Fraud and Insider Abuse

Fraud and insider abuse significantly contributed to many thrift failures during the late 1980s and early 1990s, and caused substantial losses at many others. Because of this, several federal agencies now work closely together to combat fraud and insider abuse at financial institutions.

The Interagency Bank Fraud Working Group includes the five federal banking agencies, the Department of Justice (DOJ), and the Federal Bureau of Investigation (FBI). Representatives from these government agencies work together to establish policies to improve interagency cooperation and to resolve criminal investigation and prosecution problems.

All the agencies now use a uniform interagency Suspicious Activity Report (SAR) form. This is a form that federally insured financial institutions use to report suspected violations of federal criminal law and suspicious transactions related to money laundering offenses and Bank Secrecy Act violations. In addition, all the federal banking regulators have regulations that require insured institutions and service corporations to file SARs.

LINKS

Program

Appendix A

Appendix B

DOJ maintains the Significant Referral Tracking System. This system tracks the progress of SARs that the federal financial regulators designate as most significant. The DOJ provides tracking of their progress in local U.S. Attorneys' Offices.

To facilitate these interagency efforts, OTS designates a criminal referral coordinators. Their function is to coordinate reports of suspected criminal activities and provide assistance to the FBI and DOJ in criminal investigations and prosecutions.

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.

Every year, thrifts lose a significant amount of money due to insider abuse and criminal misconduct. The FBI estimates that insiders of financial institutions steal eight times more money than is stolen through bank robberies and burglaries.

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 activities:

- 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.
- Violations of criminal statutes, 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 abusive act, OTS has the responsibility and the authority to act against all insider abuse, whether criminal or not.

Many of the largest cases of financial institution fraud involved insiders. If the insider is in a key position, the amount of loss can be significant enough to cause the institution to fail. Often, these individuals perform criminal acts 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.

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. Often, discovering fraud is 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. Because of this, the 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?
- During the examination, what specific areas should we examine to ensure that there are no major fraud problems?
- Has anyone else 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?

Criminal Statutes

The following criminal statutes apply 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 § 1001

Knowingly and 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, loan (or any change or extension of same), including willfully overvaluing land, property, or security.

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.

18 USC § 709

This criminal statute applies restrictions on advertising and names used by non-federal persons or entities.

Significant Aspects:

- Prohibition, except where permitted by law, of the use of several words relating to federal entities without authority.

- Restrictions 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.

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

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 § 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 institution, 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.

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.

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. In addition, in face of increasing competition and shrinking margins many associations desire to cut costs, particularly in areas not directly tied to income. Associations must direct expense control to areas that do not compromise critical policies and procedures governing internal controls.

Internal Control Regulatory Requirements

The Federal Deposit Insurance Corporation Improvement Act of 1991 required the banking agencies to establish certain safety and soundness guidelines. Appendix A of 12 CFR Part 570, Interagency Guidelines Establishing Standards for Safety and Soundness, includes a section on operational and managerial standards. Pursuant to the standards, each savings association must have internal controls and an internal audit appropriate to the size of the association and the nature and scope of its activities. Pursuant to FDIC regulation 12 CFR § 363.5, Audit Committees, insured depository institutions with total assets of $500 million or more must have an audit committee composed of outside directors who are independent of management.

Internal Control System

When determining the effectiveness of an association's internal control system, you must be particularly alert to the following situations:

- Management does not implement effective procedures to correct internal control deficiencies noted in reports prepared by the internal auditors or the independent accountants.
- Management scales back or suspends the internal audit function.
- The internal auditor has dual, operational responsibilities that compromise the internal audit function.
- The internal auditor reports to management instead of directly to the board of directors or an audit committee.

- The association's independent audit firm does not have banking audit experience. A similar problem may exist when a nationally recognized accounting firm assigns auditors to a savings association audit who are not familiar with banking procedures and practices.
- The association discontinues the annual independent accountant's audit.
- The association does not have proper controls in high-risk lending areas (this could be the result of poor policies, frequent exceptions to policy, or understaffing).
- The association engages in new lending activities with inadequate or unqualified staff.
- The association often deviates from board-approved policies without exception documentation.
- The association fails to effectively segregate duties and responsibilities among employees.
- The association fails to provide adequate reports to the board of directors.

Internal Control System Critical Components

There are a number of common critical components in internal control systems that are applicable to all savings associations. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a report[1] that identified five critical components of a good internal control framework:

- Control environment
- Risk assessment
- Control activities
- Accounting, information, and communication systems
- Self assessment.

COSO defines internal control as a process to achieve the following objectives:

- Effectiveness and efficiency of operations including safeguarding assets.
- Reliability of financial reporting.
- Compliance with applicable regulations.

[1] Savings associations may obtain the COSO "Internal Control – Integrated Framework" (Product code #990009) from the Order Department, American Institute of Certified Public Accountants, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881. Toll-free telephone 1-888-777-7077; FAX 1-800-362-5066.

Generally accepted auditing standards incorporate in the AICPA Statement on Auditing Standards No. 78, Consideration of Internal Control in a Financial Statement Audit, the common critical elements of internal control systems contained in COSO. OTS urges savings association directors and management to review at least the major concepts described in the COSO report or other recognized standards and compare them to their association's internal control systems. Good internal control processes are only effective if properly understood and strictly followed. The board of directors must establish internal control systems policy and properly monitor implementation of the policy. Management must properly implement internal control systems according to board policy. In addition, internal and external auditors should vigorously check the appropriateness and effectiveness of savings associations' internal controls. See Examination Handbook Section 340, Internal Control.

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

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 attempted 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 and consider it a red flag indicating potentially serious problems, and take steps to prevent it.

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 penalty assessments. In addition, examination obstruction may subject management to criminal prosecution under 18 USC § 1517.

Red Flags of 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 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). Two associations used these illegal tactics recently and criminal prosecutions followed. If you suspect records alteration, notify your EIC, field manager, or regional counsel. 18 USC §§ 1005 and 1006.

- **Removal of Records**. In several notorious 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. The documents may be in the offices of the association's litigation counsel. You are entitled to review such documents 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 to this tactic 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 these serious problems, however, until the association stops the obstruction.

Whenever you meet any of the types of obstruction 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 you do not obtain access or if the association does not resolve the situation, you should inform your EIC or field manager. They will work with you, the 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 you meet and the Chief Counsel's suggestions as to the best way 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, RD, and/or regional counsel.

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

- Filing in the local United States District Court for an Order requiring that 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 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 suspicious activity report to the Department of Justice. 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.

Detecting Fraud and Insider Abuse

Because perpetrators do not always carefully plan and discreetly carry out fraud, if you are alert to certain warning signs you may be able to detect it. It is essential, however, that you are knowledgeable of the warning signs and are alert to circumstances where fraud may exist, either by insiders or outsiders. Once you suspect fraud you should thoroughly investigate the circumstances surrounding a suspected activity.

The primary problem that you face in detecting fraud is the limited time and resources available to conduct an examination. Certainly, if you are aware of it and it is material, you should devote the time necessary to determine the appropriate action. However, when you only mildly suspect it, such as with a hunch, it is difficult to justify expanding the examination scope. 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. When you consider the risk of fraud to be high you may expand your examination scope in the appropriate areas.

You must be alert to situations that may be conducive to fraud and insider abuse. 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, improper internal audit reporting relationships, etc., 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.

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 internal audit department turnover.
- Alteration of records.
- Withholding of records.
- Delaying tactics in providing documents or 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 actual documents – only provides copies.
- Hires ex-agency officials when faced with enforcement actions.
- High turnover of officials.
- 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.

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 and 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 year after year.
- Significant related party transactions not in the ordinary course of business.
- Significant bank accounts 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 transaction activities, evidence that a system fails to provide accurate output, or evidence of design flaws, among others.
- Known criminal referrals.

Red Flags of Lending Abuse

- Poorly documented loans and appraisals.
- Lack of an acceptable past due or watch list.
- Lack of, or unsigned, borrower financial statements.
- Questionable loan disbursement transactions.
- 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 number or amount of insider loans.
- Construction draws with no 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.

Red Flags of Appraisal Abuse

- No appraisal or property evaluation in file.
- One appraisal in file, but appraisers billed institution for more than one.
- 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.
- Made for borrower.

- Appraisals performed or dated after loan.
- Close relationship between appraiser, lender and/or borrower.

Red Flags of Check Fraud

Check fraud is one of the largest challenges facing financial institutions. Forty-three percent of the Suspicious Activity Reports between April 1996 and September 1997 related to check fraud, counterfeit checks, and check kiting. A 1996 study by the Federal Reserve estimated financial institutions suffered losses of $615.4 million involving 529.1 thousand cases in 1995. Savings associations accounted for $67.5 million of the losses and 65.4 thousand of the cases. The Check Fraud Working Group, a subgroup of the Interagency Bank Fraud Working Group prepared a booklet in February 1999, Check Fraud: A Guide to Avoiding Losses. In the booklet, the Check Fraud Working Group identifies and discusses in detail the following check fraud schemes:

- Altered checks.
- Counterfeit checks.
- Forged checks.
- Checks drawn on closed accounts.
- Identity assumption.
- Fraud by bank insiders.
- Telemarketing fraud.
- Check fraud by gangs.

Savings associations can 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.

Suspicious Activity Reports (SAR)

Filing Requirements

Paragraph (d)(3) of OTS regulation § 563.180, Suspicious Activity Reports and Other Reports and Statements, requires savings associations[2] and their service corporations to report suspicious activities. They are to file SARs with the appropriate federal law enforcement agencies and the Department of Treasury by sending them to the Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury. The regulation requires a filing after the discovery of a known or suspected federal criminal violation that involves any of the following persons or transaction:

- 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.

Section 563.180(d)(5) requires a savings association or service corporation to file an SAR no later than 30 calendar days after the date of initial detection. If there is no identified suspect on the date of detection, however, an association or service corporation may delay a filing up to an additional 30 days to identify a suspect. If a violation requires immediate attention, such as when it is ongoing, an association or service corporation must by telephone immediately notify an appropriate law enforcement authority and OTS. They must also file a timely SAR.

Section 563.180(d) also does the following:

- Encourages savings associations and their service corporations to file a copy of the SAR with state and local law enforcement agencies where appropriate.

- Provides that institutions need not file SARs for robberies and burglaries that they report to appropriate law enforcement authorities.

[2] Section 563.180(d) treats a savings association and its operating subsidiaries as one unit.

- Requires that institutions retain copies of SARs, and supporting documentation, for five years from the date they file them.

- Advises that failure to file a SAR in accordance with this section may subject the savings association, or service corporation, its officers, directors, employees, agents, or other institution-affiliated parties to supervisory action.

- Advises that the law shields financial institutions and their employees from civil liability when they report suspicious activities.

Financial Crimes Enforcement Network (FinCEN) inputs the information reported in SARs into a central database, which is accessible only to federal and state financial institution regulators and law enforcement agencies. The usefulness of the 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 service corporations have the primary responsibility to file SARs. You must, however, complete and file a SAR when the required filing institution has either failed to do so or has not properly completed or filed it. 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.

USA PATRIOT Act of 2001

In October 2001, President George W. Bush signed anti-terrorism legislation that gives law enforcement authorities an array of new powers to use in the nation's campaign against terrorism. The new law, called The USA PATRIOT Act of 2001, contains sweeping new surveillance powers for law enforcement agencies, but some of these new powers will expire in four years.

The new law's money laundering provisions will accomplish the following:

- Bolster law enforcement's ability to find and destroy the financing of terrorist organizations, whether in banks or in underground "hawala" systems.

- Establish a government-industry partnership to stop terrorist funding in real-time.

- Track any terrorist money kept in secret offshore havens and increase foreign cooperation with U.S. efforts.

- Require banks to monitor certain accounts held by non-U.S. citizens.

- Give the government the power to require foreign banks to reveal customers transaction information under certain conditions.

- Make it a crime to smuggle currency in excess of $10,000 and to knowingly falsify a customer's identity when making a transaction or opening an account with a financial institution.

- Create a highly secure Web site within the FinCEN, giving financial institutions the means to notify authorities quickly when a suspicious transaction takes place. Further measures would update counterfeiting laws to address technological advances used in the counterfeiting of U.S. currency.

You should be aware of the new law when examining institutions for fraud, internal control (especially wire transfers), or when reviewing SARs. If you have concerns or questions see the FFIEC BSA/AML Examination Manual.

Confidential Individual Information System

In addition to contributing to and using the FinCEN database, OTS utilizes its own automated system, the Confidential Individual Information System (CIIS), to record information on individuals. The recorded information concerns the following types of events:

- Enforcement actions.

- Referrals to a professional organization for disciplinary reasons.

- Liability suits, investigations as to unusual transactions.

- Certain application activity (such as acquisition or change of control, and procurement of a charter).

Other federal agencies and state authorities may access CIIS information, with the approval of the OTS national administrator or a region's CIIS administrator.

Regional Fraud and Insider Abuse Program

Each region must maintain a written fraud and insider abuse program, and should designate a person to be a Criminal Referral Coordinator to administer the program. The coordinator should act as a contact person or liaison to develop and maintain both internal and external fraud and insider abuse operations and communications.

While the extent of a regional program will be dependent on the incidences of fraud and insider abuse within the region, at a minimum each region (operations or legal) is responsible to do the following:

- Monitor and review regional SARs entered into the FinCEN system, particularly those that involve institution-affiliated persons or significant losses. As appropriate, communicate to the staff the reported suspicious activities.

- Ensure that institutions (and OTS staff, when necessary) complete and file accurate and timely SARs, including the providing of assistance and advice in such filings.
- Exchange information with and provide assistance to the FBI, Department of Justice, and other agencies, and ensure that appropriate persons follow up promptly on important SARs.
- Participate with local interagency bank fraud working groups that meet within the region.
- Ensure compliance with the Right to Financial Privacy Act as it relates to providing information and documentation to law enforcement and other government agencies.
- Work with OTS regional counsel office and OTS Enforcement Division in matters that relate to investigations for criminal prosecution or civil enforcement actions.
- Be able to provide background information reports on regional fraud and insider abuse cases, including prosecutions in progress and the outcome of important institution-affiliated person cases.

Regional directors are responsible to ensure that regional staff receives adequate training to accomplish the examination objectives and procedures set forth in this handbook section.

REFERENCES

United States Code (12 USC)

§ 3401	Right to Financial Privacy Act of 1978

United States Code (18 USC)

§ 215	Kickbacks and Bribes
§ 657	Theft, Embezzlement, or Willful Misapplications of Funds
§ 709	False Advertising or Misuse of Names to Indicate Federal Agency
§ 1001	General False Statements
§ 1006	False Entries or Reports
§ 1014	False Statements
§ 1344	Bank Fraud
§ 1517	Obstructing Examination of Financial Institution

Code of Federal Regulations (12 CFR)

Part 215	Regulation O, Loans to Executive Officers, Directors and Principal Shareholders of Member Banks
§ 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
§ 563.130	Prohibition on Loan Procurement Fees
§ 563.170(a)	Examinations and Audits
§ 563.180(d)	Suspicious Activity Reports
§ 563.200	Conflicts of Interest

Office of Thrift Supervision Bulletins

RB 20	Proper Investigation of Applicants and Increased Communication Between OTS and other Financial Institution Regulatory Agencies

Interagency Guidance and Forms

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

Suspicious Activity Report Form

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)