Owner-occupied 1- to 4-family and home equity[c]	–

[a] Appendix A to Part 365 of FDIC Rules and Regulations, www.fdic.gov/regulations/laws/rules/2000-8700.html#2000appendixatopart365.

[b] Multifamily construction includes condominiums and cooperatives.

[c] A loan-to-value limit has not been established for permanent mortgage or home equity loans on owner-occupied 1- to 4-family residential property. However, for any such loan with a loan-to-value ratio that equals or exceeds 90 percent at origination, an institution should require appropriate credit enhancement in the form of either mortgage insurance or readily marketable collateral.

[4] Appendix A identifies prudent practices an institution should include in its policies in the areas of loan portfolio management, underwriting, and administration. In addition, the appendix provides supervisory loan-to-value limits. See www.fdic.gov/regulations/laws/rules/2000-8700.html#2000appendixatopart365.

[5] Appendix A to Part 365 requires that the aggregate amount of loans in excess of the supervisory loan-to-value limits should not exceed 100 percent of total capital. Within this aggregate limit, total loans for commercial, agricultural, multifamily, or other non-1–4 family residential properties should not exceed 30 percent of total capital. An institution that approaches or exceeds the aggregate limits is subject to increased supervisory scrutiny.

continued from pg. 29

actual land development loans from raw land loans or speculative investment land loans.

Mitigation Practices. Despite these weaknesses, examiners cited a number of best practices focusing on effective internal controls and management information systems that monitor the activity and control the associated risk. Establishing policy limits appropriate to the bank's size, sophistication, and appetite for risk is fundamental to managing CRE concentration risk. The primary element of a useful monitoring process is the integration of quantitative and qualitative data that provide a summary of the overall activities in the CRE portfolio in order to measure risk across all dimensions of the portfolio. The size of the portfolio should not be the sole consideration. Factors such as geographic diversification, types of property held as collateral, and underwriting practices should be considered in the development of any risk management process.

Institutions with active and meaningful monitoring programs depended on a number of in-depth reports that were reviewed periodically either by committees of the board of directors or by the full board. In addition, some institutions included these reports as a regular agenda item at monthly board meetings. The most common quantitative reports included descriptions of CRE concentration by type and geographic diversification. Limits were established, and the reports provided a mechanism to review exposure and design risk mitigation strategies. Some of the qualitative reports included quarterly raw land, lot development, and construction loan reports with a detailed narrative summary of each project's current status, percentage of completion, expected completion date, and any completion or absorption issues. Repayment sources were described, as were other risk mitigation items of interest.

Market Analysis Is Often Overlooked

Examiners report that management could improve its practices of monitoring market conditions in its lending areas. There were numerous reports of institutions that either did not prepare a market analysis or prepared one that was incomplete or flawed.

Mitigation Practices. Some boards of directors, directors' committees, or loan committees mitigate this risk by maintaining contact with real estate brokers, developers, and builders and using the resulting information to establish maximum exposure limits.

Real estate markets and economic cycles are dynamic, and policy guidelines that were once adequate may, over time, become overly liberal. Management needs to monitor both local and regional economic trends, as well as any national trend that could impact the local economy, and adjust policy guidelines accordingly. Market analysis should include a review of concentrations by type of property compared to projects throughout the market, including completed, pipeline, and proposed developments.

Lenient Terms and Weak Loan Structuring Carry Risks

Examiners described a number of incidents in which institutions had relaxed underwriting standards for CRE loans. Conditions included

- Overreliance on collateral values instead of cash flow,
- Liberal use of interest reserves,
- Loans with one- to two-year balloon maturities secured by undeveloped land, and
- Unsecured loans and letters of credit granted for the purpose of investing in units of condominium projects (located primarily in the Southeastern United States).

Examiners also reported that many borrowers were not required or were unable to put equity into development projects, and material deposit relationships were either not required or unavailable.

Mitigation Practices. Repayment of any CRE loan is dependent upon the borrower's ability to produce cash flow from the project through either rental income or the sale of the property. Collateral value, while possibly providing certain protection, does not provide cash flow. Sound lending guidelines should help reduce exposure to borrowers with insufficient cash flow to meet the repayment terms. Along with good credit selection, an institution should develop strong policy guidelines with respect to loan-to-values, allowable exceptions, and reporting requirements. Slow or no principal reduction can erode the institution's collateral protection by allowing the loan-to-value to increase above prudent levels in depressed real estate markets. This is especially true of speculative construction lending, where slowing sales may prevent borrowers from carrying the debt for a period of time.

Oversight of the Appraisal Process May Be Weak

Examination findings indicated that oversight of the appraisal process was lacking in some institutions. Problems included

- Inadequate or missing internal reviews of appraisals,
- Violations of FDIC Rules and Regulations concerning appraisals (12 CFR 323—Appraisals[6]) for absent or inadequate appraisals,
- Funding loans prior to receipt of appraisals, and
- Including the proposed loan amounts on appraisal engagement letters.

In certain markets, banks had extended funds predicated on expected future gross sell-out values of condominium conversion and construction, as well as other development projects.

Mitigation Practices. Institutions that avoided these problems generally had strong internal appraisal review programs that provided an independent analysis of appraisals or internal evaluations prior to funding. In addition, these institutions reviewed the qualifications of their appraisers on an ongoing basis and removed those that did not consistently provide a product that conformed to the requirements outlined in 12 CFR 323—Appraisals. Loan policies and practices established guidelines for types of appraisals required on the basis of the type of project (speculative versus owner-occupied). These internal requirements were often more conservative than the standards established by 12 CFR 323.

Conclusions

Anecdotal information provided by the examiners suggests that many institutions would benefit from enhancements to their existing monitoring systems. The recently reported softening of real estate markets also implies that increased attention is warranted, given the risk exposure inherent in CRE lending. A robust program of measuring and monitoring CRE portfolios, with special attention to C&D exposure, is fundamental to effective risk mitigation.

While examiners have noted some degree of deterioration in underwriting practices, these practices have not adversely impacted the overall condition of most of the institutions. Capital levels are reported to be high, with over 99 percent of all insured institutions placing in the highest regulatory capital category at year-end 2005.[7] The levels of adversely

[6] See www.fdic.gov/regulations/laws/rules/2000-4300.html.

[7] *FDIC Quarterly Banking Profile,* Division of Insurance and Research, December 2005.

From the Examiner's Desk . . .

continued from pg. 31

classified assets and past-due loans are nominal, and earnings performance is strong, with net interest income providing most of the profit reported. A strong CRE market has also mitigated the potential ill effects of weakening lending standards over the past few years.

Where significant deficiencies were found, examiners made recommendations for corrective action. Many institutions initiated their own corrective action programs based upon those recommendations or upon the advice of internal and external auditors. In very few cases, informal and formal enforcement actions were necessary. On December 6, 2006, after careful consideration of comments received on proposed guidance on commercial real estate lending issued on January 13, 2006,[8] the Federal banking agencies issued Final Guidance on Concentrations in Commercial Real Estate Lending.[9] The guidance reminds institutions that strong risk management practices and appropriate levels of capital are important elements of a sound lending progrm and reinforces and enhances existing regulations and guidelines for safe and sound sound real estate lending. Many of the best practices identified in this article reflect long-standing supervisory expectations presented in Table 2.

Marianne Lester
Examiner, Shelby, AL

Lawrence J. Nicastro
Examiner, Atlanta, GA

Tracy E. Fitzgerald
Examination Specialist, Tulsa, OK

Brian D. Regan
Examiner (Retired), Sacramento, CA

Table 2

Sound Practices for Commercial Real Estate Portfolio Oversight

- ✓ The board of directors should approve the scope of lending activities and the way real estate loans are made, serviced, and collected. Market conditions, concentrations, and lending activity should be monitored, and timely and adequate reports should be made to the board of directors.
- ✓ Internal and external factors should be considered in the formulation of loan policies and of a strategic plan considering the size and financial condition of the institution, the expertise and size of the lending staff, and market conditions.
- ✓ Prudent underwriting standards should be developed that consider relevant credit factors, including the capacity of the borrower, income from the underlying property to service the debt, the value of collateral, the creditworthiness of the borrower, the level of equity invested, and any secondary sources of repayment.
- ✓ Lending policies should reflect the level of risk that is acceptable to the board of directors and provide clear and measurable limits that include the maximum loan amount and maturities by type of property, amortization schedules, pricing structure for different types of real estate loans, loan-to-value limits by type of property, pre-leasing and pre-sale requirements, requirements for takeout commitments, and minimum covenants for loan agreements.
- ✓ Loan administration procedures should address the type and frequency of financial statements required, type and frequency of collateral evaluations, collateral administration, requirements for adequate construction inspections and loan disbursements, and collections and foreclosure.

Refer to *Part 365 of the FDIC Rules and Regulations*—***Real Estate Lending Standards; Appendix A to Part 365—Interagency Guidelines for Real Estate Lending Policies.***

[8] FIL-4-2005, *Commercial Real Estate Lending Proposed Interagency Guidance,* January 13, 2006, www.fdic.gov/news/news/financial/2006/fil06004.html.

[9] PR-114-2006, *Joint Release/Federal Banking Agencies Issue Final Guidance on Concentrations in Commercial Real Estate Lending,* December 6, 2006, www.fdic.gov/news/news/press/2006/pr06114.html.

Accounting News: Auditor Independence

This regular feature focuses on topics of critical importance to bank accounting. Comments on this column and suggestions for future columns can be e-mailed to ***SupervisoryJournal@fdic.gov.***

The words "independent" and "independence" are often used in conjunction with the services certified public accountants (CPAs or external auditors) provide to their clients, including insured depository institutions (banks or financial institutions). When CPAs and their firms provide certain services that require them to be independent, such as audits of financial statements and audits of internal control over financial reporting, they are referred to as independent public accountants, independent auditors, or external auditors. But what does "independence" mean when external auditors provide these services? It is useful for examiners to have an understanding of the general principles and concepts embodied in "independence" because examiners are expected to review and evaluate institutions' external auditing programs. This article summarizes existing professional standards for auditor independence, including recent developments regarding tax services and contingent fees as well as the use of limitation of liability clauses in engagement letters.

The American Institute of Certified Public Accountants' (AICPA) *Conceptual Framework for AICPA Independence Standards* (Conceptual Framework) defines independence as

a. Independence of mind. The state of mind that permits the performance of an attest service without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.

b. Independence in appearance. The avoidance of circumstances that would cause a reasonable and informed third party, having knowledge of relevant information, including safeguards applied, to reasonably conclude that the integrity, objectivity, or professional skepticism of a firm or member of the attest engagement team has been compromised.[1]

For financial institutions, the most common services performed by external auditors that require independence include audits of financial statements, audits of internal control over financial reporting, and attestations on management's assessment of internal control over financial reporting. Therefore, the primary focus of this discussion will be on the independence standards related to financial statement audits and internal control audits/attestations.

Importance of Auditor Independence

Why is it important for the external auditor to be independent? A properly conducted audit provides an independent and objective view of the reliability of a financial institution's financial statements. The external auditor's objective in an audit is to form an opinion on the financial statements taken as a whole. When planning and performing the

[1] ET Section 100.01, *Conceptual Framework for AICPA Independence Standards,* paragraph 6. The Conceptual Framework for AICPA Independence Standards was adopted by the AICPA's Professional Ethics Executive Committee (PEEC) on January 30, 2006, and is available on the AICPA's website. See www.aicpa.org/download/ethics/Ethics_Interpretation_101-1_and_Conceptual_Framework.pdf.

continued from pg. 33

audit, the external auditor considers the financial institution's internal control over financial reporting. Generally, the external auditor communicates any identified deficiencies in internal control to management, which enables management to take appropriate corrective action. In addition, certain financial institutions are required to file audited financial statements and internal control audit/attestation reports with one or more of the Federal banking agencies.[2] The Federal Financial Institutions Examination Council's (FFIEC) Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations[3] notes that "an institution's internal and external audit programs are critical to its safety and soundness." The FFIEC's policy statement also says that an effective external auditing program "can improve the safety and soundness of an institution substantially and lessen the risk the institution poses to the insurance funds administered by the Federal Deposit Insurance Corporation."

Many financial institutions are required to have their financial statements audited, and others voluntarily choose to undergo such audits. For example, banks and savings associations with $500 million or more in total assets are required to have annual independent audits.[4] Certain savings associations (for example, those with a CAMELS rating of 3, 4, or 5) and savings and loan holding companies are also required by the Office of Thrift Supervision (OTS) regulations to have annual independent audits.[5] The Agencies rely on the results of audits as part of their assessment of the safety and soundness of a financial institution.

Reliable financial reports, such as audited financial statements, are necessary for a financial institution to raise capital. They provide data on an institution's financial position and results of operations for stockholders, depositors, and other funds providers, borrowers, and potential investors. Such information is critical to effective market discipline of an institution.

For audits to be effective, the external auditors must be independent in both fact and appearance, and must perform all necessary procedures to comply with auditing and attestation standards established by either the AICPA or, if applicable, the Public Company Accounting Oversight Board (PCAOB).

Independence Standard-Setters

Currently, the independence standard-setters include the AICPA, the U.S. Securities and Exchange Commission (SEC), and the PCAOB. Depending upon the audit client, an external auditor is subject to the independence standards issued by one or more of these standard-setters. For nonpublic financial institutions[6] that are not required to have annual independent audits pursuant to either Part 363 of the FDIC regulations or Section 562.4 of the OTS regulations, the external auditor must comply with the AICPA's independence

[2] The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), collectively referred to as the Agencies.

[3] Published in the *Federal Register* on September 28, 1999 (64 FR 52319).

[4] See Section 36(d) of the Federal Deposit Insurance Act (12 U.S.C. 1831m) and Sections 363.1(a) and 363.2(a) of Part 363 of the FDIC's regulations (12 CFR 363).

[5] See OTS regulation at 12 CFR 562.4.

[6] Nonpublic financial institutions are companies that are not, or whose parent companies are not, subject to the reporting requirements of the Securities Exchange Act of 1934.

standards; the financial institution's external auditor is not required to comply with the independence standards of the SEC and the PCAOB.

In contrast, for financial institutions subject to the audit requirements either in Part 363 of the FDIC regulations (i.e., those with $500 million or more in total assets) or in Section 562.4 of the OTS regulations, the external auditor should be in compliance with the AICPA's Code of Professional Conduct and also meet the independence requirements and interpretations of the SEC and its staff. The SEC's independence requirements encompass the independence standards and rules adopted by the PCAOB and approved by the SEC.

For financial institutions and bank holding companies that are public companies,[7] regardless of size, the external auditor should be in compliance with the SEC's and the PCAOB's independence standards as well as the AICPA's independence standards.

The table below illustrates the applicability of the AICPA, SEC, and PCAOB independence standards.

Independence Standards

The independence standards and interpretations of the AICPA, the SEC, and the PCAOB[8] set forth rules and provide guidance regarding many facets of the external auditor's relationship with and

Applicability of Auditor Independence Standards	AICPA Independence Standards	SEC Independence Standards	PCAOB Independence Standards
Scenario 1 Nonpublic institutions **not** subject to Part 363 of the FDIC regulations or Section 562.4 of the OTS regulations	YES	NO	NO
Scenario 2 Public and nonpublic institutions subject to Part 363 of the FDIC regulations or Section 562.4 of the OTS regulations	YES	YES	YES
Scenario 3 Institutions and holding companies that are public companies (regardless of size)	YES	YES	YES

[7] Public companies are companies, or subsidiaries of companies, that are subject to the reporting requirements of the Securities Exchange Act of 1934.

[8] For the AICPA, refer to the AICPA's Code of Professional Conduct, ET Section 101, Independence; ET Section 191, Ethics Rulings on Independence, Integrity, and Objectivity; and Interpretations under Rule 101 - Independence. For the SEC, refer to Rule 2-01 of Regulation S-X (17 CFR Section 210.2-01); the Codification of Financial Reporting Policies - Section 600 - Matters Relating to Independent Accountants; and the Office of the Chief Accountant's Frequently Asked Questions: Application of the Commission's Rules on Auditor Independence. See www.sec.gov/info/accountants/ocafaqaudind121304.htm. For the PCAOB, refer to the following PCAOB Rules and Professional Standards: Rule 3500T—Interim Ethics Standards; Rule 3520—Auditor Independence; Rule 3521—Contingent Fees; Rule 3522—Tax Transactions; Rule 3523—Tax Services for Persons in Financial Reporting Oversight Roles; Rule 3524—Audit Committee Pre-approval of Certain Tax Services; and Rule 3600T—Interim Independence Standards. See www.pcaobus.org/Rules/Rules of_the_Board/Section_3.pdf.

continued from pg. 35

performance of services for an audit client, including

(1) which members of the audit engagement team are subject to the independence rules (referred to as "Covered Members or Persons");

(2) financial relationships of Covered Members/Persons or their immediate families;

(3) financial interests in nonclients having investor or investee relationships with clients;

(4) financial interests of audit firm partners and professional employees, their immediate families, and close relatives;

(5) employment relationships of the audit firm's partners, professional employees, and their immediate family and close relatives; and

(6) the performance of nonaudit services to audit clients.

However, while the independence rules and interpretations provide guidance and establish a framework for auditors to follow, they do not—nor were they meant or designed to—consider all circumstances that raise independence concerns.

The AICPA, the SEC, and the PCAOB also require audit firms to have quality controls for their audit practices.[9] The AICPA's standards define quality control as "a process to provide the firm with reasonable assurance that its personnel comply with applicable professional standards and the firm's standards of quality."[10] The AICPA's standards further set forth five broad elements of appropriate quality control in a public accounting firm, which relate to maintaining independence, integrity, and objectivity; managing personnel; establishing guidelines for accepting and continuing clients; performing engagements; and monitoring the existing quality control policies and procedures.

Audit firms that provide audit/attest services to nonpublic clients are subject to peer reviews performed in accordance with applicable AICPA standards, and audit firms that provide audit/attest services to public clients are subject to inspections performed by the PCAOB.[11] Peer reviews and inspections include an examination and/or review of an audit firm's quality controls. However, for any particular audit client, the most visible and apparent independence concerns would be manifested in the services (audit and nonaudit) provided to the client.

AICPA Independence Standards

The AICPA's professional standards require audit firms, including the firms' partners and professional employees, to be independent in accordance with AICPA Rule 101, *Independence,*[12] of the Code of Professional Conduct (Rule 101) whenever an audit firm performs an attest service for a client. Attest services include financial statement audits, financial statement reviews, and other attest

[9] For the AICPA, refer to its Quality Control (QC) Standards, QC Section 20—System of Quality Control for a CPA Firm's Accounting and Auditing Practice; QC Section 30—Monitoring a CPA Firm's Accounting and Auditing Practice; and QC Section 40—The Personnel Management Element of a Firm's System of Quality Control—Competencies Required by a Practitioner-in-Charge of an Attest Engagement. On July 28, 2006, the AICPA's Auditing Standards Board issued an Exposure Draft of a proposed Statement of Quality Control Standards that will replace all the existing QC Standards. For the SEC, refer to Rule 2-01(d) of Regulation S-X. For the PCAOB, refer to Rule 3400T—Interim Quality Control Standards—of its Rules and Professional Standards.

[10] Refer to QC Section 20.03 of the AICPA's QC Standards.

[11] The public portions of these peer review and inspection reports are available on the AICPA's and the PCAOB's websites. See www.aicpa.org/centerprp/publicfile01.htm and www.pcaobus.org/Inspections/Public_Reports/index.aspx, respectively.

[12] AICPA, *Professional Standards,* ET Section 101.01.

services as defined in the AICPA's Statements on Standards for Attestation Engagements. For all financial institution audits (whether the audit is voluntary or required; whether or not the financial institution is subject to Part 363 of the FDIC regulations or Section 562.4 of the OTS regulations; and whether the financial institution is a public or a nonpublic company), the financial institution's external auditor must comply with the AICPA's Independence Standards.

Independence is not required when an audit firm performs services that are not attest services, if those services—for example, tax preparation and consulting services—are the only services an audit firm provides to a particular client. However, Rule 101 requires an auditor to comply with the independence regulations of authoritative regulatory bodies (such as the SEC and state boards of accountancy) when the auditor performs nonattest services for an attest client and is required to be independent of the client under the regulations of the applicable regulatory body. The auditor's failure to comply with the nonattest services provisions contained in the independence rules of the applicable regulatory body that are more restrictive than the provisions of Rule 101 would constitute a violation of Rule 101.

The AICPA's Rule 101 imposes limits on the nature and scope of nonattest services an audit firm may provide to an audit (attest) client. Rule 101 specifically addresses the following nonattest services:

- Bookkeeping services,
- Payroll and other disbursement services,
- Internal audit assistance,
- Benefit plan administration,
- Investment advisory or management services,
- Tax services,
- Corporate finance consulting or advisory services,
- Appraisal, valuation, or actuarial services,
- Executive or employee search services,
- Business risk consulting, and
- Information systems design, installation, or integration.

Before an audit firm performs nonattest services for an audit client, the AICPA's Rule 101 requires the audit firm to meet certain general requirements. If certain nonattest services (for example, internal audit assistance) are to be performed, the audit firm must also satisfy service-specific requirements. In cases where the general or service-specific requirements for nonattest services are not met, the audit firm's independence would be impaired with respect to the attest services the audit firm provides to that audit client.[13]

The general requirements for performing nonattest services for audit clients under Rule 101 include

- The audit firm should not perform management functions or make management decisions for the audit client.
- The audit client must agree to perform the following functions in connection with the nonattest services:
  - Make all management decisions and perform all management functions;
  - Designate an individual who possesses suitable knowledge and/or experience to oversee the services;
  - Evaluate the adequacy and results of the services performed;
  - Accept responsibility for the results of the services; and
  - Establish and maintain internal controls, including monitoring ongoing activities.

[13] AICPA, *Professional Standards,* ET Section 101.05.

continued from pg. 37

- Before performing nonattest services, the audit firm should establish and document the following in writing with the client:
  - Objectives of the engagement,
  - Services to be performed,
  - Client's acceptance of its responsibilities,
  - Audit firms' responsibilities, and
  - Any limitation of the engagement.

Internal audit services, sometimes referred to as "internal audit outsourcing," are one of the more common nonaudit services audit firms provide to financial institutions. In evaluating whether independence would be impaired with respect to an audit client that is not a public company and is not subject to Part 363 of the FDIC regulations or Section 562.4 of the OTS regulations, the nature of the internal audit services to be provided to the client needs to be considered.[14] Assisting the client in performing financial and operational internal audit activities would impair independence unless the external auditor takes appropriate steps to ensure that the client understands its responsibilities for establishing and maintaining the internal control system and directing the internal audit function, including the management thereof. Accordingly, any outsourcing of the internal audit function to the external auditor whereby the external auditor in effect manages the internal audit activities of the client would impair independence.

In addition to the general requirements of Rule 101 for performing nonattest services for an audit client, the external auditor should ensure that client management

- Designates an individual or individuals who possess suitable skill, knowledge, and/or experience to be responsible for the internal audit function;
- Determines the scope, risk, and frequency of internal audit activities, including those to be performed by the external auditor providing internal audit assistance services;
- Evaluates the findings and results arising from the internal audit activities; and
- Evaluates the adequacy of the audit procedures performed and the findings resulting from the performance of those procedures by, among other things, obtaining reports from the external auditor.

As previously indicated, it is impossible to enumerate all circumstances in which the appearance of independence might be questioned. In the absence of an independence interpretation or ruling under the AICPA's rules that addresses a particular circumstance, a member (auditor) should consider whether that circumstance would lead a reasonable person aware of all of the relevant facts to conclude there is an unacceptable threat to the member's and the firm's independence. The AICPA's Conceptual Framework provides a risk-based approach for making that evaluation. The risk-based approach involves three steps: (1) the auditor should identify and evaluate threats to independence; (2) the auditor should determine whether safeguards already eliminate or sufficiently mitigate identified threats and whether threats that have not yet been mitigated can be eliminated or sufficiently mitigated by safeguards; and (3) if no safeguards are available to eliminate an unacceptable threat or reduce it to an acceptable level, the auditor should conclude that independence would be considered impaired.[15]

[14] For audit clients that are public companies or that are subject to Part 363 of the FDIC regulations or Section 562.4 of the OTS regulations, internal audit outsourcing to the external auditor is generally impermissible under the SEC's independence rules.

[15] ET Section 100.01, Conceptual Framework for AICPA Independence Standards, paragraph 5.

Many different circumstances (or combinations of circumstances) can create threats to an auditor's independence. It is impossible to identify every situation that threatens independence. However, seven broad categories of threats should always be evaluated when threats to independence are being identified and assessed. They are (1) self review (auditors reviewing the results of their own nonattest work); (2) advocacy (actions by the auditor to promote the client's interests or position); (3) adverse interest (actions or interests between the auditor and the client that are in opposition); (4) familiarity (auditors having a close or long-standing relationship with an attest client); (5) undue influence (attempts by the client's management to coerce or exercise excessive influence over the auditor); (6) financial self-interest (potential benefit to the auditor from a financial interest in, or from some other financial relationship with the client); and (7) management participation (the auditor taking the role of client management or performing management functions on behalf of the client).[16]

SEC Independence Standards

The SEC's independence rules are set forth in Rule 2-01 of Regulation S-X (Rule 2-01).[17] Rule 2-01 was amended in January 2003 by Release No. 33-8183, *Strengthening the Commission's Requirements Regarding Auditor Independence,* to fulfill the mandate of Title II of the Sarbanes-Oxley Act of 2002. To assist practitioners in complying with the SEC's independence rules, the SEC's Office of the Chief Accountant has also issued and periodically updates a document titled *Application of the Commission's Rules on Auditor Independence—Frequently Asked Questions.*

Unlike the AICPA's independence rules, the SEC's independence rules provide that an accountant is not independent if, at any point during the audit and professional engagement period,[18] the accountant provides any of the following nonaudit services to an audit client:

- Bookkeeping or other services related to the accounting records or financial statements of the audit client;
- Financial information systems design and implementation;
- Appraisal or valuation services, fairness opinions, or contribution-in-kind reports;
- Actuarial services;
- Internal audit outsourcing services;
- Management functions;
- Human resources services;
- Broker-dealer, investment adviser, or investment banking services;
- Legal services; or
- Expert services unrelated to the audit.

The SEC's rules state that bookkeeping, financial information systems design and implementation, appraisal or valuation services, actuarial services, and internal audit outsourcing services

[16] ET Section 100.01, Conceptual Framework for AICPA Independence Standards, paragraphs 12 to 19.

[17] See 17 CFR 210.2-01.

[18] Under Rule 2-01(f)(5), the audit and professional engagement period includes both: (1) the period covered by any financial statements being audited or reviewed (the "audit period"); and (2) the period of the engagement to audit or review the audit client's financial statements to prepare a report filed with the SEC (the "professional engagement period"). The professional engagement period begins when the accountant either signs an initial engagement letter (or other agreement to review or audit a client's financial statements) or begins audit, review, or attest procedures, whichever is earlier; and the professional engagement period ends when the audit client or the accountant notifies the SEC that the client is no longer that accountant's audit client.

continued from pg. 39

are prohibited "unless it is reasonable to conclude that the results of these services will not be subject to audit procedures during an audit of the audit client's financial statements."[19] This limited exception to the general prohibition regarding nonaudit services is quite narrow in the SEC's view, establishing a rebuttable presumption that these services are subject to audit procedures. In other words, the SEC presumes that, when an accountant audits an audit client's financial statements, the accountant will end up auditing the work he or she performed when rendering the aforementioned nonaudit services for the audit client.

Like the AICPA's independence rules, the SEC's independence rules do not purport to consider all circumstances that raise independence concerns. In this regard, the SEC considers whether a relationship or the provision of a service (a) creates a mutual or conflicting interest between the accountant and the audit client (b) places the accountant in a position of auditing his or her own work (c) results in the accountant acting as management or an employee of the audit client or (d) places the accountant in a position of being an advocate for the audit client.

The SEC will not recognize an accountant as independent, with respect to an audit client, if the accountant is not, or a reasonable investor with knowledge of all relevant facts and circumstances would conclude that the accountant is not, capable of exercising objective and impartial judgment on all issues encompassed within the accountant's engagement. In determining whether an accountant is independent, the SEC will consider all relevant circumstances, including relationships between the accountant and the audit client, and not just those relating to reports filed with the SEC.

PCAOB Independence Standards

Title I of the Sarbanes-Oxley Act of 2002 established the PCAOB and charged it with the responsibility of overseeing the audits of public companies that are subject to the U.S. Federal securities laws. Only accounting firms that register with the PCAOB (registered public accounting firms) may audit public companies. The PCAOB's duties include the establishment of auditing, quality control, ethics, independence, and other standards relating to public company audits.

The PCAOB adopted all of the independence standards described in the AICPA's Code of Professional Conduct Rule 101, and the interpretations and rulings thereunder, as in existence on April 16, 2003, as the PCAOB's Interim Independence Standards. These Interim Independence Standards also include Standards Nos. 1, 2, and 3 and Interpretations 99-1, 00-1, and 00-2 of the former Independence Standards Board. Generally, this means that the PCAOB applies the independence standards/principles discussed under the "AICPA Independence Standards" section of this article to registered public accounting firms.

The PCAOB's Interim Independence Standards do not supersede the SEC's auditor independence rules. Therefore, to the extent that a provision of the SEC's rules is more or less restrictive than a provision of the PCAOB's Interim Independence Standards, a registered public accounting firm must comply with the more restrictive rule.

The PCAOB's interim standards will remain in effect until modified or superseded, either by PCAOB action approved by the SEC, or by SEC action pursuant to its independent authority under the Federal securities laws to establish independence standards for auditors of public companies.

[19] See Rule 2-01(c)(4)(i) through (v) of SEC Regulation S-X (17 CFR 210-01).

Recent Developments in Auditor Independence

Recent AICPA Developments

On September 8, 2006, the AICPA's Professional Ethics Executive Committee (PEEC) re-exposed its Proposed Interpretation 101-16 under Rule 101: Indemnification, Limitation of Liability, and ADR Clauses in Engagement Letters. The comment period for the revised Exposure Draft (ED) ended on December 8, 2006. The AICPA's initial ED on this subject was issued on September 15, 2005.

The revised ED is significantly different from the September 2005 ED. The revised ED has an underlying principle that would permit external auditors to include indemnification and limitation of liability provisions in audit engagement letters if such provisions are contingent upon the related services being performed in compliance with professional standards, in all material respects. However, the revised ED would also permit certain indemnification and limitation of liability provisions to be included in audit engagement letters and not be subject to the underlying principle. For example, under the revised ED, the audit client could waive the right to seek punitive damages and indemnify the auditor for third-party punitive damage awards, the time period for the client to file a claim for damages could be limited, and the client's right to assign or transfer a claim could be limited.

On February 3, 2006, the Federal banking agencies, together with the National Credit Union Administration, issued an Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters.[20] The Interagency Advisory applies to audit engagement letters executed on or after February 9, 2006, and provides that the inclusion of indemnification and limitation of liability provisions in external audit engagement letters will generally be considered an unsafe and unsound practice. Appendix A of the Interagency Advisory contains examples of unsafe and unsound limitation of liability provisions.

While the Interagency Advisory addresses indemnification and limitation of liability from a safety and soundness perspective, rather than from an auditor independence perspective, it is fairly consistent with the PEEC's September 2005 ED. However, the PEEC's September 2006 revised ED is generally inconsistent with its September 2005 ED and the Interagency Advisory.

Recent PCAOB Developments

On April 19, 2006, the SEC approved the PCAOB's proposed ethics and independence rules concerning independence, tax services, and contingent fees. These rules have varying effective dates, most of which are in 2006.

Besides establishing general rules with respect to ethics and independence, these new PCAOB rules restrict certain types of tax services a registered public accounting firm may provide to an audit client and certain members of the client's management, and prohibit contingent fee arrangements for any services a registered public accounting firm provides to an audit client, in order for the firm to maintain its independence with respect to that client. Nonpublic financial institutions subject to Part 363 of the FDIC regulations or Section 562.4 of the OTS regulations and their auditors

[20] FIL-13-2006, External Audit Engagement Letters: Unsafe and Unsound Use of Limitation of Liability Provisions, February 9, 2006, www.fdic.gov/news/news/financial/2006/fil06013.html. Also see the February 3, 2006, Joint Press Release, www.fdic.gov/news/news/press/2006/pr06011.html and the *Federal Register,* Volume 71, Page 6847, www.fdic.gov/regulations/laws/federal/2006/06notice29.pdf.

continued from pg. 41

should note that these new independence rules from the PCAOB apply to institutions' external auditors.

Examiner Considerations

Auditor independence is the cornerstone for CPAs and audit firms that provide audit/attestation services to financial institutions. Sometimes concerns regarding an auditor's independence with respect to a specific audit client are "black and white" and a decision as to whether the auditor's independence is impaired can be reached rather easily. However, many times, the resolution of concerns regarding auditor independence requires a thorough and complete analysis of all of the relevant facts and circumstances before a conclusion can be made. In the end, ensuring auditor independence is a responsibility of both the auditor and the client financial institution.

Accordingly, as noted in the February 2006 Interagency Advisory and the 1999 Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations, examiners should consider an institution's policies and processes surrounding its external auditing program, including those for determining whether the auditor maintains appropriate independence in its relationship with the institution under applicable professional standards, when they evaluate the institution's program. Examiners should also review external audit engagement letters to determine whether they include any limitation of liability provisions of the types that are deemed unsafe and unsound by the Interagency Advisory.

Harrison E. Greene, Jr.
CPA, CBA, Accounting and Securities Disclosure Section
Washington, DC

Overview of Selected Regulations and Supervisory Guidance

This section provides an overview of recently released regulations and supervisory guidance, arranged in reverse chronological order. Press Release (PR) or Financial Institution Letter (FIL) designations are included so the reader may obtain more information.

Subject	Summary
Comments Requested on Proposed *Illustrations of Consumer Information for Nontraditional Mortgage Product Risks* (PR-93-2006, October 18, 2006; FIL-90-2006, October 5, 2006; and *Federal Register* Vol. 71, No. 192, p. 58672, October 4, 2006)	The FDIC, the Board of Governors of the Federal Reserve System (Federal Reserve Board), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA) (collectively, the Federal financial regulatory agencies) sought comment on proposed *Illustrations of Consumer Information for Nontraditional Mortgage Product Risks* (the illustrations). The illustrations were intended to assist institutions in implementing the consumer protection portion of the *Interagency Guidance on Nontraditional Mortgage Product Risks.* Comments were due December 4, 2006.
Final Rule Issued to Provide One-Time Assessment Credits to Insured Institutions (PR-91-2006, October 10, 2006; FIL-93-2006, October 18, 2006; and *Federal Register* Vol. 71, No. 201, p. 61374, October 18, 2006)	The FDIC issued the final rule to implement the One-Time Assessment Credit, as required by the Federal Deposit Insurance Reform Act of 2005. Under this rule, eligible institutions will share in an aggregated one-time deposit insurance assessment credit of $4,707,580,238.19. The final rule took effect November 17, 2006.
Final Rule Issued on Assessment Dividends (FIL-92-2006, October 18, 2006; and *Federal Register* Vol. 71, No. 201, p. 61385, October 18, 2006)	The FDIC issued the final rule to implement assessment dividends, as required by the Federal Deposit Insurance Reform Act of 2005. The Act generally requires the FDIC to pay dividends from the Deposit Insurance Fund (DIF) to insured institutions when the DIF reserve ratio at the end of a calendar year exceeds 1.35 percent. The final rule takes effect January 1, 2007.
Interagency Guidance Issued on Nontraditional Mortgage Product Risks, and an Addendum to Credit Risk Management Guidance for Home Equity Lending Issued (PR-86-2006, September 29, 2006; FIL-89-2006, October 5, 2006; and *Federal Register* Vol. 71, No. 192, p. 58609, October 4, 2006)	The Federal financial regulatory agencies issued *Interagency Guidance on Nontraditional Mortgage Product Risk*s and an *Addendum to the Credit Risk Management Guidance for Home Equity Lending.* These documents describe how financial institutions should both address the risks associated with underwriting nontraditional mortgage loan products and provide consumers with clear and balanced information before they make a product or payment choice.
Final Rule Issued Covering Changes to Deposit Insurance Coverages (FIL-83-2006, September 18, 2006; and *Federal Register* Vol. 71, No. 176, p. 53547, September 12, 2006)	The FDIC Board of Directors permanently adopted the final rule implementing provisions of the Federal Deposit Insurance Reform Act of 2005 pertaining to deposit insurance coverage. The final rule took effect October 12, 2006.
Comments Requested on a Proposed Rule on Risk-Based Capital Standards: *Market Risk* (PR-82-2006, September 5, 2006; FIL-87-2006, September 25, 2006; and *Federal Register* Vol. 71, No. 185, p. 55958, September 25, 2006)	The FDIC, Federal Reserve Board, OCC, and OTS (collectively, the Federal bank and thrift regulatory agencies) jointly issued a notice of proposed rulemaking (NPR) on possible modifications to the risk-based capital standards for market risk. The proposed rule would incorporate improvements to the current trading book regime as proposed by the Basel Committee on Bank Supervision and the International Organization of Securities Commissions in the joint document *The Application of Basel II to Trading Activities and the Treatment of Double Default Effects,* published in July 2005. The proposed rule would also apply to certain savings associations, which currently are not covered under the rule. The FDIC will accept comments on the NPR through January 23, 2007.

Regulatory and Supervisory Roundup

continued from pg. 43

Comments Requested on a Proposed Rule on Risk-Based Capital Standards: *Advanced Capital Adequacy Framework* (PR-82-2006, September 5, 2006; FIL-86-2006, September 25, 2006; and *Federal Register* Vol. 71, No. 185, p. 55830, September 25, 2006)	The Federal bank and thrift regulatory agencies jointly issued and sought comment on an NPR concerning the domestic application of selected elements of the Basel II capital framework. The proposed rule would require some core banks, and permit other banks, to use an internal ratings-based approach to calculate regulatory credit risk capital requirements and an advanced measurement approach to calculate regulatory operational risk capital requirements. The FDIC will accept comments on the NPR through January 23, 2007.
Comments Requested on Wide-Ranging Issues Related to Industrial Loan Companies (PR-77-2006, August 17, 2006; FIL-79-2006, August 29, 2006; and *Federal Register* Vol. 71, No. 163, p. 49456, August 23, 2006)	The FDIC sought public comment on wide-ranging issues involving industrial loan company charters. Comments were due by October 10, 2006.
Frequently Asked Questions Published Regarding Authentication in an Internet Environment (FIL-77-2006, August 21, 2006)	The Federal Financial Institutions Examination Council (FFIEC) published frequently asked questions to assist financial institutions and their technology service providers in conforming to the FFIEC guidance entitled *Authentication in an Internet Banking Environment,* which was issued on October 12, 2005.
Revised *Bank Secrecy Act/Anti-Money Laundering Examination Manual* Released (FIL-71-2006, August 2, 2006)	The FFIEC released a revised *Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual* on July 28, 2006. The manual can be accessed on the FFIEC BSA/AML InfoBase at http://www.ffiec.gov/bsa_aml_infobase/default.htm.
Revisions Issued to the FDIC Statement of Policy Regarding the National Historic Preservation Act (FIL-70-2006, August 1, 2006; and *Federal Register* Vol. 71, No. 143, p. 42399, July 26, 2006)	The FDIC revised its Statement of Policy (SOP) Regarding the National Historic Preservation Act of 1966. The purpose of the SOP is to inform affected parties of the FDIC's practices in applying the requirements of the National Historic Preservation Act and its implementing regulations. The SOP is relevant to applications for deposit insurance for de novo institutions, applications for establishment of domestic branches, and applications for the relocation of domestic branches or main offices.
Comments Requested on Proposed Deposit Insurance Rules (PR-70-2006, July 11, 2006; FIL-65-2006, July 25, 2006; and *Federal Register* Vol. 71, No. 141, p. 41910, July 24, 2006)	The FDIC sought comment on three proposed rules. The first proposed rule would create a new system for risk-based assessments. The second proposed rule would set the designated reserve ratio at 1.25 percent. The third proposed rule would govern the penalties for failure to pay assessments. Comments on the first two proposed rules were due September 22, 2006; comments on the third proposed rule were due September 18, 2006.
Comments Requested on Proposed Guidelines for Identity Theft Procedures (PR-71-2006, July 18, 2006; FIL-64-2006, July 18, 2006; and *Federal Register* Vol. 71, No. 137, p. 40786, July 18, 2006)	The Federal financial regulatory agencies and the Federal Trade Commission requested public comment on the proposed regulation to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The proposed regulation would require financial institutions and creditors to adopt reasonable policies and procedures to indicate the possible existence of identity theft and to validate addresses under certain circumstances. Comments were due September 18, 2006.

Revisions Issued to the Uniform Standards of Professional Appraisal Practice (FIL-53-2006, June 23, 2006)	The Federal financial regulatory agencies issued a statement notifying regulated institutions of the Appraisal Standards Board's issuance of the 2006 version of the Uniform Standards of Professional Appraisal Practice. These changes were effective July 1, 2006.
Guidance Issued on Managing Risks in Relationships with Foreign-Based Third-Party Service Providers (FIL-52-2006, June 21, 2006)	The FDIC issued guidance to address the risks inherent in outsourcing relationships between U.S. financial institutions and foreign-based third-party service providers. The guidance outlines steps institutions should take to manage reputational, operational/transactional, compliance, strategic, and country risks.
Standard Flood Hazard Determination Form Updated (FIL-51-2006, June 21, 2006)	The FDIC notified FDIC-supervised institutions that the Federal Emergency Management Agency had issued a revised Standard Flood Hazard Determination Form, which included a new Office of Management and Budget control number and a revised expiration date of October 31, 2008. The form's format and content have not changed. Institutions were required to use the updated form beginning July 1, 2006.
Booklet Issued to Institutions on Lessons Learned from Hurricane Katrina (FIL-49-2006, June 15, 2006)	The FFIEC and the Conference of State Bank Supervisors jointly issued a booklet of the lessons that financial institutions learned in the aftermath of Hurricane Katrina. Institutions can use the booklet in preparing to respond to a catastrophic event. The booklet can be found at http://www.fdic.gov/regulations/resources/lessons/index.html.
Examination Procedures Issued for New Regulations on Medical Information (FIL-47-2006, May 25, 2006)	The FFIEC Task Force on Consumer Compliance issued examination procedures to assess compliance with the medical information regulations that became effective on April 1, 2006. The regulations implement the Protection of Medical Information provisions of the Fair Credit Reporting Act, as amended by the FACT Act. The new procedures were effective May 25, 2006.
Comments Requested on a Revised Statement Concerning Elevated Risk in Complex Structured Finance Activities (PR-44-2006, May 9, 2006; FIL-45-2006, May 16, 2006; and *Federal Register* Vol. 71, No. 94, p. 28326, May 16, 2006)	The Federal bank and thrift regulatory agencies and the Securities and Exchange Commission requested public comment on a revised proposed statement on the complex structured finance activities of financial institutions. The revised statement describes the types of internal controls and risk management procedures that should help financial institutions identify, manage, and address the heightened legal and reputational risks that may arise from certain complex structured finance transactions. Comments were due June 16, 2006.
Comments Requested on Access to Banking Services by Money Services Businesses (FIL-37-2006, May 2, 2006; and *Federal Register* Vol. 71, No. 47, p. 12308, March 10, 2006)	The FDIC notified FDIC-supervised institutions that the Department of the Treasury's Financial Crimes Enforcement Network had issued a request for public comment on an Advance Notice of Proposed Rulemaking regarding the impact of Bank Secrecy Act regulations on the ability of money services businesses to open and maintain accounts and obtain other banking services at banks and other depository institutions. Comments were due July 9, 2006.

Subscription Form

To obtain a subscription to ***Supervisory Insights***, please print or type the following information:

Institution Name _____

Contact Person _____

Telephone _____

Street Address _____

City, State, Zip Code _____

Please fax or mail this order form to:

FDIC Public Information Center
3501 North Fairfax Drive, Room E-1022
Arlington, VA 22226
Fax Number (703) 562-2296

Subscription requests also may be placed by calling 1-877-ASK-FDIC or 1-877-275-3342.

Federal Deposit Insurance Corporation
Washington, DC 20429-9990

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

PRESORTED
STANDARD
MAIL
Postage &
Fees Paid
FDIC
Permit No. G-36