PROGRAM MATERIALS
Program #3596
June 25, 2025

Fraud Program: Designing, Monitoring and Updating Your Fraud Program

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Fraud: Creating and maintaining a fraud program

Speaker: Justin Muscolino,
JTM Compliance Training

JTM Compliance TRAINING

Justin Muscolino

Justin brings over 20 years of wide-arranging experience in compliance training and regulations. He previously led the compliance training function for JPMorgan Chase Macquarie Group, UBS, Bank of China, and GRC Solutions. Justin also runs his own compliance training company focusing on US & International regulations providing real-life training.

Justin also worked for FINRA, a US regulator, where he created Examiner University to train examiners on how to perform their function. He also serves as an advisor for the Global Compliance Institute (GCI) and instructs at the Barret School of Business and various compliance training providers.

JTM Compliance
TRAINING

Agenda

- Overview & Background
- Preventing Fraud
- A Fraud program
- The different types of Fraud
- Regulatory implications
- Takeaways

Agenda

- Introduction to Fraud Risk Management
- Current Fraud environment
- Creating and maintaining a fraud program
- How to be prepared and handle to incidents
- Tips and other thoughts

JTM Compliance
TRAINING

Introduction to Fraud Risk Management

- Banks play a vital role in identifying and preventing fraud.
- Banks and particularly Compliance Officers, need to ensure that their controls are effective to protect their organizations and customers from fraud.
- In fraud risk management, there are basic principles and recommendations to follow in fraud awareness and having internal controls that provide solutions that should be tailored based on the risk of the bank.

JTM Compliance TRAINING

Introduction to Fraud Risk Management

- As fraud schemes increase in quantity and sophistication, banks are challenged with remaining steadfast in their response to protecting their reputations and assets, as well as those of their customers.
- Banks benefit from strong relationships with their customers built through consistent interaction and community engagement.
- This affords bank a heightened ability to recognize out-of-pattern transactions and educate staff and customers on fraud awareness.

Introduction to Fraud Risk Management

- Bank fraud is a federal crime that occurs when people use illegal means to obtain money or assets from a bank or related financial institution.
- It can involve scenarios where a person pretends to be a bank for the purpose of getting a person's deposits or investments.
- Although it is impossible to identify and prevent all attempted fraud, successful fraud risk management starts with awareness and education regarding the fraud risks for your bank employees and customers.

Stats back it up!

The top three categories of reports for each of these three groups are as follows

Group	Categories	# of Reports	% of Group
Fraud	Imposter Scams	854K	33%
	Online Shopping and Negative Review	368K	14%
	Prizes, Sweepstakes, and Lotteries	157K	6%
Identity Theft	Credit Card Fraud, including new and existing accounts	416K	40%
	Other Identity Theft	261K	25%
	Loan or Lease	150K	14%
Other	Credit Bureaus, Information Furnishers, and Report Users	712K	39%
	Banks and Lenders	230K	13%
	Auto-Related	178K	10%

Published Reports & Assessments

- Nasdaq's 2024 Global Financial Crime Report revealed that fraud scams and bank fraud schemes resulted in $485.6 billion in losses globally last year.
  - In the Americas alone, payments fraud accounted for $102.6 billion of those losses.
- Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing
  - The reports detail recent, significant updates to the U.S. anti-money laundering/counter-financing of terrorism framework and explain changes to the illicit finance risk environment.
  - These include the ongoing fentanyl crisis, foreign and domestic terrorist attacks and related financing, increased potency of ransomware attacks, the growth of professional money laundering, and continued digitization of payments and financial services.

Recent Enforcement Actions

- Three individuals sentenced for 3.5-million-dollar COVID-19 relief fraud scheme for fraudulently obtaining and misusing Paycheck Protection Program (PPP) loans that the U.S. Small Business Administration guaranteed under the Coronavirus Aid, Relief, and Economic Security (CARES) Act in connection with their involvement in a COVID-19 fraud ring.
- Counterfeit Check Scheme: Eight defendants were sentenced for their role in an elaborate counterfeit check cashing scheme. The ringleader deposited counterfeit checks into various banks. The checks were often deposited via ATMs. The scheme was discovered when the vice president of Southwest Georgia Bank (SWGB) reported fraudulent checks being deposited. The investigation revealed that co-defendants opened or used existing bank accounts to deposit these fraudulent checks, resulting in a fraud loss between $40,000 and $95,0001.
- Zelle Payment Scams: An investigation led by U.S. Senator Warren found that in 2021 and the first half of 2022, four banks had 192,878 cases worth $213.8 million where customers claimed they'd been tricked into making Zelle payments. Banks reimbursed customers in only 3,500 of those cases. PPP Loan Recipient Pleaded Guilty to Bank Fraud.

The Mind of a Fraudster: Fraud Triangle

- Pressure: Financial difficulties, personal problems, or a desire for a lavish lifestyle can create pressure on individuals. They may feel compelled to commit fraud as a means of addressing these issues. Financial pressure is a common motivator, as individuals may be facing debts, high expenses, or other financial challenges.
- Opportunity: Fraudsters require an opportunity to exploit weaknesses in a system or process. This could involve having access to financial systems, weaknesses in internal controls, or exploiting vulnerabilities in a company's processes. The presence of opportunities increases the likelihood that an individual will act on their motivations.
- Rationalization: Fraudsters often justify their actions to themselves through rationalization. They might convince themselves that their actions are necessary or that they are somehow entitled to commit fraud. Rationalization is a psychological mechanism that helps individuals reconcile their fraudulent behavior with their personal values.

Types of Fraudulent Acts

- Bank Impersonation
- Stolen Checks
- Forgery
- Fraudulent loans
- Internet Fraud
- Identity theft
- Friendly fraud
- Affiliate fraud
- Accounting fraud
- Remotely created check fraud
- Duplication or skimming of card information
- Empty ATM envelope deposits

Prevention of Fraud

- All employees have a duty to guard against fraud. Employees are expected to identify processes and procedures that may be vulnerable to fraud and to draw such instances to the attention of management in their division.
- Once fraud is detected, Heads of departments are responsible for taking appropriate corrective action to ensure adequate controls are put in place to prevent reoccurrence of improper activity.
- Management has a responsibility to be familiar with and alert to the types of fraud that might occur in their area and to put in place effective controls to avoid such occurrences.

5 Principles of Effective Fraud Risk Management

1. Fraud Risk Governance: Oversight from Board, Management, and designated employees.
2. Fraud Risk Assessment: The foundation for the prevention and detection of fraud is a structured risk assessment that addresses the actual risks faced by the organization as determined by its purpose, industry (products or services), complexity, scale, and exposure to network risks.
3. Fraud Prevention: Culture of fraud awareness, understanding policies and procedures, a safe harbor for whistleblowers, and communication about the importance of fraud prevention
4. Fraud Detection: Controls, monitoring, and reporting promote faster detection of fraud
5. Monitoring and Reporting: Responsibilities and processes to ensure that timely information is reported to someone who can address a problem

Creating and maintaining a Fraud Prevention program

- Developing a robust fraud prevention program in the finance sector is crucial for safeguarding against misconduct.
- A fraud program should take into account:
  - Assess the risk
  - Segregation of duties
  - Fraud Awareness Training
  - Implement Controls
  - Having a culture of compliance

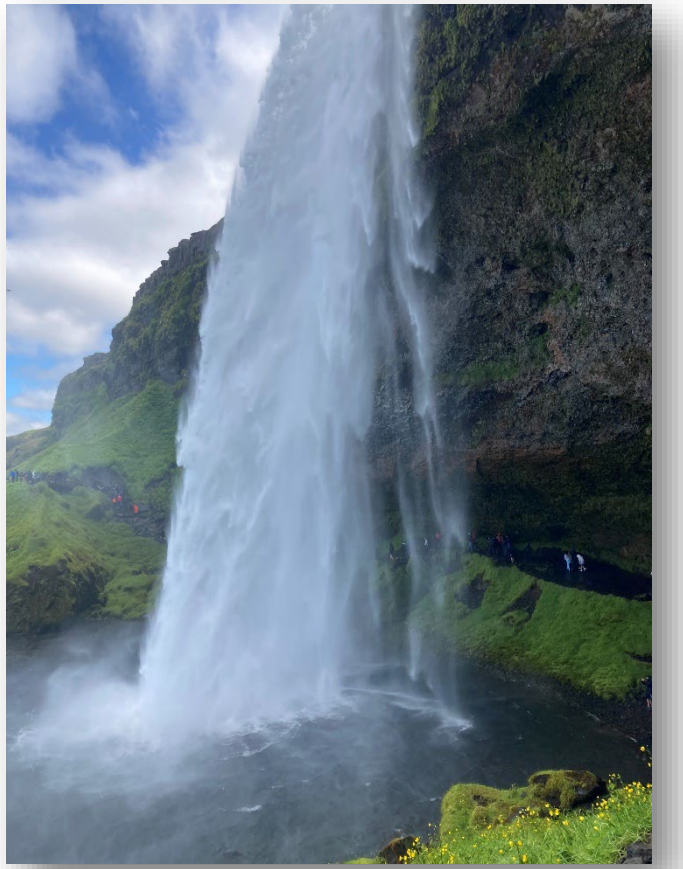
JTM Compliance TRAINING

Creating and maintaining a Fraud Prevention program

- The ideal program will protect a company from itself should:
  - setting the principled “tone at the top”;
  - developing a code of conduct and a confirmation process
  - hiring and promoting appropriate employees
  - identifying and measuring fraud risks
  - implementing and monitoring internal controls

Internal Procedures and Controls

- Establish fraud prevention best practices and responsibilities
- Educate personnel regularly on the importance of safeguarding sensitive information, following established procedures and preventing fraud losses
- Ensure your staff understands they have the most important role in preventing fraud losses
- Refresh training regularly
- Establish clear division of duties and access
- Update signing authority
- Protect your workstations
- Prevent malware infection
- Safeguard your communications and confidential data



JTM Compliance
TRAINING

Build your Fraud Program

- After conducting a risk assessment, we can use the analysis and data to build our fraud program.
  - Goal: To develop a plan to detect and respond quickly to all types of fraud incidents.
  - Implement real-time monitoring, alerts, and automated responses to suspicious activities.
  - Establish Clear Policies and Procedures: Develop clear and concise fraud policies and procedures tailored to your organization's unique risks and requirements. Policies should outline acceptable conduct, reporting mechanisms, and consequences for fraudulent behavior
  - Implement internal controls: Internal controls play a crucial role in minimizing fraud risks. Segregation of duties, access controls, and authorization mechanisms are essential components of a robust control framework.

Ongoing Maintenance and upkeep

- Real-time Monitoring: Implement real-time monitoring of transactions and account activities to quickly identify and respond to suspicious behavior.
- Set up alerts for unusual patterns or deviations from normal customer behavior.
- Customer Authentication Protocols: Implement multi-factor authentication (MFA) to ensure that customers are who they claim to be.
  - Regularly update and strengthen authentication protocols.
- Collaboration and Information Sharing: Collaborate with industry peers, law enforcement agencies, and relevant organizations to share information about emerging fraud trends.
- Conduct Regular Fraud Awareness Training: Provide regular fraud awareness training for all employees to recognize potential red flags, fraud indicators, and the importance of reporting suspicions promptly.

What to Do After Fraud Is Identified?

- Even the best fraud risk management program cannot stop all fraud.
- Banks have the advantage of knowing their customers, which helps to identify unusual activity, and the likelihood of recovery is higher if the fraud is identified quickly, and the recovery steps are followed.
- Recovery steps will vary depending on the type of transaction. It is important to understand the types of fraud that could occur at your institution.
- Educating bank staff on these options will improve response time and higher recovery rates.
- The plan should include protocols for investigation, involving relevant internal and external parties, and complying with legal and regulatory requirements.

What to Do After Fraud Is Identified?

- Prepare a response plan for handling suspected fraud incidents.
- Swift action is crucial to mitigate potential damages and prevent recurrence.
- Banks should develop a structure for an effective investigation that will help identify the root cause of the fraud and corrective actions.
- The investigative process provides for a review of a fraudulent incident, communication the results, remediation of the incident and determining internal control weaknesses.
- Fraud attempts against a bank or its customers, even if unsuccessful, are criminal acts. Determine if a SAR filing is needed.
- A bank's incident response process should outline options to recover funds that left the institution. This includes losses experienced by the bank as well as incidents in which a customer was targeted that may result in bank exposure.

Incident Response Plan

- An incident response plan outlines the steps an organization should take in the event of a security incident.
- Incident Response Plan for Bank Fraud Prevention
  - Preparation: Establish an incident response team with defined roles and responsibilities
  - Detection and Identification: Implement monitoring tools and techniques to detect potential fraud incidents. Train staff to recognize and report suspicious activities
  - Containment: Isolate affected systems or accounts to prevent further compromise. Implement temporary fixes and controls to limit the impact of the incident
  - Recovery: Restore affected systems to normal operation. Validate that all security controls are functioning as expected.

Incident Response Plan

- Communication: Establish a communication plan for internal and external stakeholders. Notify law enforcement, regulatory bodies, and affected customers as necessary.
- Documentation: Maintain detailed records of the incident, including timelines, actions taken, and lessons learned. Document any changes made to systems or procedures as a result of the incident. Use the information gathered for continuous improvement of the incident response plan.
- Post-Incident Analysis: Conduct a thorough analysis of the incident, focusing on the effectiveness of the response. Review and update incident response playbooks and procedures based on lessons learned. Share insights and findings with relevant stakeholders for ongoing education and improvement.
- Legal and Compliance Considerations: Ensure compliance with relevant regulations and coordinate with regulators.
- Training and Awareness: Conduct regular training sessions for incident response team members and others involved.

Regulatory

- Any type of fraud subjects the perpetrator to serious penalties, the severity of which often depend on the monetary amount of the fraud, whether the fraud was committed against a protected class of person, and whether the crime is classified as a state or federal crime.
- The proof requirements for criminal fraud charges in the United States are essentially the same as the requirements for other crimes: guilt must be proved beyond a reasonable doubt.
- Whoever knowingly executes, or attempts to execute, a scheme or artifice
  - to defraud a financial institution; or
  - to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises;

JTM Compliance TRAINING

THANK YOU!

Contact Information:
JTM Compliance Training
Justinmuscolino@gmail.com

JTM Compliance
TRAINING