EXHIBIT 108

OCC Bulletin 2019-37 | July 24, 2019

Operational Risk: Fraud Risk Management Principles

To

Chief Executive Officers and Chief Risk Officers of All National Banks, Federal Savings Associations, and Federal Branches and Agencies; Technology Service Providers; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Summary

The Office of the Comptroller of the Currency (OCC) is issuing this bulletin to inform national banks, federal savings associations, and federal branches and agencies (collectively, banks) of sound fraud risk management principles. This bulletin supplements other OCC and interagency issuances on corporate and risk governance, including the references listed in appendix A of this bulletin.

Note for Community Banks

This guidance applies to all OCC-supervised banks.

Highlights

The risk management principles addressed in this bulletin include the following:

- A bank should have sound corporate governance practices that instill a corporate culture of ethical standards and promote employee accountability.
- A bank's risk management system should include policies, processes, personnel, and control systems to effectively identify, measure, monitor, and control fraud risk consistent with the bank's size, complexity, and risk profile.
- A bank's risk management system and system of internal controls should be designed to
  - prevent and detect fraud.
  - appropriately respond to fraud, suspected fraud, or allegations of fraud.
- Bank management should assess the likelihood and impact of potential fraud schemes and use the results of this assessment to inform the design of the bank's risk management system.
- Senior management and the board of directors should measure, monitor, and understand fraud losses across the enterprise and employ tools that appropriately quantify and assess loss experience and exposure.
- Control reviews and audits should include fraud risk as part of their assessments.

Fraud risk management principles can be implemented in a variety of ways and may not always be structured within a formal fraud risk management program. Regardless of the structure, fraud risk management should be commensurate with the bank's risk profile. Banks with significant and far-reaching retail-oriented business activities should have well-documented fraud risk management programs with appropriate monitoring, measurements and reporting, and mitigation.

Background

Fraud may generally be characterized as an intentional act, misstatement, or omission designed to deceive others, resulting in the victim suffering a loss or the perpetrator achieving a gain.[1] Fraud is typically categorized as internal or external.

- **Internal fraud** occurs when a director, an employee, a former employee, or a third party engaged by the bank commits fraud, colludes to commit fraud, or otherwise enables or contributes to fraud.
- **External fraud** consists of first-party fraud and victim fraud. External fraud is committed by a person or entity that is not a bank employee, a former employee, or a third party engaged by the bank.
  - **First-party fraud** occurs when an external party, including a bank customer, commits fraud against the bank.
  - **Victim fraud** occurs when a bank customer or client is the victim of an intentional fraudulent act.

Fraud schemes are often ongoing crimes that can go undetected for months or even years and can be time consuming and costly to address. It is often difficult to fully understand and quantify the extent of the fraud and the harm caused. Measuring losses associated with fraud is often an inexact process. Typically, the true cost of fraud is greater than the direct financial loss, given the time and expense to investigate, loss of productivity, potential legal and compliance costs associated with remediation, and impact on a bank's reputation.

Fraud risk is a form of operational risk, which is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.[2] Operational risk management weaknesses can result in heightened exposure to fraudulent activities, which can increase a bank's exposure to reputation and strategic risks. Failure to maintain an appropriate risk management system could expose the bank to the risk of significant fraud, defalcation (e.g., misappropriation of funds by an employee), and other operational losses.

Governance

Strong governance is of paramount importance to controlling the bank's exposure to fraud, and a strong corporate culture against fraud is crucial regardless of a bank's size or complexity. The tone at the top sets the foundation on which the bank operates. The board and senior management have a responsibility to lead by example and demonstrate that the bank is serious about promoting ethical behavior to deter and prevent fraud. The board-adopted code of ethics (or code of conduct) should encourage the timely communication and escalation of suspected fraud through the appropriate oversight channel.

The board is ultimately responsible for oversight but may delegate fraud risk management-related duties to specific committees (for example, the audit committee or operational risk management committee). The board also may delegate anti-fraud responsibilities to specific executives and managers, including those in charge of managing risks and controls. Roles and responsibilities should be clearly defined. The board should hold management accountable for effective fraud risk management and alignment of anti-fraud efforts with the bank's strategy, objectives, risk appetite, and operational plans. While not all fraud can be avoided, an active board can foster an environment in which fraud is more likely to be prevented, deterred, and promptly detected.

A sound corporate culture should discourage imprudent risk-taking. Incentives or requirements for employees to meet sales goals, financial performance goals, and other business goals, particularly if such goals are aggressive, can result in heightened fraud risk.[3]

Risk Management

Sound fraud risk management principles should be integrated within the bank's risk management system commensurate with the bank's size, complexity, and risk profile. Bank management should periodically assess the likelihood and impact of

potential fraud schemes and use the documented results of this assessment to inform the design of the bank's risk management system and evaluate fraud control activities. Policies should clearly define, establish, and communicate the board's and senior management's commitment to fraud risk management. Processes should be designed to anticipate fraud and deploy a combination of preventive controls and detective controls. Detective controls are important because even with strong governance and oversight, collusion or circumvention of internal controls can allow fraud to occur. Some practices and controls may be both preventive and detective in nature.

Preventive controls are designed to deter fraud or minimize its likelihood. The following are some examples:

- Policies and processes (e.g., ethics policies, code of conduct, identity theft program,[4] and elder abuse policies)
- Anti-fraud awareness campaigns for board, senior management, staff, and third parties
- Fraud risk management training for employees and contractors commensurate with roles and responsibilities
- Customer education on fraud risks and preventive measures customers can take to reduce the risk of becoming victims
- System controls designed to prevent employees, agents, third parties, and others from conducting fraudulent transactions, performing inappropriate manual overrides, or manipulating financial reporting
- Controls to prevent fraudulent account opening, closing, or transactions
- Dual controls (e.g., over monetary instruments, accounting, customer transactions, and reporting)
- Segregation of duties
- Background investigations for new employees and periodic checks for existing employees and third parties

- Training customer-facing employees to identify potential victim fraud
- Sound information security programs[5]
- Job breaks, such as mandatory consecutive two-week vacations or rotation of duties
- Customer identification program procedures, customer due diligence processes, and beneficial ownership identification and verification[6]
- Real-time transaction analysis and behavioral analytics

Detective controls are designed to identify and respond to fraud after it has occurred. The following are some examples:

- Models, monitoring systems, or reports designed to detect fraudulent activity across all lines of business and functions (e.g., exception reports, unusual card activity, unauthorized transactions, file maintenance reports, fee waiver analysis, and employee surveillance processes [account monitoring, system access patterns, and overrides])
- Data analytics (e.g., loss data analysis, transactions, fee waivers, interest forgiven, charge-offs, errors, and consumer complaint data)
- Effective complaint resolution processes[7]
- Monitoring and analysis of civil and criminal subpoenas received by the bank or information requests under section 314 of the USA PATRIOT Act[8]
- Monitoring and analysis of Bank Secrecy Act report filings by the bank and its affiliates
- Monitoring of news and other information concerning civil and criminal lawsuits
- Ethics and whistleblower reporting channels or hotlines
- Exit interviews for departing employees

Software and technology tools, developed internally or purchased from a third party, can assist with anti-fraud efforts. Bank management should consider the cost

and value of fraud prevention tools selected, consistent with the bank's overall strategy, complexity, and risk profile. Depending on the specific products and services offered, management might deploy solutions that serve to detect anomalies and prevent potential fraudulent transactions or activities. These solutions can monitor transactions and behaviors, employ layered or multifactor authentication, monitor networks for intrusions or malware, analyze transactions on internal bank platforms, and compare data with consortium or publicly available data. Banks' fraud prevention and detection tools should evolve and adapt to remain effective against emerging fraud types.

Fraud Risk Measurement and Monitoring

Senior management should understand the bank's exposure to fraud risk and associated losses across all business lines and functions and use this information to effectively monitor and manage fraud risk. The board should receive regular reporting on the bank's fraud risk assessment, resulting exposure to fraud risk, and associated losses to enable directors to understand the bank's fraud risk profile. Reporting should allow management and directors to measure performance. Practices can include benchmarking current fraud losses against loss history or industry data.

Examples of metrics and analysis banks can use to measure and monitor fraud risk include the following:

- Metrics by fraud type (e.g., internal, external, loan, card, account opening, check, or embezzlement)
- Fraud losses (e.g., per open account, closed account, or litigation)
- Fraud recoveries
- Net fraud losses
- Fraud loss budget variance
- Automated clearing house return rates

- Percentage of customers claiming victim fraud
- Fraud control performance and control testing results
- Trend analysis of data such as
  - number and dollar of fraud investigations
  - customer complaints
  - Bank Secrecy Act report metrics (e.g., Suspicious Activity Report [SAR] filings)
  - civil and criminal subpoenas
  - information requests under section 314 of the USA PATRIOT Act

Management should identify fraud losses as internal or external. Larger, more complex banks generally maintain this information in an operational loss database or similar system.[9]

Fraud Response, Reporting, and Information Sharing

A bank's policies, processes, and control systems should prompt appropriate and timely investigations into, responses to, and reporting of suspected and confirmed fraud. Banks should have processes for internal investigations, law enforcement referrals, regulatory notifications,[10] and reporting. A bank is required to file a SAR for known or suspected fraud meeting regulatory thresholds.[11] Reporting mechanisms should relay relevant, accurate, and timely fraud-related information from all lines of business to appropriate oversight channels.

Sound fraud risk management processes can include voluntary sharing of information with other financial institutions under section 314(b) of the USA PATRIOT Act. Pursuant to section 314(b), before exchanging information, the bank must register with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). Current section 314(b) participants may share

information with one another regarding individuals, entities, organizations, and countries for purposes of identifying and, when appropriate, reporting activities that may involve possible specified unlawful activities. FinCEN has issued guidance clarifying that, if section 314(b) participants suspect that transactions may involve the proceeds of specified unlawful activities, such as fraud, under the money laundering statutes,[12] information related to such transactions can be shared under the protection of the section 314(b) safe harbor.[13]

Reviews and Audits

A bank should design and perform reviews and audits specific to the bank's size, complexity, organizational structure, and risk profile. Reviews and audits should be designed to assess the effectiveness of the bank's internal controls and fraud risk management. Effective internal and external audit programs are a critical defense against fraud and provide vital information to the board of directors about the effectiveness of internal control systems.

Reviews and audits typically include the following:[14]

- Quality assurance and quality control reviews
- Independent risk management reviews
- Internal and external audits
- Retrospective reviews after fraud is identified
- Third-party relationship audits (or audit reports) consistent with contractual provisions

When auditing financial statements and asserting effectiveness of internal controls over financial reporting, auditors must consider a material misstatement due to fraud.[15] If the auditor identifies that fraud may be present, the auditor must discuss these findings with the board or management in a timely fashion.[16] The auditor

must also determine whether they have a responsibility to report the suspected fraud to the OCC.[17]

Findings and results from audits and reviews should be communicated to the relevant parties in a timely manner. Management should take timely and effective corrective action in response to deficiencies identified.

Further Information

Please contact Tanya A. Oskanian, Payments Risk Policy, Operational Risk Division, at (202) 649-6550.

Grovetta N. Gardineer
Senior Deputy Comptroller for Bank Supervision Policy

Appendix A

OCC Publications

- *Comptroller's Handbook*
  - "Bank Supervision Process"
  - "Community Bank Supervision"
  - "Corporate and Risk Governance"
  - "Federal Branches and Agencies Supervision"
  - "Insider Activities"
  - "Internal and External Audits"
  - "Large Bank Supervision"
- "Check Fraud: A Guide to Avoiding Losses"
- OCC Advisory Letter 1996-6, "Check Kiting, Funds Availability, Wire Transfers"

- OCC Advisory Letter 2001-4, "Identity Theft and Pretext Calling"
- OCC Bulletin 2007-2, "Guidance to National Banks Concerning Schemes Involving Fraudulent Cashier's Checks"
- OCC Bulletin 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies"
- OCC Bulletin 2011-21, "Interagency Guidance on the Advanced Measurement Approaches for Operational Risk"
- OCC Bulletin 2013-29, "Third Party Relationships: Risk Management Guidance"
- OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"
- OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
- OCC News Release 2009-65, "Agencies Issue Frequently Asked Questions on Identity Theft Rules"
- *Office of Thrift Supervision Examination Handbook* section 360, "Fraud and Insider Abuse" (federal savings associations)

FFIEC Publications

- "The Detection, Investigation and Prevention of Insider Loan Fraud: A White Paper," May 2003
- "The Detection, Investigation, and Deterrence of Mortgage Loan Fraud Involving Third Parties: A White paper," February 2005
- "The Detection and Deterrence of Mortgage Fraud Against Financial Institutions: A White Paper," February 2010
- *FFIEC Information Technology Examination Handbook*
- *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*

Other

- American Institute of Certified Public Accountants, AU-C section 240
- Committee of Sponsoring Organizations of the Treadway Commission and Association of Certified Fraud Examiners, "Fraud Risk Management Guide" and "Executive Summary"
- FinCEN, FIN-2009-G002, "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act"
- FinCEN, "Section 314(b) Fact Sheet" (November 2016)
- International Standard on Auditing 240
- Public Company Accounting Oversight Board, Auditing Standard 2401

---

[1] This bulletin discusses fraud in a broad context and is not limited to bank fraud as defined in 18 USC 1344, "Bank Fraud."

[2] Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for a full definition of operational risk.

[3] Refer to OCC Bulletin 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies," and 12 CFR 30, appendix D, II.M.4, "Compensation and Performance Management Programs."

[4] Refer to 12 CFR 41, subpart J, "Identity Theft Red Flags," which addresses identity theft red flags and address discrepancies under sections 114 and 315 of the Fair and Accurate Credit Transactions Act, 15 USC 1681m and 1681c.

[5] Refer to 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards," and the *Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook*.

[6] Refer to 12 CFR 21.21, "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance"; 31 CFR 1010.230, "Beneficial Ownership Requirements for Legal Entity Customers"; and the *FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*.

[7] Refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook* for more information.

[8] Refer to 31 CFR 1010.520, "Information Sharing Between Government Agencies and Financial Institutions," and 1010.540, "Voluntary Information Sharing Among Financial Institutions." Refer also to the "Information Sharing" section of the *FFIEC BSA/AML Examination Manual*.

[9] Refer to the "Large Bank Supervision" booklet of the *Comptroller's Handbook* and OCC Bulletin 2011-21, "Interagency Guidance on the Advanced Measurement Approaches for Operational Risk."

[10] Banks should notify regulators of significant incidents that could affect the bank's condition, operations, reputation, or customer information. Banks also should notify regulators of significant incidents that could affect the financial system.

[11] Refer to 12 CFR 21.11, "Suspicious Activity Report" (national banks), and 12 CFR 163.180, "Suspicious Activity Reports and Other Reports and Statements" (federal savings associations).

[12] Refer to 18 USC 1956–1957.

[13] For more information, refer to FinCEN's FIN-2009-G002, "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act," and "Section 314(b) Fact Sheet."

[14] Refer to the "Corporate and Risk Governance" and "Internal and External Audits" booklets of the *Comptroller's Handbook*. Refer also to OCC Bulletins 2013-29, "Third Party Relationships: Risk Management Guidance," and 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29."

[15] Refer to the American Institute of Certified Public Accountants' AU-C section 240, Public Company Accounting Oversight Board Auditing Standard 2401, and International Standard on Auditing 240.

[16] Refer to the American Institute of Certified Public Accountants' AU-C section 240.39.

[17] Refer to the American Institute of Certified Public Accountants' AU-C section 240.42.

Topic(s):
- BANK INFORMATION TECHNOLOGY (BIT)
- CORPORATE & RISK GOVERNANCE (CARG)
- OPERATIONAL RISK MANAGEMENT