Bank Fraud Risk Management

VIRGINIA BANKERS ASSOCIATION

May 9, 2023

360factors™

Session Objectives

Key learning objectives include:

- Fraud Examples – Old and New
- Fraud Risk Management – OCC Bulletin 2019-37, July 2019
- Data tracking – Type, amount, sources of information

What is important to you?

Fraud Types

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.

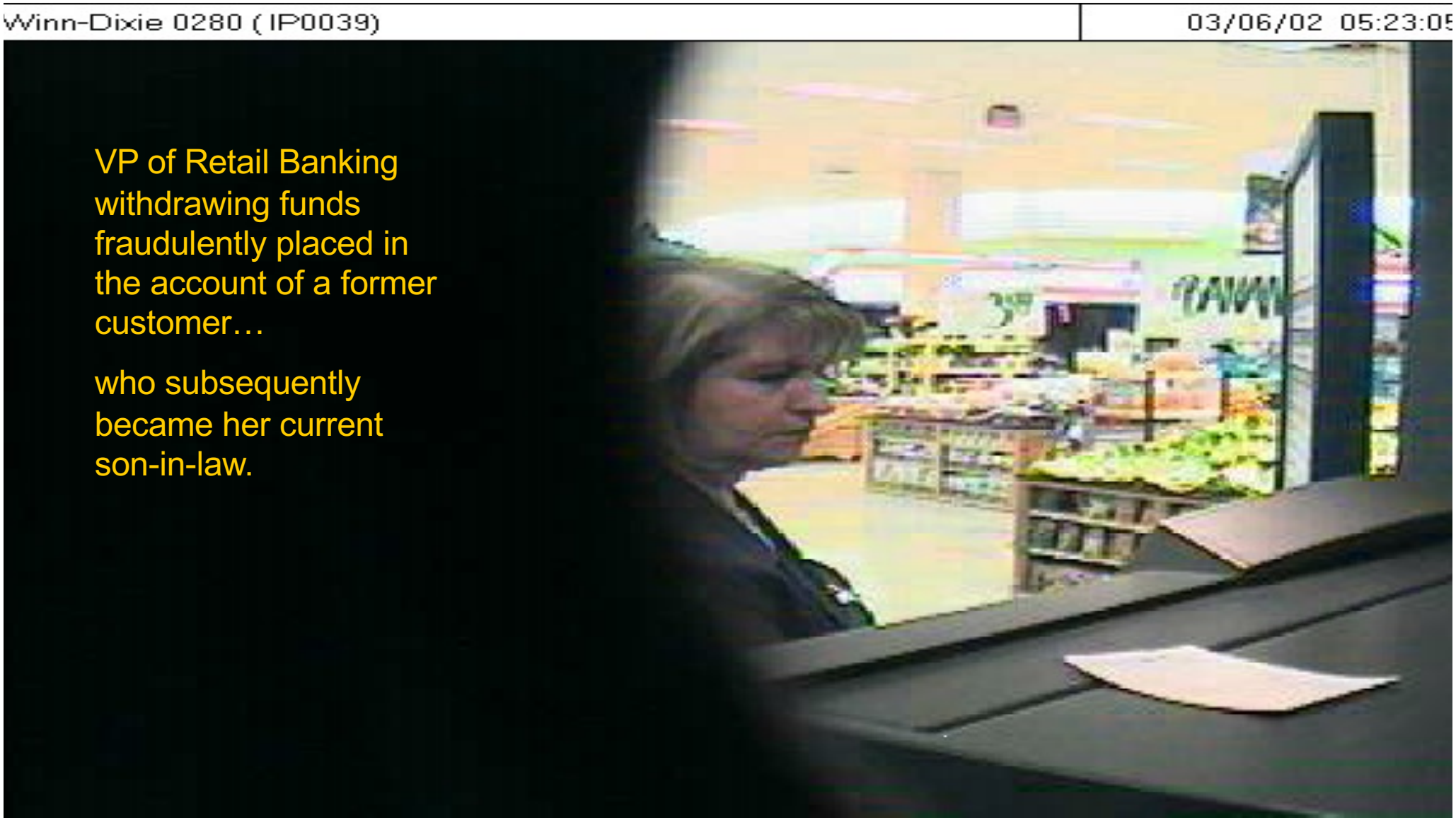
- Internal fraud occurs when a director, an employee, a former employee, or a third party engaged by the bank commits fraud, colludes to commit fraud, or otherwise enables or contributes to fraud.
- External fraud is committed by a person or entity that is not a bank employee, a former employee, or a third party engaged by the bank. (1)
  - **First-party fraud occurs when an external party, including a bank customer, commits fraud against the bank. Providing false information on a loan application for example. (1)**
  - **Victim fraud occurs when a bank customer or client is the victim of an intentional fraudulent act. (1)**
  - You may hear fraud types described as First, Second and Third-Party fraud – Credit Bureaus, Payment companies
    - First-party – Same as above, a person knowingly gives false financial information or misrepresents their identity for financial gain
    - Second-party – Friendly fraud, gives identity information to a friend, family member or acquaintance to commit a fraud
    - Third-Party – Fraud committed against a financial institution or merchant by an unrelated and/or unknown third party

(1) From OCC Bulletin 2019-37|July 24, 2019

Fraud Examples

Internal Frauds

- Fictitious loans/renewals, payment lapping & suicide
  - Segregation of Duties
  - No Whistleblower process
- Trusted employee serving the Bank's elderly customers
  - Segregation of Duties
  - No Whistleblower process
- The ever-increasing vault balance
  - Segregation of Duties
  - Poor Audits
- And one of my favorites – Return Items, Fed Reconcilement, ATMs & Son-in-law's Closed Account
  - Collusion between two officers and an employee


Winn-Dixie 0280 (IP0039)
03/06/02 05:23:05
VP of Retail Banking withdrawing funds fraudulently placed in the account of a former customer…
who subsequently became her current son-in-law.

External Frauds

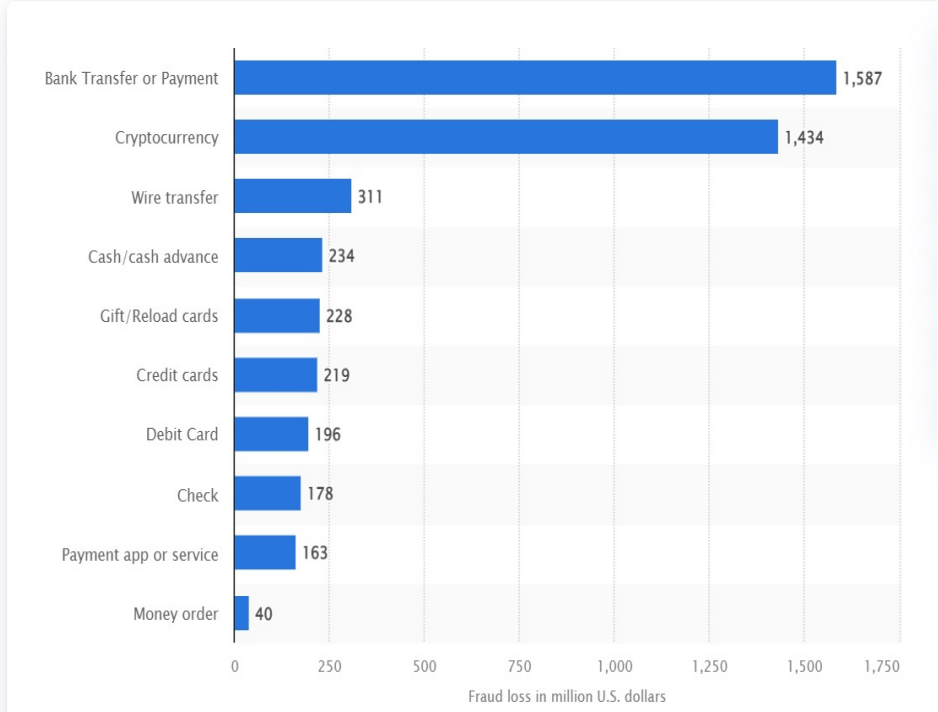
- Man-in-the-middle ACH fraud - $600,000 Hospital Loss
  - Failed to follow authentication procedure
- Loan fraud – $14 million
  - Bribed Loan officers (Trips to Europe)
  - Land flips (Appraisers colluded)
  - Segregation of duties controls poor (Weak Credit Admin)

Current Fraud Issues

- Alloy (ID Software) polled more than 250 compliance, fraud and risk decision-makers at U.S. financial institutions ranging from start-up fintech companies to enterprise banks
  - 91% of said fraud increased year-over-year since 2021 – Includes pandemic relief program frauds. Also includes data breaches, an increase in stolen mail with checks and sophisticated approaches to victimize bank clients through email, phone and text schemes.
  - 70% of respondents lost over $500K in the last twelve months, and 27% of respondents lost over $1M to fraud last year.
- Recent Lexis-Nexis survey found that new account creation accounted for 36% of fraud losses among U.S. banks in November 2022 (fictitious accounts, stolen identities, etc.).
- Fraud targeting mobile channel transactions. 96% of banks responding indicated this fraud type increased in 2022. Includes Identity theft from phishing and social engineering. Frauds like these particularly hitting Zelle. Many banks do not reimburse these since customer "authorized" the transaction. (Example, deposit on rental home scam. Everything from concert tickets to puppies). CFPB Guidelines now say banks must reimburse customers for losses on transfers that were "initiated by a person other than the consumer without actual authority to initiate the transfer
- Check Fraud Up 106% according to Actimize. Reports of check fraud filed by banks nearly doubled to 680,000, from 350,000 in 2021, according to FinCEN.
- Every $1 lost to fraud now costs $4.36 in related expenses such as legal fees and recovery, according to LexisNexis Risk.

Fraud Losses in US in 2022 –

Data is never complete, little data on internal frauds, Banks don't like to disclose. Numbers generally focused for a reason.



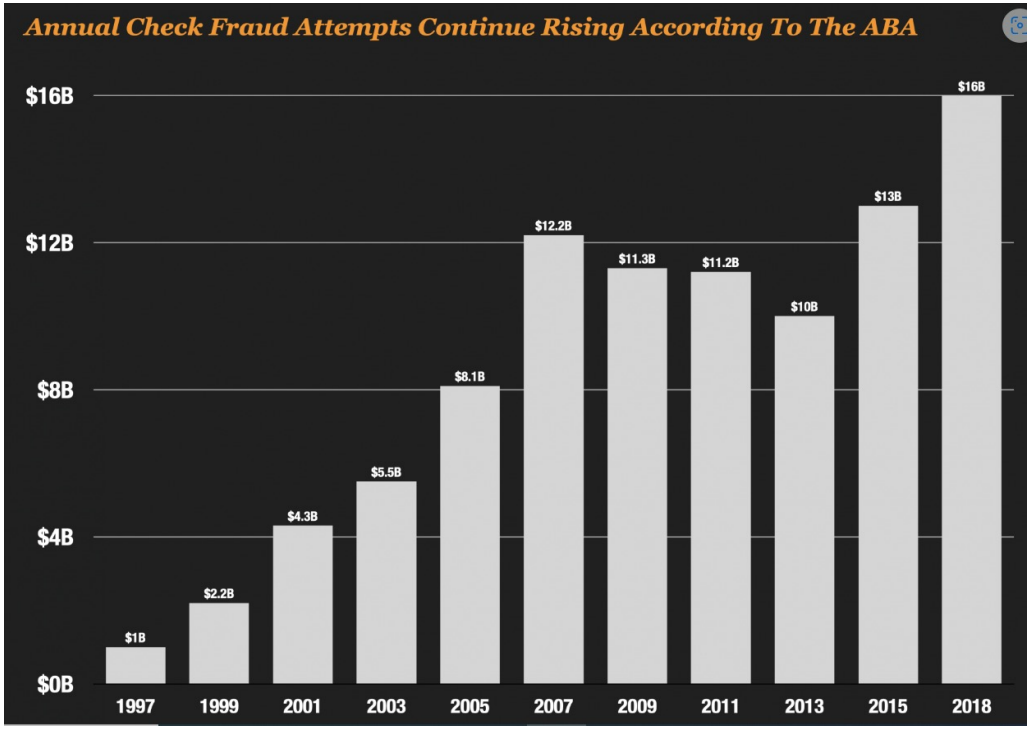


Chart and information from Statista and ABA

Fraud Risk Management Strategy

OCC Bulletin 2019-37, July 24, 2019 - Operational Risk: Fraud Risk Management Principles.

Five Key Areas:

- Assessment
- Governance
- Prevention
- Fraud risk detection
- Monitoring and reporting

Fraud Risk Assessment

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. (1)

- Risk Assessments using stock risks
  - Good approach
  - Applicable to both internal and external fraud
- Interviews with employees, understand how they do their job, they know where the vulnerabilities are
  - Think like a criminal
  - Better approach
- External fraud – Scenario test the processes, products, services, systems for fraud types you are aware of and learn of from other Bank's experience/losses

(1) From OCC Bulletin 2019-37|July 24, 2019

Fraud Risk Governance

A bank should have sound corporate governance practices that instill a corporate culture of ethical standards and promote employee accountability. A solid fraud management strategy solution will likely include: [1]

- A clear strategy for upper management and a fraud risk manager to educate and enforce requirements
- Delegated responsibilities with specific role descriptions
- Whistleblower and reporting procedures
- Quality assurance and internal audit measures
- Documented investigation process and process for corrective actions
- Fraud awareness training, techniques and tools
- Research and analysis of market fraud prevention and mitigation technologies

Policies and practices should be documented, shared, and easily accessible to employees.

The best strategy for effective governance is to assign one designated leader for the entire fraud risk management program.

- All communications run through this person or team.
- This group will also be in charge of fraud training, monitoring, and remediation.

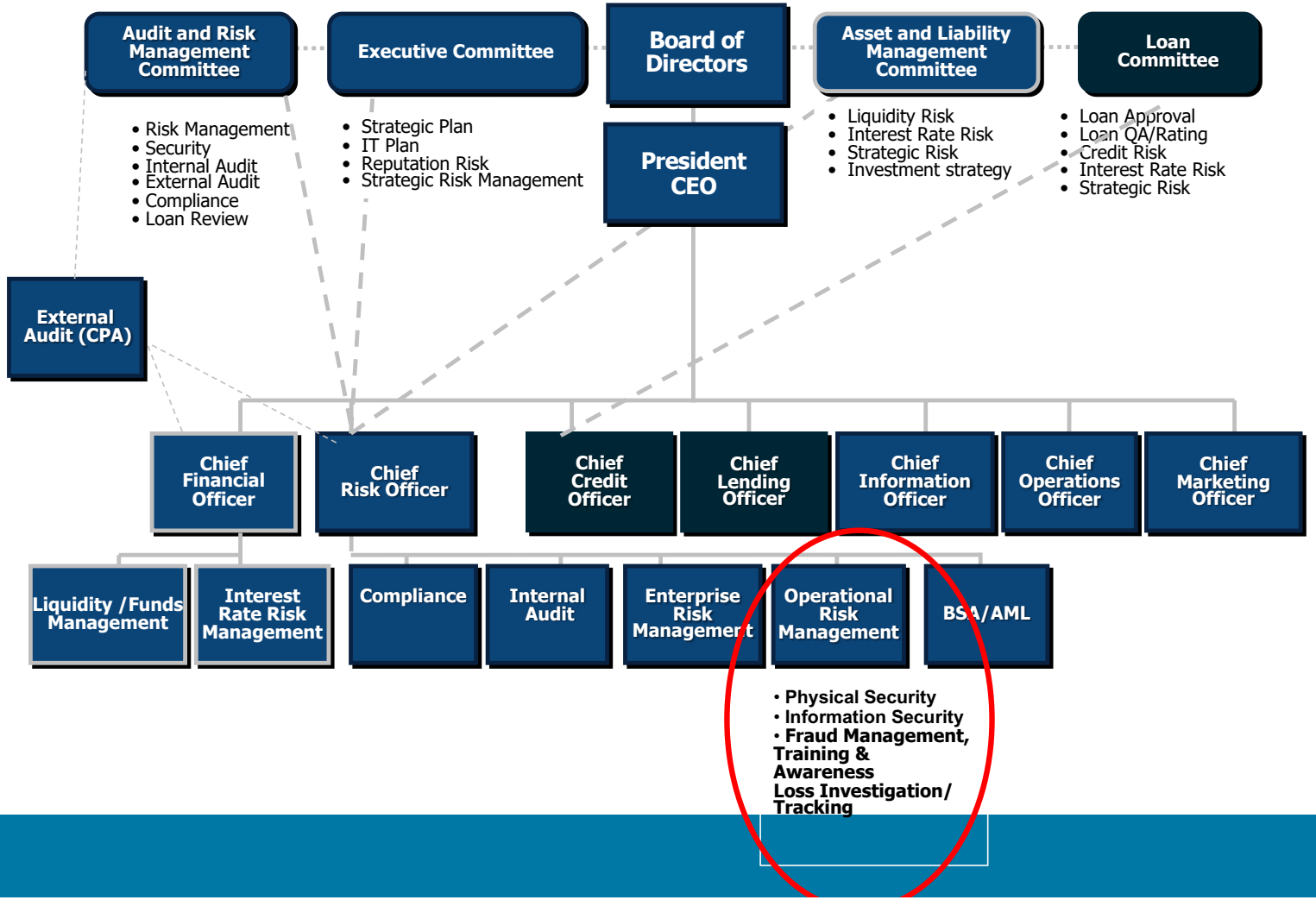
[1] From OCC Bulletin 2019-37|July 24, 2019

Fraud Management Organization

Organizational Alternatives:

- Financial Crimes Unit, combined with BSA/AML
  - Leverages BSA and fraud technology systems
- Operational Risk Manager
- Separate Security Function

Governance, Risk & Compliance Structure



Fraud Prevention

Bank should deploy a combination of preventive controls and detective controls.

Detective controls important because even with strong governance and oversight, collusion or circumvention of internal controls can allow fraud to occur.

Preventive controls are designed to deter fraud or minimize its likelihood and include:

- Policies and processes (e.g., ethics policies, code of conduct, identity theft program, and elder abuse policies)
- **Fraud risk management training and anti-fraud awareness** programs for board, senior management, staff, and third parties
- 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. Include Fraud Dept when new products are being designed.
- Customer identification program procedures, customer due diligence processes, and beneficial ownership identification and verification
- 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**
- **Job breaks, such as mandatory consecutive two-week vacations or rotation of duties**
- **Multi-layer and Multi-factor authentication**
- **Real-time transaction analysis and behavioral analytics (Limits**

Fraud Risk Detection

Detective controls are designed to identify and respond to fraud after it has occurred. 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
- Monitoring and analysis of Bank Secrecy Act report filings by the bank and its affiliates
- Ethics and **whistleblower reporting channels or hotlines (Critical, must be anonymous)**
- Exit interviews for departing employees
- Software and technology tools, developed internally or purchased from a third party, can assist with anti-fraud efforts. Bank's might deploy technology solutions that:
  - Detect anomalies (violations of transaction or total limits) and prevent potential fraudulent transactions or activities (Positive Pay for checks, Signature Image Validation software)
  - Monitor transactions and behaviors (Analyze debits and credits to identify suspicious items, such as duplicate check numbers and out-of-range check numbers and unusual amounts)
  - Monitor networks for intrusions or malware
  - Manage patching of systems

Fraud Monitoring & Reporting

Board and Management should receive regular reporting on the bank's fraud risk assessment, resulting exposure to fraud risk, and associated losses

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

- **Incidents and losses 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

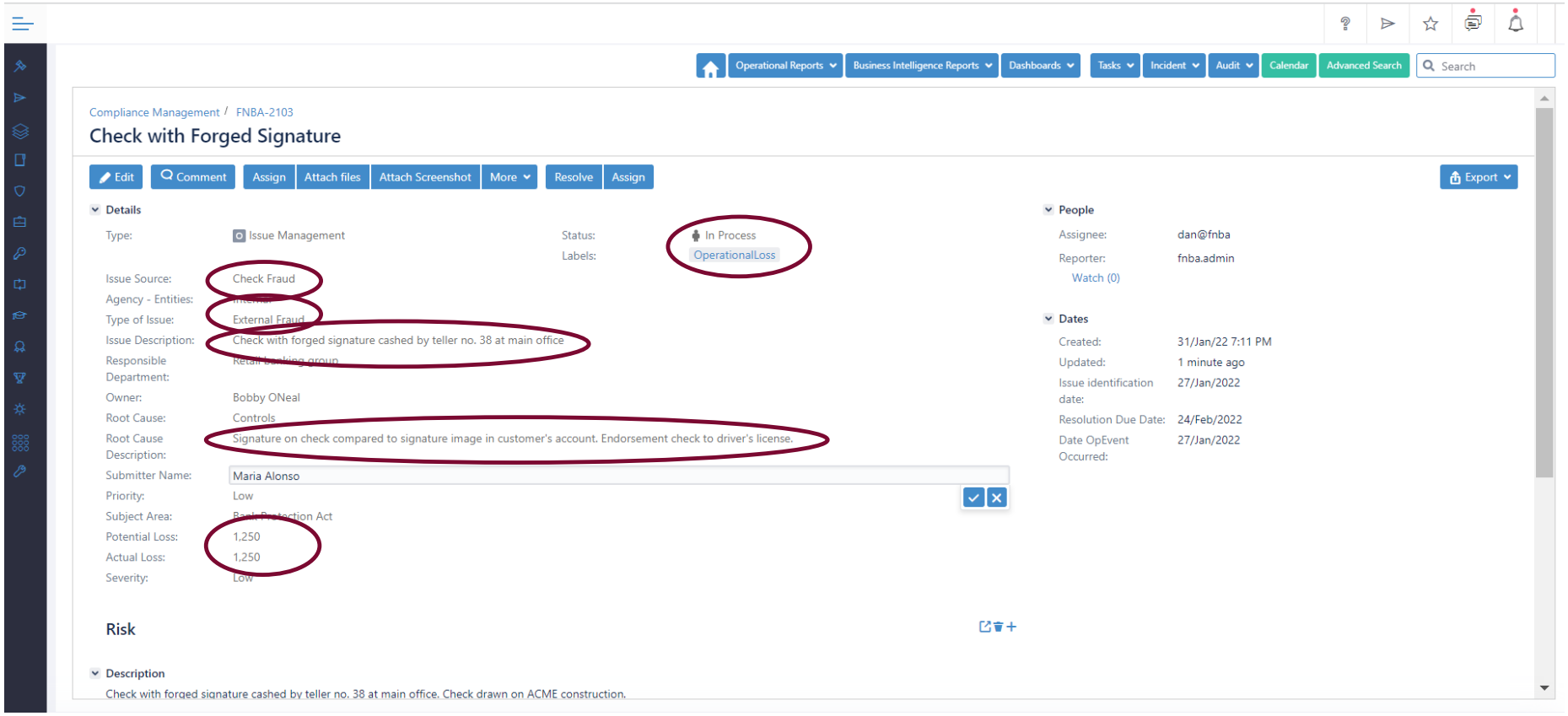
Trend analysis of data such as

- **Number and dollar of fraud investigations**
- Customer complaints
- Suspicious Activity Report [SAR] filings)

Fraud Loss Data

- Banks need to track fraud losses better
- Too decentralized, descriptions inconsistent
- Charging them to various G/L accounts with vague descriptions is not adequate
- Need a system to track:
  - Type of fraud
  - Amount
  - Root cause
  - Remediation efforts
  - Recovery efforts

Fraud Tracking



Fraud Information Sources

Fraud Risk Information Sharing

- According to the OCC, Banks can share fraud information under section 314(b) of the USA PATRIOT Act.
- 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 issued guidance that, if section 314(b) participants suspect transactions may involve proceeds of specified unlawful activities, such as fraud, under the money laundering statutes, information related to such transactions can be shared under the protection of the section 314(b) safe harbor.

Fraud Prevention - American Bankers Association (aba.com)

- https://www.aba.com/banking-topics/risk-management/fraud
- https://www.aba.com/training-events/online-training/the-2023-fraud-landscape-mid-year-update

Association of Certified Fraud Examiners

- https://www.acfe.com/fraud-resources

360factors™

SPEAKER BIOGRAPHY

Professional Biography

Ken Proctor

CPA, CERP, CBA

Director

Ken is a Director of Sales and Consulting at 360 factors. He is a Certified Public Accountant, Certified Bank Auditor and Certified Enterprise Risk Professional. During his 48-year professional banking and consulting career, Ken has served as an internal consultant with a major regional bank, held responsible management positions in the auditing departments of two southeastern regional commercial banks.

Ken has extensive experience as a risk manager, project manager, auditor and strategic planner for banks, credit unions, credit card and mortgage companies in the U.S., U.K., Central America, South America and Southeast Asia ranging in asset size from $200 million to $155 billion. He has performed over 400 risk assessments of financial institutions for insurers at Lloyds of London, Swiss Re, Munich Re, Chubb, AIG and others in the US, Latin America and Southeast Asia.

Ken is a frequent speaker for financial institution industry conferences and seminars, including those sponsored by the American Bankers Association, Bank Administration Institute, Financial Managers Society, Federal Home Loan Bank Board, FDIC, and the National Association of Federal Credit Unions. In addition, he has delivered workshops and presentations on risk management, technology risk and other topics for numerous State and Community Banking Associations, for technology vendors, including FISERV and FIS and international banking associations, including the Federation of Latin American Banks (FELABAN), Central Bank of Paraguay and ASOBANCARIA, the Banking Association of Colombia and Bureau International Informacion y Negocios in Argentina.

Ken served as an instructor on risk management at the LSU Graduate School of Banking (15 years) and is currently a member of the faculty of SMU's Southwest Graduate School of Banking at SMU (9 years). He also served as an instructor on risk management and other topics for the LSU sponsored Professional Masters of Banking program and on retail banking and lending topics for Bank Administration Institute Graduate School of Retail Banking.

Kenneth W. Proctor, Director

Kenneth.proctor@360factors.com

Phone: Office (512) 842-7481, ext. 129

(Cell) 603-801-9722