Office of Thrift Supervision **May 18, 2010**

Department of the Treasury

Regulatory Bulletin

RB 37-54

Handbook: **Examination**
Subject: **Management** **Section: 360**

Fraud and Insider Abuse

Summary: This Regulatory Bulletin transmits a revised Examination Handbook Section 360, Fraud and Insider Abuse.

For Further Information Contact: Your Office of Thrift Supervision (OTS) Regional Office or the Examination Programs Division of the OTS, Washington, DC. You may access this bulletin and the Examination Handbook at our web site: www.ots.treas.gov.

Regulatory Bulletin 37-54

SUMMARY OF CHANGES

OTS is issuing revised Examination Handbook Section 360, Fraud and Insider Abuse. We restructured the entire section so we did not include change bars in the margins. We provide a summary of all substantive changes below.

360 Fraud and Insider Abuse

We revised the narrative to expand and update discussions in many areas and add some new information:

- Added a discussion on SAR reporting requirements and the applicability of the "Safe Harbor" provisions for SAR filers.
- Added a discussion on the FDIC's white paper entitled, "Impact of New Activities and Structures on Bank Failures" and highlighted factors that contributed to the four costliest institution failures from 1997 through 2002.
- Provided updated statistics and red flags on mortgage fraud, identity theft, check fraud and payment card fraud.
- Added a discussion on fraud risk management and detection methods based on AICPA guidance.
- Streamlined the internal controls section.

—Tom Barnes
Deputy Director
Examination, Supervision, and Consumer Programs

Fraud and Insider Abuse

Difficult economic times often lead to an increase in fraud and insider abuse. During the market downturns of the late 1980s and early 1990s, fraud and insider abuse significantly contributed to thrift failures and caused substantial losses at many others. Since the recession began in 2007, there have been increases in white collar crime as well as changes in the way fraud scams are carried out. Although certain crimes such as, investment fraud and Ponzi schemes are not new, they are increasing as a result of market deterioration.

The difficult times of the past year have lead the federal government to commit considerable amounts of financial resources through the Troubled Asset Relief Program and other stimulus programs to spur the economy. Inevitably, the flow of massive amounts of federal assistance lends itself to various forms of fraud. In an effort to safeguard the use and expenditure of public dollars, Congress passed the Fraud Enforcement and Recovery Act of 2009 (FERA) on May 20, 2009. FERA's amendments to the civil False Claims Act broadens the risk of liability in a manner that warrants the attention of not just fraudsters, but to anyone doing business with the federal government.

LINKS

Program

Appendix A

Appendix B

The Department of Justice (DOJ) labels financial fraud "one of the most glaring threats" facing the US economy and has prioritized the fight against fraud to a level that merits the close attention of American corporate leaders. Following a wave of major corporate scandals, Congress established the President's Corporate Fraud Task Force to restore public and investor confidence in American businesses. In 2009, the President elevated the fight against mortgage fraud to a cabinet-level priority and expanded the taskforce to include OTS, OCC, the Federal Reserve, The Federal Housing Finance Agency, HUD, and the Special Inspector General for the Troubled Asset Relief Program. The President's task force joins the work that the Federal Trade Commission has already begun with their "Operation Stolen Hope" to crack down on mortgage foreclosure rescue and loan modification scams. The latest effort to expand the taskforce emphasizes the continued need to crack down on mortgage fraud, particularly with regard to ongoing investigations into securitization fraud. In addition to the President's taskforce, several other federal agencies work together to combat fraud and insider abuse at financial institutions.

The Securities and Exchange Commission (SEC) adopted rules to enhance shareholder disclosure and improve safeguards to protect the public after the Madoff Ponzi scheme and other fraudulent activities caused investors to question whether their assets are safe. The SEC amended its custody rules to increase the protections for investors who turn their money and securities over to investment advisers registered with the SEC. The amended rules provide safeguards where there is a heightened potential for fraud or theft of client assets. The SEC also approved new rules to enhance the information provided to shareholders so they are better able to evaluate the leadership of public companies.

The Interagency Bank Fraud Working Group is comprised of the five federal banking agencies, DOJ, the Federal Bureau of Investigation (FBI), and the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), among others. Representatives from these government agencies work together to establish policies to improve interagency cooperation and to resolve criminal investigation and prosecution problems.

Suspicious Activity Reporting Requirements

The five federal banking agencies and FinCEN issued parallel regulations that require their respective supervised institutions to file Suspicious Activity Reports (SARs) whenever they know or suspect suspicious or potential criminal activity. Various federal laws, including the Bank Secrecy Act, authorize the agencies' SAR rules. Pursuant to these rules financial institutions must file SARs with law enforcement and bank supervisory authorities (12 CFR § 563.180 and 31 CFR Part 103).

The SAR regulations require a filing after the discovery of a known or suspected federal criminal violation that involves any of the following persons or transactions:

- Any officer, director, employee, agent, or other institution-affiliated person.
- Transaction(s) aggregating $5,000 or more in funds or other assets when there is a factual basis for identifying a suspect.
- Transaction(s) aggregating $25,000 or more even though a suspect is unidentified.
- Transaction(s) aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.

Savings associations must file a SAR within 30 calendar days after the date of initial detection of the facts that may constitute a basis for filing a SAR. If the association cannot identify a suspect on the date of detection the savings association may delay filing a SAR for an additional 30 calendar days in order to identify the suspect. Reporting may not be delayed more than 60 calendar days after the date of initial detection of a suspicious transaction. The phrase initial detection should not be interpreted as meaning the moment a transaction is highlighted for review. The 30-day or 60-day period does not begin until an appropriate review is conducted and a determination is made that the transaction is suspicious within the meaning of the SAR regulation. Management must promptly notify its board of directors, or a committee thereof, of any SAR filed. For violations requiring immediate attention, such as when a reportable violation is ongoing, the savings association must immediately notify an appropriate law enforcement authority and OTS.

Applicability of Safe Harbor

Federal law protects financial institutions and their employees from civil liability for filing a SAR or for making disclosures in a SAR (31 USC § 5318(g) (3)). This protection, generally referred to as a "Safe Harbor" applies even if the report of suspicious activity is made orally or in some form other than through the use of a SAR. The SAR regulations require that savings associations make all supporting

documentation related to a filing available upon request to appropriate law enforcement agencies, federal banking agencies, and FinCEN. FinCEN inputs the information reported in SARs into a central database, which is accessible to federal and state financial institution regulators and law enforcement agencies. The information obtained from SARs plays an important role in identifying potential and actual illegal activities, such as money laundering, fraud and abuse. SAR information also assists in detecting and preventing the flow of illicit funds through our financial systems. Given more recent concerns like mortgage fraud, consumer loan fraud and identity theft, SARs data is more important than ever. Law enforcement agencies use the information reported on the SARs to initiate investigations and the agencies use the information in their examination and oversight of supervised institutions. The usefulness of the SAR database depends on the completeness and accuracy of the reported information. Accordingly, you should ensure that associations are accurately and fully completing SARs.

Examiner and Regional Reporting Requirements

Savings associations and their subsidiaries and service corporations have the primary responsibility to file SARs. However, the examiner must complete and file a SAR when the required filing institution has either failed to do so or failed to do so properly. When necessary, you should seek filing guidance from your supervisors or regional legal or enforcement personnel, including guidance concerning Right to Financial Privacy Act issues.

FRAUD, INSIDER ABUSE, AND CRIMINAL MISCONDUCT

Fraud is the intentional misrepresentation of a material fact(s), or a deception, to secure unfair or unlawful gain at the expense of another. Either insiders or outsiders, or both acting in concert, can perpetrate fraud on financial institutions.

> Many of the largest cases of financial institution fraud involved insiders.

Every year, thrifts lose a significant amount of money due to insider abuse and criminal misconduct. Many of the largest cases of financial institution fraud involved insiders. The FBI estimates that insiders of financial institutions steal eight times more money than is stolen through bank robberies and burglaries. If the insider is in a key position, the amount of loss can be significant enough to cause the institution to fail. The term insider abuse refers to a wide range of activities by officers, directors, employees, major shareholders, agents, and other controlling persons in financial institutions. The perpetrators intend to benefit themselves or their related interests. Their actions include, but are not limited to, the following:

- Unsound lending practices, such as inadequate collateral and poor loan documentation.
- Excessive concentrations of credit to certain industries or groups of borrowers.
- Unsound or excessive loans to insiders or their related interests or business associates.

- Violations of civil statutes or regulations, such as legal lending limits or loans to one borrower.

- Criminal violations of law and statute, such as fraud, misapplication of bank funds, or embezzlement.

In addition to criminal misconduct, insider abuse includes other actions or practices that may harm or weaken an institution, but that do not violate criminal statutes. While every criminal violation by an insider constitutes insider abuse, not all insider abuse constitutes criminal misconduct. In most problem financial institutions where regulators find insider abuse, they also find a variety of unsafe and unsound banking practices and mismanagement that may involve criminal acts. While a thin line often separates a criminal act from an unsafe or unsound act, OTS has the responsibility and the authority to act against all insider abuse, whether criminal or not.

The Federal Deposit Insurance Corporation (FDIC) wrote a white paper entitled, "Impact of New Activities and Structures on Bank Failures" dated September 30, 2003. The paper examines those business activities in the four costliest institution failures from 1997 through 2002. It is written from the FDIC's resolution perspective and identifies factors other than fraud that may have contributed to the high cost of these failures, including the impact of:

- Rapid growth in securitization of subprime loans and associated risks.

- Information technology fueling rapid growth in a national deposit market.

- Increased reliance on outsourcing, creating atypical organizational and operating structures.

Policy issues or lessons learned from these failures show that, at their core, many of the activities at these failed institutions were atypical and costly because they were fraudulent attempts to engage in business practices for profit.

In particular, the loss at one institution resulted in a 71.8 percent loss of total assets, the highest loss rate in the FDIC's history among institutions with reported assets of over $1 billion. The failure was primarily fraud-related and was exacerbated by accounting and audit failures. The complexity of the bank's operating structure may have been intentionally designed to make it more difficult for outsiders to understand its operations. Complex operating structures raise questions about whether such a structure is necessary for efficient business reasons or whether the contorted structure was developed, in part, to make it more difficult for regulators to understand the bank's business operations and indentify fraudulent activity. Insiders may intentionally design atypical operating structures to hide fraudulent or otherwise inappropriate activities.

Insiders often commit crimes using subordinates who do not question their instructions. In some instances, however, the subordinates may be astute enough to know that what the insiders instructed them to do is questionable or wrong and may freely discuss the situation if the regulators simply inquire.

According to FBI reports, fraud is becoming more expensive for financial institutions over time. An estimated 46 percent of all operational risk loss events are related to fraud and the average loss equals about $70 thousand per instance.

Mortgage Fraud

Of all frauds perpetrated against financial institutions, mortgage fraud in particular has spiked. While the total dollar loss attributed to mortgage fraud is unknown, at least 63 percent of all pending FBI mortgage fraud investigations during fiscal year 2008 involved dollar losses of more that $1 million each. During 2009, the FBI investigated more than 2,100 mortgage fraud cases, up 400 percent from five years ago. The increase in mortgage fraud can be attributed to the following:

- Declining economic conditions.
- Liberal underwriting.
- Declining housing values.

With the rapid growth of markets such as real estate and the development of new technology associated with refinancing and computer-driven underwriting methods, the opportunity for mortgage fraud continues to escalate. Warehouse lines have been particularly vulnerable, with their 90-day window of "purchasing" mortgages and awaiting ultimate repayments from final investors.

The FBI reports that equity stripping and property flipping are common activities. This problem is compounded in instances where an institution has ineffective policies and procedures that are poorly formulated or outdated. The FBI estimates that 80 percent of all mortgage fraud involves collaboration or collusion by industry insiders. Overall though, according to an FBI Financial Institution Fraud and Failure Report, external fraud schemes outnumber those involving insiders due to the following:

- Pervasiveness of check fraud and counterfeit negotiable instrument schemes.
- Technological advances.
- The availability of personal information through illicit information networks.

The FBI reports that mortgage fraud schemes continue to adapt as the economy changes and that individuals are victimized even as they are about to lose their homes. Foreclosure rescue scams take several forms but usually involve payment of an upfront fee in exchange for a promise to resolve a pending foreclosure. Ultimately, the scam results in unsuspecting victims losing their homes to foreclosure. While this type of fraud is not perpetrated directly against the savings association, the end result can have a negative impact on the association.

Identity Theft

Identity theft is the unauthorized transfer or use of another person's identification with the intent to profit illegally. The crime of identity theft varies widely, and can include check fraud, credit card fraud, and identity theft. According to FinCEN's 2008 Mortgage Loan Fraud report, cases of identity theft associated with mortgage fraud increased 95.62 percent over a previous study in 2006.

Criminals continue to attack financial institutions at the points of customer payments, from established mechanisms such as ATMs, cards and checks to newer Internet-based points of interaction. Fraudsters still use traditional fraud schemes, but they also are exploiting the latest technologies to further gain advantage. Schemes have become more complex in nature to avoid the radar of risk management systems. Even more disconcerting are trends toward assaults at the core customer accounts. Police say identity theft is increasingly difficult to track because criminals move quickly from one jurisdiction to the next. Fraudsters act so quickly after they steal that they are counting their money before the victims know that they have been compromised. Identity theft and phishing are major industry concerns and threaten to erode consumer confidence.

Identity theft and phishing are major industry concerns and threaten to erode consumer confidence.

The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. While consumers suffer the frustration of restoring their credit and identity, financial institutions will incur some if not all of the financial losses experienced by their customers. If the institution is at fault, they will more than likely lose the customer's business as well. In some extreme cases, other penalties may be assessed to the institution if they were blatant or careless with the customer's nonpublic information or failed to file a SAR in the event of a questionable transaction. The Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act of 2003 require that financial institutions implement policies and procedures to detect, prevent, and mitigate identification theft. Financial institutions must remain vigilant in ensuring the safety of their customer's personal information because as technology grows in sophistication, so will fraud schemes.

Check Fraud

Check fraud is one of the biggest challenges facing financial institutions. As it becomes more difficult to get new lines of credit, identity thieves are more likely to commit check fraud. According to FinCEN, SARs filings associated with check fraud grew from 12 percent in 2007 to 17 percent of all fraud filings in 2008. According to the America Bankers Association Deposit Account Fraud Survey Report, actual dollars lost to check fraud was amounted to an estimated 1.024 billion in 2008, up slightly from the $969 million in 2006.

According to the U.S. Department of Treasury, an estimated 1.2 million fraudulent checks are written each year in the United States. With effective kiting methods, losses can grow quickly. Advances in desktop publishing software and the quality of home office copy machines, scanners, and printers make it more difficult to identify counterfeit checks. Also, with the growth in electronic check processing, it

will not take long for criminals to adapt fraud schemes to take advantage of image replacement documents and the lack of a physical check.

Savings associations should take the following preventive measures to reduce check fraud:

- Establish and maintain strong organizational controls.
- Ensure that effective internal controls are actively in place to prevent check fraud by insiders.
- Provide effective check fraud prevention programs through education and training for front-line personnel, managers, and operations personnel.
- Furnish a special section in teller manuals about check fraud that includes a detailed list of common warning signs.
- Establish guidelines for check cashing.
- Provide specialized training for new account representatives and establish guidelines for opening new accounts.

Credit/Debit Card Fraud

Payment card fraud is also evolving and becoming more dangerous to consumer accounts. According to the ABA Deposit Account Fraud Survey, industry losses from debit card fraud alone reached an estimated $788 million in 2008. Even more threatening, however, are its ties to organized crime and terrorist funding.

Skimming methods are becoming significantly more sophisticated as technology improves. For example, organized criminals access resources that create ATM "overlays" that imitate actual ATM devices. The overlay devices include:

- Card skimmers to capture card data.
- PIN pads to capture PIN numbers.
- Transmitters to immediately send the information to personal computers inside vehicles in the vicinity.

The fraudster's computer receives the information and downloads it to a portable card encoder. The computer generates a white plastic card containing the skimmed data and criminals engage in fraudulent activities almost immediately. Overlays are generally left on a particular ATM for several hours then moved to another location making it difficult to determine the actual point of compromise. ATM skimming is on the rise in every major financial market.

MANAGING THE RISK OF FRAUD

The board's oversight role in managing fraud risk is critically important because historically most major frauds are perpetrated by senior management in collusion with other employees. While the format of a fraud risk management program may vary, good governance is the key to the program's success. The American Institute of Certified Public Accountants (AICPA) issued guidance, "Managing the Business Risk of Fraud: A Practical Guide" that provides five key principles for proactively managing fraud risk:

Principle 1: As part of an organization's governance structure, a fraud risk management program should be in place, including written policies to convey the expectations of the board and senior management regarding managing fraud risk.

Principle 2: The organization should periodically assess the fraud risk exposure to identify specific potential schemes and events that the organization needs to mitigate.

Principle 3: Establish prevention techniques to avoid potential key fraud risk events, where feasible, to mitigate possible impacts on the organization.

Principle 4: Establish detection techniques to uncover fraud events when preventive measures fail or unmitigated risks are realized.

Principle 5: Develop a reporting process to solicit input on potential fraud and use a coordinated approach to investigation and corrective action to help ensure potential fraud is addressed appropriately and timely.

Importance of Internal Controls

Savings associations facing increased competition often consider implementing new strategies including cutting costs, offering different products, and pursuing other activities that have higher yields. While OTS recognizes that savings associations must adapt to changing business conditions, it is critically important that management maintain strong internal controls to address the business risks of fraud. Lack of proper supervision and lack of effective internal controls can make an association especially vulnerable to fraud and insider abuse. See Examination Handbook 760, New Activities.

> The primary responsibility to prevent fraud and insider abuse rests with the board of directors and senior management.

The primary responsibility to prevent fraud and insider abuse rests with the board of directors and senior management. To properly execute their fiduciary duties, management must implement internal controls and other safeguards to prevent fraud and theft whether internally or externally perpetrated. However, sometimes even the best safeguards can be circumvented. Therefore, management must continuously assess and monitor systems to detect suspicious activity. Once detected, management must report suspicious activities to the board of directors.

An association's internal systems for capturing suspicious activities should provide essential information about the nature and volume of activities passing through customer accounts. Staff should pursue any information suggesting that suspicious activity has occurred and, if an explanation is not forthcoming, report the matter to management. The examiner should ensure that the association's approach to SARs is proactive and that well-established procedures cover the SAR process. Accountability should exist within the organization for the analysis and follow-up of internally identified suspicious activity. See the FFIEC BSA/AML Examination Manual for the core procedures concerning SAR requirements.

The following are some examples of unsafe, unsound, and sometimes fraudulent activities that have caused savings associations to suffer significant financial losses due to breakdowns in internal controls:

- Unauthorized and unsupervised overdrafts of customers' checking accounts.
- Unauthorized loans and falsified loan records.
- Employee embezzlements involving check-kiting schemes.
- Unauthorized withdrawals from a correspondent account.
- Unreported teller shortages.

Inadequate internal controls also contribute to losses associated with a shift from traditional activities to higher risk commercial and consumer lending. Because of increased competition and decreased margins, many associations have cut costs in such areas as BSA/AML compliance and SAR policy and procedure oversight. Associations must direct expense control to areas that do not compromise critical policies and procedures governing internal controls.

See Handbook Section 340, Internal Controls, for more detailed information.

Detecting Fraud and Insider Abuse

When you know the warning signs and are alert to circumstances where fraud may exist, you are better equipped to detect it. Although the majority of bank fraud involves insiders, you should also be alert to attempts by outsiders to defraud the association.

Once you suspect fraud you should thoroughly investigate the circumstances surrounding a suspected fraudulent activity. If a situation exists where an officer or employee is able to control a sizable transaction from beginning to completion, you should notify the board of directors. The board should immediately correct the situation. You should not think of internal control weaknesses, poor loan documentation, or improper internal audit reporting relationships only as technical violations, but also as potential opportunities for large frauds. Such weaknesses should receive appropriate treatment in the report of examination and should result in effective supervisory action.

It is not possible to eliminate the risk of fraud entirely. There are always people who are motivated to commit fraud and there will always be opportunities to override a control or collude with others in doing so. Therefore it is important that fraud detection programs be periodically monitored and made flexible enough to meet the various changes in risk. The AICPA's "Guide to Managing the Business Risk of Fraud" recommends several important detection methods:

- Anonymous reporting mechanism, such as whistleblower hotlines.
- Process controls specifically designed to detect fraudulent activity, as well as errors, include reconciliations, independent reviews, physical inspections/counts, analyses or audits.
- Proactive fraud detection such as data analysis, continuous auditing techniques, and technology tools such as data mining and digital analysis.

If you become aware of fraud, alert your field manager so you can devote the time necessary to determine the appropriate action. To assist you in assessing an institution's risk of fraud, this section attaches a Fraud Risk Evaluation Form (Appendix A) and includes the following subsection: Red Flags of Fraud and Insider Abuse. If you consider the risk of fraud to be high you should expand your examination scope in the appropriate areas.

Red Flags of Fraud and Insider Abuse

Experience has taught OTS staff that certain common elements are often present in cases of fraud and insider abuse. The following listings are warning signs of possible fraud and insider abuse.

General

- Dominant officer with control over the institution or a critical operational area.
- Internal audit restrictions or unusual reporting relationships (the internal auditor not reporting directly to the board or audit committee).
- Lack of written or inadequately written policies.
- Lack of adherence to written policies.
- Unusual or lavish fixed assets (for example, aircraft or art work).
- Management attempts to unduly influence examination or audit findings.
- Material internal control deficiencies.
- Frequent changes of auditors.

- High turnover in the internal audit department.
- Delay tactics, alteration or withholding of records.
- Large transactions with small out-of-town banks.
- Ownership or control vested in a small group.
- Difficulty in determining who is in control.
- Overly complex organizational structure, managerial lines of authority, or contractual arrangements without apparent business purpose.
- Inaccurate, inadequate, or incomplete board reports.
- Discontinuation of key internal reports.
- No vacation taken by employee or officer.

Management Level

- Routinely contests exam findings by filing appeals, complaining to congresspersons, or directly or indirectly contacting agency officials.
- Routinely accuses you of being unfair, acting overzealously, or making errors.
- Fails to provide original documents – only provides copies.
- Hires ex-agency officials when faced with enforcement actions.
- High turnover or loss of substantial number of officers and directors.
- Motivation to engage in fraudulent financial reporting – significant portion of management's compensation is contingent upon aggressive targeted financial achievements, stock prices, or earnings.
- Use of aggressive accounting practices or tax-motivated behavior.
- High degree of competition in the community accompanied by declining margins of profit or customer demand.
- Management lacks expertise needed to fully understand ramifications of proposals made by third parties or they perceive unrealistic opportunity to enhance income.

Exam Level

- Inability to generate cash flows from operations.
- Assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgments or uncertainties.
- Unusually rapid growth in comparison to other institutions.
- High vulnerability to interest rate changes.
- Inadequate monitoring of significant controls.
- Lack of timely or appropriate documentation for transactions.
- Significant unexplained items on reconciliations.
- Falsified bank documents.
- Weak loan administration and out of balance loan accounts.
- Repeated regulatory violations including significant Thrift Financial Report violations.
- Significant related party transactions not in the ordinary course of business.
- Significant numbers of bank accounts located in tax haven jurisdictions.
- Weak internal controls and risk management such as:
  - — Inadequate overall internal control design.
  - — Inadequate procedures to assess and apply accounting principles.
  - — Absence of controls for certain transactions.
  - — Evidence that a system fails to provide accurate output, or evidence of design flaws, among others.
- Known SARs.

Lending Abuse Red Flags

- Poorly documented loans and appraisals.

- Lack of an acceptable past due or watch list.
- Lack of, or unsigned, borrower financial statements.
- Questionable loan disbursements.
- Loan funds disbursed to a third party.
- Corporate loans with no endorsements or guarantors.
- Large pay-down of problem loans prior to an audit or examination.
- Large overdrafts.
- Refinancing of debt in a different department.
- Loans secured by flipped collateral.
- Nominee loans.
- Loans of unusual size or with unusual interest rates or terms.
- Loans with unusual, questionable, or no collateral.
- Loan review restrictions.
- Questionable, out-of-territory loans.
- Evergreen loans (loans continuously extended or modified).
- A considerable amount of insider loans.
- Construction draws with nonexistent or inadequate inspection reports.
- Construction inspections conducted by unauthorized or inappropriate persons.
- Market study on proposed project not on file.
- Loan approvals granted to uncreditworthy employees.
- Lack of independence between the approval and disbursement functions.
- Frequent sales of collateral (land flips) indicating related party transactions.

- Predatory lending practices.

Appraisal Abuse Red Flags

- No appraisal or property evaluation in file.
- Mortgage broker or borrowers that always use the same appraiser.
- Appraiser bills association for more than one appraisal when there is only one in the file.
- Unusual appraisal fees (high or low).
- No history of property or prior sales records.
- Market data located away from subject property.
- Unsupported or unrealistic assumptions relating to capitalization rates, zoning change, utility availability, absorption, or rent level.
- Valued for highest and best use, which is different from current use.
- Appraisal method using retail value of one unit in condo complex multiplied by the number of units equals collateral value.
- Use of superlatives in appraisals.
- Appraisal made for borrower.
- Appraisals performed or dated after loan.
- Close relationship between builder, broker, appraiser, lender and/or borrower.
- Overvalued (inflated) or high property value.

Mortgage Fraud Red Flags

Straw Borrower Schemes

- Borrowers purchasing property described as a primary residence, but outside of their home states, or located an unreasonable commuting distance from their stated employers.
- A quit claim deed is used either right before, or soon after, loan closing.
- Investment property is represented as owner-occupied.

- Someone signed on the borrower's behalf.
- Names were added to the purchase contract.
- Sales involve a relative or related party.
- No sales agent involved.
- Indication of default by the property seller.
- High FICO score.
- Power of attorney for borrowers.
- Good assets, but gift used as down payment.
- Repository alerts on credit report.

Builder Bailout Schemes

- The builder is willing to "do anything" to sell property.
- The borrower is barely qualified or unqualified.
- The sales price and appraisal are inflated.
- No-money-down sales are included.
- "Silent" second mortgages are involved.
- The sales price is adjusted upwards.
- The source of funds is questionable.
- There is a reference to secondary financing on HUD-1 or purchase contract.
- Parties to the transaction are affiliated.
- Multiple sales to the same person.

Flipping Schemes

- Fraudulent appraisal.

- Inflated buyer income.
- Ownership changes two or more times in a brief period of time.
- Two or more closings occur almost simultaneously.
- The property has been owned for a short time by the seller.
- The property seller is not on the title.
- There is a reference to double escrow or other HUD-1 form.

Check Fraud Red Flags

Check fraud is one of the biggest challenges facing financial institutions.

- Check lacks perforations.
- The check number is either missing or does not change.
- The check number is low (such as, 101 up to 400) on personal checks or (such as, 1001 up to 1500) on business checks. (90 percent of bad checks are written on accounts less than one year old.)
- The type of font used to print the customer's name looks visibly different from the font used to print the address.
- Additions to the check have been written in by hand.
- The bank or customer's address is missing.
- The Magnetic Ink Character Recognition coding at bottom of the check looks altered, is missing numbers, or does not match the bank district and routing symbol.
- Payee name appears to have been typed in.
- The word VOID appears across the check.
- Notations appear in the memo section listing "load," "payroll," or "dividends" (legitimate companies have separate accounts for these functions).

Access to Savings Association Directors, Employees, Agents, and Books and Records

During formal and informal discussions with employees, you should listen carefully and be attuned to signals of possible illegal activity by others within the institution. Discovering fraud is often a matter of

talking with the right person who knows what is occurring. Inside abusers often start with small transactions and engage in increasingly larger transactions as their confidence level rises. Hence, early detection of insider abuse is an essential element in limiting risks to the insurance fund.

Generally, you should bring up fraud as part of another discussion. Once you have established some rapport, you should first ask, as appropriate to the person you are interviewing, general questions and then more specific questions:

- What kind of history does the association have with fraud in general, including defalcations and employee thefts?
- What specific areas should we focus on during the examination to ensure that there are no major fraud problems?
- Has anyone ever asked you to do something that you thought was illegal or unethical?
- If someone wanted to commit fraud against the association, what would be the easiest way to do it?
- Is the association in any kind of financial trouble that would motivate someone to commit fraud?
- Is anyone in any personal financial difficulty that you are aware of?
- Have you ever committed fraud against the company?

A number of federal statutes entitle you to prompt and unrestricted access to savings association directors, employees, agents, books, and records. In some instances, association management may attempt to delay or limit your access to information with the intent to conceal fraud, derogatory information, or insider abuse. Such obstruction, however, more often occurs due to a lack of understanding by association personnel. In either case, you can usually promptly resolve access problems by reviewing the appropriate statutory requirements with association management. You must recognize obstruction, consider it a red flag indicating potentially serious problems, and take steps to prevent it.

> You must recognize obstruction and consider it a red flag indicating potentially serious problems.

Tools to Prevent Examination Obstruction

The following statutes and regulations grant you prompt and complete access to savings association directors, employees, agents, and books and records:

- 12 USC § 1464(d)(1)(B)(ii) requires associations to give you prompt and complete access to its officers, directors, employees, and agents, and to all relevant books, records, or documents of any type during an examination.

- 12 USC § 1464(d)(1)(B)(iii) requires associations to give you prompt and full access to all records and staff for regulatory purposes at all other times.

- 12 USC § 1467a (b) (4) provides you with authority to examine savings and loan holding companies.

- 12 USC § 1467a(b)(3), 12 CFR § 563.170(c) requires institutions and their holding companies to maintain complete records of their business and make them available to you wherever they are located.

- 12 USC §§ 1464(d) (7) (D) (i) and 1831v, and 12 CFR § 563.170(e) provides you with access to the records and staff of service providers unless the service provider is functionally regulated.

- 12 USC §§ 1464(d)(1)(B)(i), 1467a(b)(4) and 1831v allows you unrestricted access to records of affiliates (including holding company subsidiaries) whose affairs affect insured institutions, unless the affiliate is functionally regulated.

When appropriate, you should remind associations that OTS may use its enforcement tools to obtain management's compliance with these access provisions. These tools include cease and desist orders, removal and prohibition orders, and civil money penalties. In addition, examination obstruction may subject management to criminal prosecution under 18 USC § 1517.

Examination Obstruction

Recognizing and refusing to tolerate obstruction is critical to preparing an accurate report of examination. It is important that you promptly notify your Examiner-in-Charge (EIC) or field manager of an association's attempt to obstruct your examination. If you try to ignore it, the evasion generally gets worse, as do the problems concealed by the obstruction.

Appendix B of this handbook section consists of a number of examination obstruction questions and answers.

Examples of Obstruction

- Delaying Tactics. Savings associations sometimes do not provide requested information within a reasonable time. For example, the association may tell you that:

  — The only staff member who knows the location of the records is unavailable right now – and continues to be unavailable.

  — An association employee urgently needs a particular computer with the necessary records for other purposes.

  — The records are off site and there will be a delay in obtaining them.

Your response should be polite but firm: under federal statutes, unreasonable delays are impermissible (12 USC § 1464(d) (1) (B) (ii)).

- Screening Tactics. Associations may try to prescreen the documents you need to review requiring that you request documents or staff in advance. The association's intent may be to review or sanitize requested documents before you see them. Screening is impermissible (12 USC § 1464(d) (1) (B) (ii) and 12 CFR § 563.170(c)).

- Alteration of Records. Association employees may attempt to alter records before your review to prevent you from discovering significant losses, fraud, or insider abuse. The employees may remove key documents from files, destroy records, or create required records (known as file stuffing). Association employees who use these illegal tactics can subject themselves to criminal prosecution. If you suspect altered records, notify your EIC, field manager, or regional counsel (18 USC §§ 1005 -1006).

- Nonresponsive Answers. Incomplete information or different information than requested.

- Removal of Records. In several cases, management removed important documents from association offices and hid them off site from examiners. You can only discover this conduct when you remain alert to the fact that obstruction may be occurring, and persistently follow up on employee comments and cross references to missing documents in other files. Removal of records violates several of the civil and criminal statutes cited above. If you suspect that this has occurred, you should notify your EIC, field manager, or regional counsel of your concerns.

- Withholding Information Based on Assertions of Privilege. Associations, their attorneys, or their accountants may attempt to prevent you from accessing documents based on assertions of privilege or confidentiality. Because rulings on privilege claims can turn on specific facts, you should consult with your regional counsel whenever an association raises privilege claims. Generally, associations cannot properly use these assertions to bar you from attending executive board of director sessions or reviewing minutes of its meetings, including draft minutes. These assertions also may not prevent you from reviewing records of the association's operations, such as documents relating to loans that may be the subject of ongoing litigation between the association and third parties. Even if such documents are in the offices of the association's attorney, you are entitled to review them wherever they are (12 USC § 1464(d) (1) (B) (ii) and 12 CFR § 563.170(c)).

- Attacks on Your Credibility. Associations sometimes attempt to neutralize negative examination findings by attacking the credibility of individual examiners. Your best defense is prevention. Use good judgment, comply with OTS policy, and make it a practice to have another examiner present during important or potentially hostile meetings with association employees.

Stopping Examination Obstruction

You must promptly stop examination obstruction. We have found repeatedly that obstruction is a red flag for a variety of more serious problems. You cannot always identify and address the problems, however, until the association stops the obstruction.

When you encounter any of the obstruction tactics noted above, you should immediately discuss the problem with senior management and seek a quick resolution of what could be a simple misunderstanding. You should explain to senior management the statutory basis for gaining access to all records. If are still unable to obtain access and the association does not resolve the situation, you should inform your EIC or field manager. They will work with you, the Assistant Regional Director (ARD), and the regional counsel to address the problem. Any continued obstruction will involve other attorneys of the Chief Counsel's office as appropriate.

The following are several tools available for a prompt and complete remedy. The right response depends on the type and seriousness of the obstruction and the Chief Counsel's advice as to how to proceed.

- Reviewing with the association's board of directors the applicable statutes that compel prompt and complete access of records and politely insisting on compliance. This course might involve arranging a meeting of the board with the field manager, ARD, Regional Director, and/or regional counsel.

- Delivering a supervisory letter instructing the association to promptly comply with examiner requests for information or face formal enforcement action.

- Petitioning the local United States District Court for an Order requiring the association provide the requested information immediately (12 USC § 1464(d)(1)(B)(iv)).

- Issuing a temporary cease and desist order requiring that inaccurate or incomplete records be restored immediately to a complete and accurate state (12 USC § 1818(c)(3)(A)).

- In extreme cases, or where OTS has exhausted all other remedies, appointing a conservator or receiver based on the association's concealment of records and obstruction of the examination (12 USC § 1821(c)(5)(E)).

- Where appropriate, or in conjunction with the remedies listed above, filing a SAR. Such filings may be for obstructing an examination, making false entries to defraud the association or deceive regulators, or concealing assets from an association's conservator, receiver, or liquidating agent. These illegal actions are subject to 18 USC §§ 1005, 1006, 1517, and 1032.

Criminal Statutes

The federal criminal statutes that you might encounter are generally found in Title 18 of the United States Code. The following list is not exhaustive, but it provides a brief description of some criminal statutes applicable to financial fraud.

18 USC § 215

Kickbacks and bribes. Section 215 makes it unlawful for any officer, director, employee, agent, or attorney to solicit, accept, or give anything of value with intent to corrupt, in connection with any transaction or business of any financial institution.

Significant Aspects:

- Intent to corrupt requires intent to receive a personal financial benefit or to direct to another person such benefit.
- Applies to noncustomer transactions, for instance, suppliers.
- Applies where a person makes a payment after the fact to reward another person for a prior act.
- Can apply where a third party receives the benefit if the intent is to influence the insider.

18 USC § 657

Theft, embezzlement, or willful misapplication of an insured institution's funds by an officer, director, agent, or employee with intent to defraud the institution.

Significant Aspects:

- Applies to check kites, nominee borrowers, and in some cases unauthorized loans.
- Violation of internal policies, violation of regulations, and personal benefit to the insider.

18 USC § 709

- This criminal statute prohibits false advertising or misuse of a federal agency name.

Significant Aspects:

- Prohibition, except where permitted by law, of the use of several words relating to federal entities without authority.
- Prohibitions include the use, except where permitted by the laws of the United States, of the words national, federal, United States, reserve, or deposit insurance as part of the business or firm name of a person, corporation, partnership, business trust, association, or other business

entity engaged in the banking, loan, building and loan, brokerage, factorage, insurance, indemnity, savings or trust business.

- Prohibitions also apply to many other words, acronyms, advertisements or representations.

18 USC § 1001

Knowingly or willfully falsifying or concealing a material fact or making a false statement or making or using false writing knowing it to be false.

18 USC § 1006

False entries and reports or statements. Includes material omissions, with intent to injure or defraud an insured institution or deceive an OTS regulator. The statute also covers an officer's, agent's, or employee's receipt of any benefits from an institution transaction with intent to defraud.

Significant Aspects:

- Misstatement should be material.

- Often used in conjunction with misapplication statutes such as 18 USC § 657.

18 USC § 1014

False statement, oral or written (for instance, loan applications), made knowingly for the purpose of influencing OTS or any federally insured institution. False statements apply to any application, purchase agreement, commitment, or loan (or any change or extension of same). For example, willfully overvaluing land, property, securities, or other assets; or understating liabilities.

Significant Aspects:

- Usually used against borrowers for submitting false financial statements.

- Statute applies to all persons, not just insiders.

18 USC § 1344

Bank fraud. A scheme or artifice to defraud a federally insured institution or take money, funds, credit, assets, security, or other property by misrepresentation.

Significant Aspects:

- Applies to most activities that are violations under the statutes.

- Generally must find deceit, trickery, deception, falsehood, or failure to provide information when there is an obligation to do so.

18 USC § 1517

Obstructing an examination. It is a crime to corruptly obstruct or attempt to obstruct an examination of a financial institution.

Significant Aspects:

- The examination must be one that an agency of the United States, with examination jurisdiction, is conducting.
- Applies to whoever corruptly obstructs or attempts to obstruct.

CONFLICTS OF INTEREST

There remains a continuing need for regulatory personnel to scrutinize all conflict of interest transactions in the context of OTS's Conflicts of Interest regulation 12 CFR § 563.200. You should, accordingly, comment on and request appropriate corrective action on any actual or apparent conflict of interest situation that adversely affects the association, even though a regulation may not specifically address the conflict. You should also comment on and request appropriate corrective action whenever people involved in a conflict situation participate in or exercise an undue influence over the approval of the transactions. For additional guidance, see Examination Handbook Section, 380, Transactions with Affiliates and Insiders.

REFERENCES

Statutes

The Fraud Enforcement and Recovery Act of 2009 (FERA), Pub. L. 111-21, 123 Stat. 1617, S. 386.

United States Code (12 USC)

§ 1464	Homeowner's Loan Act
§ 1467	Examination of Savings and Loans
§ 1818(c)	Temporary Cease and Desist Orders
§ 1821(c)	Appointment of Corporation as Conservator or Receiver
§ 1828(k)	Authority to Regulate or Prohibit Certain Forms of Benefits to Institution-Affiliated Parties
§ 1831v	Authority of State Insurance Regulator

§ 3401	Right to Financial Privacy Act of 1978

United States Code (18 USC)

§ 211	Bribery, Graft, and Conflicts of Interest
§ 215	Kickbacks and Bribes
§ 657	Lending, Credit and Insurance Institutions
§ 709	False Advertising or Misuse of Names to Indicate Federal Agency
§ 1001	General False Statements
§ 1006	False Entries or Reports
§ 1014	False Statements
§ 1032	Concealment of Assets from Conservator, Receiver, or Liquidating Agent of Financial Institution
§ 1344	Bank Fraud
§ 1517	Obstructing Examination of Financial Institution

United States Code (31 USC)

§ 5318(g)(3)	Bank Secrecy Act, Confidentiality of SARs

Code of Federal Regulations (CFR)

12 CFR

Part 215	Regulation O, Loans to Executive Officers, Directors and Principal Shareholders of Member Banks
§ 510.5	Release of Unpublished OTS Information
§ 560.130	Prohibition on Loan Procurement Fees
§ 561.14	Controlling Person
§ 561.18	Director
§ 561.24	Immediate Family

§ 561.35	Officer
§ 563.33	Directors, Officers, and Employees
§ 563.41	Loans and other Transactions with Affiliates and Subsidiaries
§ 563.43	Loans by Savings Associations to Their Executive Officers, Directors and Principal Shareholders
§ 563.170	Examinations and Audits; Appraisals; Establishment and Maintenance of Records
§ 563.177	Procedures for Monitoring Bank Secrecy Act (BSA) Compliance
§ 563.180	Suspicious Activity Reports and other Reports and Statements
§ 563.200	Conflicts of Interest
§ 571.90	Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft

31 CFR

Part 103	The Bank Secrecy Act
§§ 103.100 and .110	USA PATRIOT Act – Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity
§ 103.121	USA PATRIOT Act – Customer Identification Program (CIP)
§§ 103.177 and .185	USA PATRIOT Act – Correspondent Accounts for Foreign Shell Banks; Recordkeeping and Termination of Correspondent Accounts for Foreign Banks

Office of Thrift Supervision Bulletins

RB 20a	Investigation of Applicants Proposing to Directly or Indirectly Acquire Control of, or to Exercise Control or a Controlling Influence Over OTS Regulated Savings Institutions and Savings and Loan Holding Companies

Interagency Guidance and Forms

Check Fraud: A Guide to Avoiding Losses (February 1999)

The SAR Activity Review – By the Numbers

Interagency Advisory dated May 24, 2004, Federal Court Reaffirms Protections for Financial Institutions Filing Suspicious Activity Reports

Federal Financial Institutions Examination Council (FFIEC) BSA/Anti-money Laundering Examination Manual dated August 24, 2007

FFIEC, the Detection and Deterrence of Mortgage Fraud against Financial Institutions (2009 White Paper)

FFIEC Information Technology Examination Handbook

FinCEN's 2008 Mortgage Loan Fraud Report

American Institute of Certified Public Accountants

Statement on Auditing Standards, No. 82, Consideration of Fraud in a Financial Statement Audit (February 1997) (AU 316)

The Auditor's Responsibility to Consider Fraud and Error in an Audit of Financial Statements – International Standards on Auditing (ISA No. 8240, Appendix 3)

Forensic Accounting: Fraudulent Reporting and Concealed Assets (Investigating Misappropriation of Assets and Fraudulent Financial Reporting)

Managing the Business Risk of Fraud: A Practical Guide

OTHER RESOURCES

American Bankers' Association Deposit Account Fraud Survey Report, November 2009

Fraud and Insider Abuse Program

Examination Objectives

To determine if the savings association has a fraud risk management program to manage fraud risk.

To recognize warning signs of fraud and insider abuse and to take appropriate measures to follow-up on possible instances of such activity.

To determine if the association's internal control system is applicable to officers and directors as well as other employees.

To determine the association's risk exposure associated with each significant instance of fraud or abuse.

To identify weaknesses in the association's internal controls through detection and analysis of any patterns of fraud or abuse.

To properly report suspected criminal misconduct uncovered during the examination to appropriate law enforcement authorities.

To determine if the association is reporting suspected criminal acts as § 563.180(d) requires.

To determine if the institution is properly completing Suspicious Activity Reports (SARs).

To determine if the association has an adequate program of follow-up with law enforcement authorities regarding SARs it has filed.

Examination Procedures

Level I

WKP. REF.

1. Review the associations fraud risk management program. Determine whether it includes written policies that convey expectations for the board and senior management regarding managing fraud risk.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

2. Review the adequacy of the association's policies and procedures with respect to conflicts of interest. Determine whether the association requires directors, officers, and employees to sign a Code of Ethics statement.

3. Discuss the issue of fraud and insider abuse with the internal auditors and, if necessary, the external auditors to assess whether they have any concerns. Determine if they have made any reports on suspected fraud to the board or others.

4. Review the previous three or four reports of examination and all related exceptions noted and determine whether management has taken appropriate corrective action.

5. Review the results of the questionnaires to determine if adequate controls are in place to mitigate fraud. Assess the adequacy of controls that would prevent officers and directors from perpetrating fraud.

6. Review the results of the various examination programs to determine if problems exist that may be symptomatic of fraud. In cases where fraud may be likely, investigate such problems to determine the cause of the problem (for example, poor staff training, errors, poor judgment).

7. Review the association's policies and procedures on reporting suspected criminal activity to law enforcement agencies and its board of directors for compliance with § 563.180(d).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

8. Review the association's Identity Theft Program in compliance with 12 CFR Part § 571.90.

9. Review the association's SARs, including those that OTS has filed, to determine if any patterns of criminality exist:

   - Identify multiple SARs on individual suspects, location of violation (for example, loan center, savings branch), or type of violation.
   - Analyze any apparent pattern of fraud or abuse to determine if enhanced internal controls would deter any future abuse.

10. Review all significant SARs, other reports, and patterns to determine if the association has properly identified and addressed all related financial, operational, and legal risks; for example, valuation allowances established, internal controls strengthened, etc.

11. Assess the association's risk of fraud by reviewing the red flag warning signals and conditions in the association. You should do this in conjunction with performing other examination programs and procedures, completing the Fraud Risk Evaluation Form (Appendix A) and, if necessary, by other appropriate means. You should notify your supervisor when you have rated any individual fraud risk score 4 or 5, and you believe that there is significant potential for insider abuse or fraud.

12. Consult with the Examiner-in-Charge (EIC), field manager and other examiners concerning the need to expand examination scope within certain areas based on an indication of a higher than acceptable risk of fraud within certain areas of the association.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

13. Notify the regional legal staff if any person attempts to obstruct the examination, in possible violation of criminal statute 18 USC 1517.

14. Obtain a list of deposit and loan accounts of directors, officers, and other affiliated persons. Test check these accounts for preferential rates and, for deposit accounts, appropriate board approval of any overdrafts.

15. Review Level II procedures and perform those necessary to test, support, and present conclusions derived from performance of Level I procedures.

LEVEL II

16. Choose a sample of SARs that the association has filed. Review each sample SAR to determine its accuracy, completeness, timeliness, and propriety.

17. Complete the following procedures if you identify any instance of suspected criminal misconduct:

- Immediately notify the EIC and field manager.
- Consult with appropriate regional office staff or counsel to determine a course of action, including preparation of a SAR.
- Obtain input from regional office legal staff on Right to Financial Privacy Act issues during the preparation of every SAR.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

18. The following elements are particularly important in preparing a successful SAR:

- A chronology of events.
- A summary of suspected violations.
- A list of key participants or affiliates.
- A list of potential helpful witnesses.
- Any supporting documentation.

19. Review the association's independent audit reports to determine if specific procedures exist to detect fraud, as the American Institute of Certified Public Accountants (AICPA) rules require.

20. Review the association's program of follow-up with law enforcement authorities to determine if timely and adequate follow-up is being conducted on significant SARs.

21. For associations with composite ratings of 4 or 5, determine if, in possible violation of 12 USC § 1828(k), the association has done either of the following:

- Made, or has entered into an agreement to make, any golden parachute or indemnification payments.
- Prepaid any salary, or any liability or legal expense, in anticipation of insolvency and with a view towards preventing the proper use or purpose of assets.
- Notify the regional legal staff if the association has done either one.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

22. Ensure that your review meets the Objectives of this Handbook Section. State your findings and conclusions, and appropriate recommendations for any necessary corrective measures, on the appropriate work papers and report pages.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

Fraud Risk Evaluation Form

Institution

Docket No.

Prepared by

Date

Reviewed by

Date

Instructions

This form documents your overall assessment of the level of fraud risk within the institution. Rate each risk factor from 1 to 5 with 1 indicating the lowest level of concern and 5 indicating the highest level of concern.

An individual factor rated 4 or 5 indicates that the institution is vulnerable to fraud. If fraud conditions or circumstances other than the factors listed below indicate a higher risk than normal, describe them on a separate sheet and attach it to this form. After you consider all relevant factors you should make an overall assessment of fraud risk and indicate its effect, if any, on the scope of the examination.

General Factors	Indicator		Comment or Description[1]	Risk Factor
	Lower	Higher		
Top management operating style	Effective board oversight	Domination of decisions by a single person		
Financial reporting	Conservative; accurate	Liberal; questionable; inaccurate		
Management turnover, including senior accounting personnel	Nominal	High		
Emphasis on meeting earnings projections	Little	Very high		
Profitability relative to industry	Adequate and consistent	Inadequate or inconsistent		
Growth within last three years	Stable	Rapid		
Financial condition	Healthy	Distressed		
Oversight of branches and subsidiaries	Centralized; strong oversight	Decentralized; weak oversight		
Indicators of going-concern problems	No serious indications of failure	Failure a distinct possibility		
Disagreements with auditors or examiners	None	Many		
Difficult-to-audit transactions or balances	Few	Many		
Misstatements detected in prior audits or examinations	Few and immaterial	Significant or material misstatements		
Examiner relationship with management	Cordial and constructive	Confrontations		
Response to supervision	Very responsive	Unresponsive		
Disclosures of director's and officer's outside interests	Fully disclosed	Not disclosed		
Background checks made on new directors, officers, and employees	Checked and verified	Not checked		
Internal auditor restrictions	None; auditor performs full scope reviews	Auditor works with restrictions, or on limited projects		
Internal auditor reporting	Reports to board or audit committee	Reports to management		
Internal audit department turnover	None or minimal	High		

General Factors	Indicator: Lower	Indicator: Higher	Comment or Description	Risk Factor
Liquid assets	Adequate (many primary and secondary sources)	Inadequate (few primary and secondary sources of liquidity)		
Policy exceptions to Board approved guidelines	No policy exceptions	Many policy exceptions		
Policies and procedures	Well developed for all areas of operations	None or poorly developed		
	Applied equally to employees and management	Not followed or circumvented by management or key employees		
Unusual or lavish fixed assets	None	Boats, aircraft, artwork, condos, etc.		
Internal controls	Sound system of controls	Material control deficiencies; or controls do not apply to top management		
Response of management in providing documents to examiners	Documents provided quickly	Long delays in getting documents		
Transactions with other financial institutions	Appropriate for business activities	Large transactions with small out of state banks		
Board reports	Accurate and complete	Inaccurate; inadequate; incomplete		
Organizational structure	Simple	Overly-complex		
Aggressive accounting practices/tax-motivated behavior	Few	Many		
Regulatory violations	Few	Many		
Criminal Referrals	Few	Many		
Consumer Complaints	Few	Many		
Falsified bank records	None	Many		

Lending Factors

Loan documentation	Well-documented loans and credit quality	Poorly documented loans		
Loan Concentrations	None	Many loan concentrations		
Loan performance tracking	Close review of problem credits by management and the board	No (or erroneous) past due or watch list reports		
Borrower financial statements	Borrowers' financial position well documented	No (or unsigned) financial statements		
Loan disbursements	Well documented; approved by an independent officer	Questionable; approved by loan officer		
Corporate loans	Proper endorsements and guarantees	No (or inadequate) endorsements and guarantees		
Resolution of problem loans	Well documented and reasonable	Questionable pay-downs prior to examination or audit		
Overdrafts	Properly approved; reasonable amounts	Large questionable overdrafts		
Refinancing	Well documented; properly approved	Poorly documented; refinanced by a different department		
Nominee loans	No nominee loans	Nominee loans made		
Loan terms	Loan size, rates and maturities appropriate	Loans of unusual size, rates, and maturities		
Evergreen/non-amortizing loans	No evergreen/ nonamortizing loans	Several large evergreen/ nonamortizing loans		
Real property sales history	Well-documented history of sales and ownership	No history of sales or ownership		
Out of territory loans	No out of territory loans	Many out of territory loans		
Brokered loans	No brokered loans	Loans from brokers		

Lending Factors	Indicator: Lower	Indicator: Higher	Comment or Description	Risk Factor
Adequacy of collateral	Loans adequately collateralized when appropriate	Large loans with unusual, questionable, or no collateral		
Collateral sales history	Collateral sales history is reasonable	Frequent sales; flipped collateral		
Loans to directors, officers, and employees	Properly underwritten and reported to the board of directors	Loans to uncreditworthy directors, officers, or employees		
Lending authority	Large approval limits are vested in the board or its committee	Large approval limits given to individuals or to inexperienced or inappropriate employees		
Third-party disbursements	Disbursements made to borrowers	Disbursements made to third parties		
Construction disbursements	Property inspected by independent institution officer prior to disbursement	No or poorly documented inspections; no rotation of inspectors		
Asset performance	Very low percentage of delinquent/nonperform-ing/classified assets	High percentage of delinquent/nonperforming/ classified assets		
Independent loan review function	Effective; independent loan review function	No (or ineffective) loan review		
Speculative, high-risk lending activities	Institution has conservative lending practices	Institution engages in high-risk lending activities		
Predatory lending practices	None	Institution engages in predatory lending practices		

Deposit Factors

Concentrations of deposits	No concentrations of deposits	High concentration of deposits by individuals, firms, or public entities		
Brokered deposits	No brokered deposits	High level of brokered deposits		
Growth in account types or account balances	No or low steady growth	Excessive volatile growth		
Training for all personnel on check fraud prevention	Comprehensive training program for all personnel on check fraud prevention	No training on check fraud prevention		
Training for all personnel on Identity Theft	Comprehensive training on Identity Theft	No training on Identity Theft		
Check cashing guidelines	Comprehensive check cashing guidelines	No check cashing guidelines		
New accounts	Comprehensive guidelines for opening new accounts	No guidelines for opening new accounts		
Signature cards	Signature cards secure, permanent, and updated	No control over signature cards		
Account changes	Account changes require identification and written requests	No controls over account changes		
Dormant accounts	Dormant account activity requires extra approvals or mandatory holds	No controls on dormant accounts		

[1] Required if factor is rated 4 or 5.

We modified the examination scope in the following areas in consideration of the risk factors identified above:

Questions and Answers - Examination Obstruction

Question: What should I do if an association tells me that the documents that I need are inaccessible because they are in remote storage off site?

Answer: Advise the association that it must give you the documents' specific location and immediate and complete access to wherever the association stored the documents (12 USC §1464(d)(1)(B)(ii) and 12 CFR § 563.170(c)).

Question: What should I do if an association refuses to provide me with access to any records until the OTS Director requests access, since 12 USC § 1464(d)(1)(B)(ii) uses the phrase, "upon request by the Director"?

Answer: As an examiner appointed by the Director, you have the delegated authority to act on the Director's behalf in the examination of federally insured thrifts (12 USC §§ 1462a(h)(4), 1463(a)(1) and 1464(a)). Your request for records meets these statutory requirements; the association must provide you with prompt and complete access.

Question: What should I do if an association asserts privilege and refuses to provide me with access to documents about a large, nonperforming commercial property loan because the borrower has sued the institution?

Answer: Consult with your Examiner-in-Charge (EIC), field manager, or regional counsel, as this is not a matter protected from regulatory review by an attorney-client privilege. The association must immediately instruct its counsel to provide you with prompt and complete access to all documents and records concerning the status of this loan (12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 563.170(c)).

Question: What should I do if an association tells me it has no underwriting records on a large, real property loan?

Answer: Advise the association that OTS will cite it for violation of 12 CFR §§ 560.100, 560.101, and/or 563.170(c), and proceed with a more thorough review of this asset. Remain alert to the possibility that the documents exist but are being withheld. Staff comments or documents in other files might indicate the missing association records were created. Like withholding documents, failure to create and maintain critical documents is a red flag indicating possible fraud, insider abuse, or financial manipulation. Keep your EIC or field manager apprised of your findings.

Question: What should I do if I request documents during a focused, special limited examination and the association denies me access because it is not a regularly scheduled, full-scope examination?

Answer: Federal law requires associations to provide examiners, including safety and soundness, compliance, trust, and information technology examiners, prompt and complete access to all association records and employees during any type of examination. The statue does not limit the authority to examinations of a specific length, scope, or type (12 USC § 1464(d)(1)(B)(ii)).

Question: What should I do if I request accounting records on a particular transaction and the association's auditor denies me access based on an assertion of accountant-client privilege?

Answer: There is no such generally recognized privilege. The auditor must provide you with prompt and complete access to the documents. Notify your regional counsel and regional accountant because this may be an ethical or contractual breach by the auditor.

Question: What should I do if an association denies my request outside an examination for access to the documents necessary to perform a status update on a large, troubled loan?

Answer: You are working to determine the condition of the association in the course of supervision. The association must give you prompt and complete access to all relevant documents and records of any type (12 USC § 1464(d)(1)(B)(iii)).

Question: What should I do if an association tells me that I may review copies of loan files maintained by computer, but may not review originals because the originals are stored off site in a remote facility for safekeeping and cannot retrieve the originals without considerable expense.

Answer: This is an impermissible screening tactic. As yet, you have no assurances that the copies are exactly the same as the originals or that the originals have all the required disclosures and signatures. You have no assurances that the originals ever existed, or still exist. Additionally, the association's computer may be tracking which documents you are retrieving, permitting the association to review and "correct" any problems with the originals before you see them. The association must provide you with prompt and complete access to all relevant documents of any type, especially originals, wherever those documents may be (12 USC § 1464 (d)(l)(B)(ii) and 12 CFR § 563.170(c)).

Question: What should I do if an association's board of directors refuses to allow me to observe their meetings, citing reasons such as highly confidential merger discussions, personnel issues, or the like?

Answer: 12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 563.170(c) obligate the association to allow you to attend the meetings. Additionally, you may remind the directors that 12 CFR § 510.5 prohibits you, as an examiner, from disclosing or permitting the disclosure of proprietary or confidential association information obtained through OTS examination and supervision functions.

Question: What should I do if an association designates a particular employee to assist the examination team to find and locate documents, but that employee is frequently unavailable to assist?

Answer: It may be appropriate for the association to designate an individual to assist the examination team, as long as the arrangement provides you with "prompt and complete" access to records and staff. You should insist upon access to information within a reasonable time. In some circumstances, a "reasonable" time may require immediate access to information. In all cases, because of examination schedules, the association must arrange to comply quickly with your information requests.

Question: What should I do if an association requires that outside counsel review requested documents for privilege before producing them for my review, or that an attorney be present when I wish to interview an employee?

Answer: In both cases, alert your EIC, field manager or regional counsel. In the first case, insist that counsel's review be conducted quickly and without unreasonably delaying your access to the documents. Insist upon access to the original documents and a written list of any requested documents withheld based on a claim of privilege. In the second case, requiring association counsel to be present is an impermissible restriction on your access to information. You should inform management that you would not agree to any such restrictive condition on your right to interview and obtain information from any officer, employee, or agent of the association.

Question: What do I do if the thrift holding company is an insurance company regulated by a state Insurance Commissioner?

Answer: Continue with your holding company exam as you normally would. (You may use information from, or provided to the state Insurance Commissioner. Regional offices should request applicable information in advance.) The Gramm-Leach-Bliley Act (GLBA) does not apply to holding companies or insured depository institutions themselves. Therefore, you may perform a full examination of the holding company (12 USC §§ 1831v(c) and 1467a(b)(4)).

Question: What do I do if I discover extensive business records of a functionally regulated affiliate at the holding company, along with other records that I have access to?

Answer: You may review any records maintained on holding company premises. Generally, the GLBA limits the circumstances under which you may go on the premises of a functionally regulated entity. The GLBA also limits your ability to order documents or talk to the staff of a functionally regulated entity. The GLBA does not prevent you from reviewing records maintained on holding company or association premises (12 USC § 1831v(a)).

Question: What do I do if I determine, in the course of an examination, that an insurance subsidiary of a thrift holding company may pose a material risk to the safety and soundness of the association? The functionally regulated affiliate provides low premium, large limit coverage for high risk items (concentrations of hurricane coverage along the Southeast Atlantic) and places its portfolio in high risk investments (junk bonds)?

Answer: You should have already reviewed the publicly available records, externally audited financial statements, information available at the holding company's premises, and any available state insurance commissioner's or regulator's examinations and other reports about the functionally regulated affiliate. You or your supervisor should have discussed your concerns with the commissioner's or regulator's office. Highlight the bases for your concerns in the documents available and discuss the information with your supervisor, regional counsel, and (possibly) the regional director. Together you will determine whether these facts warrant an on-site OTS examination of the functionally regulated affiliate. You should document your work paper files to indicate which of the GLBA criteria you base the justification for your examination. If there is the potential for enforcement action, such as the issuance of a subpoena, you should include regional enforcement counsel in your discussions.

Question: What should I do if the association engages in transactions with an affiliate that is functionally regulated and all of the transactions with affiliates (TWA) records are on the functionally regulated affiliate's premises?

Answer: We enforce the rules concerning the association's transactions with affiliates. Therefore, the association must provide you with "prompt and complete" access to all relevant documents and staff concerning any transaction involving the association wherever they may be, even if located on the premises of a functionally regulated affiliate. You may require an association to obtain and keep records necessary for it to oversee the transactions (12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 570(c)). Your review of the association's TWA materials at their storage site does not constitute the examination of a functionally regulated affiliate under the GLBA. An association or a thrift holding company cannot shield its documents or transactions from your review by storing them at the offices of a functionally regulated affiliate.

Question: What should I do if I need to interview a dual employee, a person who is employed both by the association and a functionally regulated affiliate?

Answer: You may interview the employee concerning matters within the scope of his or her duties and responsibilities on behalf of the association.