INSIDER FRAUD AND ABUSE

Core Analysis Procedures

Examiners are to consider these procedures but are not expected to perform every procedure at every bank. Examiners should complete only the procedures relevant for the bank's activities, business model, risk profile, and complexity. References to laws, regulations, supervisory guidance, and other resources are not all-inclusive.

Background: The purpose of this module is to assist examiners in assessing an institution's controls that can prevent and mitigate fraudulent activities from institution insiders.

Often insider fraud occurs because of poorly designed controls and weak governance, undermining the institution's processes. Examiners are responsible for assessing the adequacy of, and identifying any deficiencies in an institution's internal control environment, audit functions, and board and management oversight. The presence of dominant officials, or the presence of officials and employees with close personal or business ties to controlling shareholders, when coupled with other risk factors such as weak internal controls, elevates the risk of fraudulent activity. Additionally, institutions exhibiting weak corporate governance, weak board oversight, or a lack of influence by independent directors can diminish an institution's ability to establish, adhere to, and monitor compliance with internal controls and policies. Other warning signs include but are not limited to: a high volume of insider transactions, uncooperative or hostile management, and inadequate internal or external audit programs.

Examiners are encouraged to refer to the following ED Modules and work programs during this review:

- *Other Assets/Other Liabilities*
- *Loan Operations*
- *Management and Internal Control Evaluation*
- *InTREx*
- *BSA Workprogram*

Preliminary Review

1. If not already completed, review prior examination reports and work papers, Suspicious Activity Reports (SAR) filed with the Financial Crimes Enforcement Network (FinCEN) indicating possible insider fraud,[1] and file correspondence for any insider fraud and abuse exceptions or other potentially adverse management related issues, including dominant management officials[2] allowed to exert influence without restraint.

2. Determine whether management and the board have taken corrective actions to address concerns identified in prior examinations.

[1] **SARs associated with insider abuse would most likely be filed on individuals whose "Relationship to Institution" is employee, officer, director, and sometimes shareholder.**

[2] **The presence of a dominant official should not be viewed negatively or as a supervisory concern in and of itself. Rather, the presence of a dominant official coupled with other risk factors such as ineffective internal controls, lack of board independence or oversight, or engaging in risky business strategies, may create supervisory concerns or require enhanced supervision.**

3. If not already completed, review internal and external audit reports. • **For external audit reports, determine the type of opinion provided (i.e., unqualified, qualified, adverse, or disclaimer). If the opinion is qualified, adverse, or disclaimer, obtain an understanding of the reason for the opinion.** • **For internal audit reports, review the conclusions drawn by internal auditors on audits that included insider threat within the scope of the review.** • **Assess whether internal or external auditors worked with any restrictions imposed by management.[3]**
4. Discuss insider fraud and abuse with appropriate institution personnel, internal auditors, and, if necessary, external auditors to assess the institution's monitoring and controls to mitigate insider fraud and abuse. Determine whether auditors have made any reports (formal or informal) on suspected insider fraud and abuse to the board or others.
5. Review off-site risk monitoring tools to identify whether the institution warrants increased supervisory attention because of an increased susceptibility to insider fraud. Focus on risk indicators in those tools.[4]
6. Review for general signs of potential insider fraud and abuse. Consider whether there is evidence of: • **Misstatements by management detected in prior audits or examinations.** • **Restrictions on internal auditors, or limits on audit projects.** • **Restrictions on the flow of information to the board, e.g., situations in which a dominant official is the only insider on the board.** • **An overly complex organizational structure, particularly considering the size of the institution.** • **Unusual or lavish lifestyles of institution personnel.**
Policies and Procedures

[3] Independence and objectivity is a key component of an internal audit system, which includes appropriate segregation from management and operations personnel. Appropriate segregation is generally evidenced by independent reporting lines and procedures that are independent of the influence of management or operations personnel. Restrictions imposed by management may impede independence.

[4] FDIC: Refer to ICARuS.

7. If not already completed, evaluate the institution's policies and procedures[5] addressing insider fraud and abuse. Consider whether policies and procedures address:

- **Communication from the board that establishes the board's attitude towards insider abuse or conflict of interest.**
- **Processes for assessing the institution's risk exposure to insider fraud and abuse.**
- **Prevention techniques to avoid potential insider fraud and abuse events.**
- **Detection and analysis techniques to uncover insider fraud and abuse.**
- **An insider fraud response plan that outlines a process for the Audit Committee to investigate and report fraud allegations or suspicious activity involving officers and directors.**
- **An established set of potential consequences for institution insiders noncompliant with policies such as the Code of Conduct.**
- **Ongoing background screening to periodically review insider activity, credit reports (where allowed by law), employee email accounts, public records, deposit and loan accounts, and accounts that insiders have signature authority over.**
- **A retrospective review process for situations where insider abuse and fraud occurs.**

8. Review and assess policies to determine whether:

- **All institution affiliated parties (including directors and officers) are required to sign a code of conduct statement acknowledging that they have reviewed and will abide by the code of conduct.**
- **The written policies provide clear guidance on what behaviors and actions are permitted and which are prohibited, including theft and embezzlement.**
- **Policies address allowable nonbank activities, acceptance of gifts or gratuities in the normal course of business, potential conflicts of interest, related-party transactions, and illegal acts and fraud.**
- **Policies govern access to work areas during mandatory time-off or enforced leave.**
- **Policies address restrictions on unauthorized removal of documents, work papers, computer files, and other proprietary data and records from the institution's premises by physical or electronic means, including customer personally identifiable information (PII).**
- **Policies advise insiders that they may be held personally liable for acts of willful misconduct, gross negligence, theft, or embezzlement-related activity.**
- **The institution has established mechanisms to monitor and enforce its conflict of interest policies.**
- **The policies are applied universally and enforced uniformly at all levels (employee, officer, director).**

9. Evaluate policies and practices regarding background and credit checks performed on new hires. Consider whether:

- **Background checks include researching regulatory enforcement action databases, and criminal background checks;**
- **Credit checks (where allowed by law and in compliance with legal protections) are conducted at intervals throughout an insider's employment with the institution; and**

[5] Policies and procedures may include the employee handbook, code of conduct, employee ethics, and other similar policies and procedures.

- **Board members and officers are subject to a background check process consistent with that of employees.**

10. Determine whether the institution provides periodic training on its code of conduct, employee ethics policy, and conflicts of interest policy.

11. Determine whether the institution tracks exceptions to these policies and the reasons for the exceptions. Consider whether any such exceptions are reported to the board or Audit Committee.

AUDIT

12. Determine whether internal audit coverage over insider transactions and activities is sufficient to substantiate the effectiveness of internal controls. Consider:

- **Whether auditors have unrestricted authority and qualifications to audit all insider activities, including activities of officers and directors.**
- **If the institution has no internal audit function, the board and management's rationale and mitigating factors (e.g., strong external audit or director's examination and internal control system, extensive separation of duties, strictly enforced mandatory vacation policies with duties handled by other employees).**
- **The extent to which internal auditors perform employee account reviews. Consider whether:**
  - **Director and officer accounts are also subject to review; and**
  - **Travel expenses and corporate credit card records are reviewed for potential abuses.**

13. Determine whether internal audit reviews and assesses the effectiveness of internal policies, such as the employee handbook, code of conduct, employee ethics, and other policies and procedures with respect to conflicts of interest, as well as compliance with these policies by staff and management.

14. If not already completed, review whether audit assesses the controls that could prevent employees, officers, and directors from perpetrating fraud and abuse. If significant control weaknesses or higher than acceptable risk of fraud was identified by audit, expand the examination scope.

15. Evaluate the board and management's follow-up actions regarding specific audit findings involving insider activity, and any other reported discrepancies that could indicate potential insider fraud and

abuse. This includes determining whether the institution has reported suspicious activity related to insider fraud to law enforcement through filing a SAR.[6] If the institution has not filed a SAR as required, examiners should follow their Agency's protocol.

16. Evaluate any recent internal audit that reviewed insider lending activities. Consider whether:

- **The internal audit includes a review of compliance with the code of conduct, employment practices, loan review systems, and internal controls.**
- **Internal audit procedures target insider loan transactions.**
- **The internal audit scope includes a review of general ledger suspense accounts such as loans in process, and charged-off loans and recoveries.**
- **The audit identified inaccuracies or a lack of completeness in documentation.**
- **Post-mortem reviews of large loan charge-offs are conducted to identify possible insider misconduct.**

17. Determine whether internal audit reports to an Audit Committee or the full board, or whether internal audit reports directly to management.

Lending Factors

18. Determine whether the institution has systems in place to detect and report insider loan frauds. Consider what the institution's processes are for identifying insider loan frauds, such as the following:

- **Nominee loans and similar transactions constructed to circumvent laws, regulations, and the internal lending limits or internal lending policies.**
- **Loans to limited liability companies and other such entities where an insider may have an undisclosed financial interest in the entity.**
- **Bribes and kickbacks arising from loan origination activities.**
- **Loans tied to favors for friends and family members, including non-monetary consideration.**
- **Fictitious loans.**
- **Manipulation in the sale and purchase of loan pools.**
- **Other real estate owned sold through preferential contracts not at arm's length.**
- **Inappropriate or fraudulent loan arrangements used to purchase bank or bank holding company stock.**
- **Unusual lending-related transactions, such as large or frequent cash payments.**

[6] An institution is required to file a SAR when it detects a known or suspected criminal violation of federal law (including violations involving insider abuse of any amount), a suspicious transaction related to potential money laundering, or a violation of the Bank Secrecy Act (31 CFR 1020.320; 12 CFR Title 208.62 (FRB); 12 CFR 353.3 (FDIC)).

19. Evaluate the institution's independent loan review system relative to insider loans. Effective procedures and practices generally include:

- **Reviewing insider loans within a reasonable time period after origination.**
- **Reviewing loan disbursements to ensure they are well documented and approved by an independent officer.**
- **Promptly identifying loans with well-defined weaknesses that may indicate fictitious or fraudulent activity benefitting insiders.**
- **Identifying loans with multiple extension renewals, or rewrites that are exceptions to policy.**
- **Assessing lending and conflict of interest policies and adherence to these policies.**
- **Loan samples determined independently by the loan reviewer.**
- **Empowering loan review personnel to challenge transactions that look suspicious, especially if the transactions have been executed by or on behalf of an executive officer or board member.**
- **Individual loan reviews sufficient in depth and documentation.**

20. Use examination loan analysis tools to identify and assess anomalies in the loan portfolio that may suggest evidence of loan fraud. Factors to consider include:

- **Lack of loan balance amortization.**
- **Loans with excessive accrued interest not listed as past due.**
- **Loans with interest rate anomalies.**
- **Loans to different borrowers who all list the same address or P.O. box.**

21. Review board packets and other documentation provided to board members.

- **Determine whether the board monitors and supervises the actions of the loan officers to ensure that loan officers are executing their duties and loan authority under the loan policy and delegations of authority granted by the board.**
- **Review overdraft and past due loan reports at random date(s) other than quarter-end or month-end and identify and investigate any major variations versus the reports provided to the board.**

Other Factors

22. Determine whether the institution displays a pattern of inaccurate accounting practices or disclosure of errors and omissions. Consider whether there is evidence of:

- **Frequent or material errors and omissions on Call Report filings.**
- **High management turnover in senior accounting or internal audit department personnel.**
- **Significant volumes of difficult-to-audit transactions or balances.**
- **Concentrations in complex and hard to value assets.**
- **Poorly designed or ineffective accounting controls.**
- **Income and expense posting, reconcilement, and review functions that are not independent of each other.**

23. Determine whether the institution maintains a list of directors' and officers' outside interests (refer to Regulation O ED Module, if completed). Review whether the institution conducts due diligence, such as public records searches, to identify any interests that may not have been disclosed.
24. Consider whether there is evidence of potential insider fraud and abuse. Signs may include: • **High emphasis placed on meeting earnings projections.** • **Policies and procedures are poorly developed or not applied universally to employees, officers, and board members.** • **Abnormally long delays by management in providing documents to examiners.** • **Falsified records.** • **File maintenance entries made without review by an independent party.**
25. Review correspondent account activity for unusual or stale items. Consider obtaining a transcript of debits and credits on general ledger correspondent accounts and trace a sample of entries.
26. Determine whether the institution is completing appropriate customer due diligence and ongoing monitoring on insider accounts in order to identify potential suspicious activity.[7]
27. Review insider account activity, and account activity on accounts where insiders have signature authority, but are not the account owner. Consider obtaining: • **A list of all insider deposit account statements mailed to or retained by the institution.** • **An electronic download of all deposit accounts, to verify all accounts associated with insiders and their related interests.**

[7] Refer as needed to CDD Overview and Procedures, CDD Work Program/Procedures, SAR Overview and Procedures, and SAR Work Program/Procedures.

28. Obtain a copy of the general ledger and income statement for a date(s) other than quarter-end or month-end. Compare account balances for that date to quarter-end figures and investigate the cause of material and unusual variances.[8]
29. Evaluate the trend in cash and due from balances to average assets over time. Determine the cause(s) for any significant sustained buildup or large balances in these noninterest earning accounts.
30. Determine whether the general ledger system and information technology access rights are appropriately assigned, reviewed, and managed (discuss with IT examiner). Determine whether only authorized employees may edit or post to general ledger accounts.
31. Determine whether the institution has a policy requiring an annual two-week absence from duties, with someone else actually performing those duties. Consider whether electronic/remote access is disabled for the individual during those two weeks to prevent potential clandestine ongoing maintenance.
32. Determine whether the institution performs periodic insider fraud and abuse awareness training[9] at all levels in the institution.
33. Assess whether controls are in place over teller drawers, automated teller machines (ATM), and vault cash. • **Determine whether procedures for periodically verifying vault cash are adequate.** • **Review the vault cash, ATM, and teller drawer audits to determine the frequency, scope, and extent of the verifications.** • **Determine whether audits have been conducted of <u>all</u> personnel responsible for handling vault, ATM, and teller drawer cash within an acceptable time frame.**

[8] E.g., the Other Liabilities account may reflect fraudulent entries for suspense or inter-branch accounts that could be rolled over every other day to avoid stale dates, causing shortages of any amount to be effectively concealed for indefinite periods of time.

[9] Such training not only puts all directors, officers, and employees on notice about the institution's attitude towards fraud, it increases the perception of detection in the mind of the at-risk individual, and increases the odds of coworkers noticing red flags and enabling them to tip off the institution to potential risk.

End of Core Analysis