



MANAGING FRAUD RISK



Teresa D. Thamer, CPA, CFE
Brenau University

Overview

- I. Understanding what Fraud is and is not
- II. Identifying and assessing key fraud risk areas
- III. Developing a Comprehensive Fraud Policy

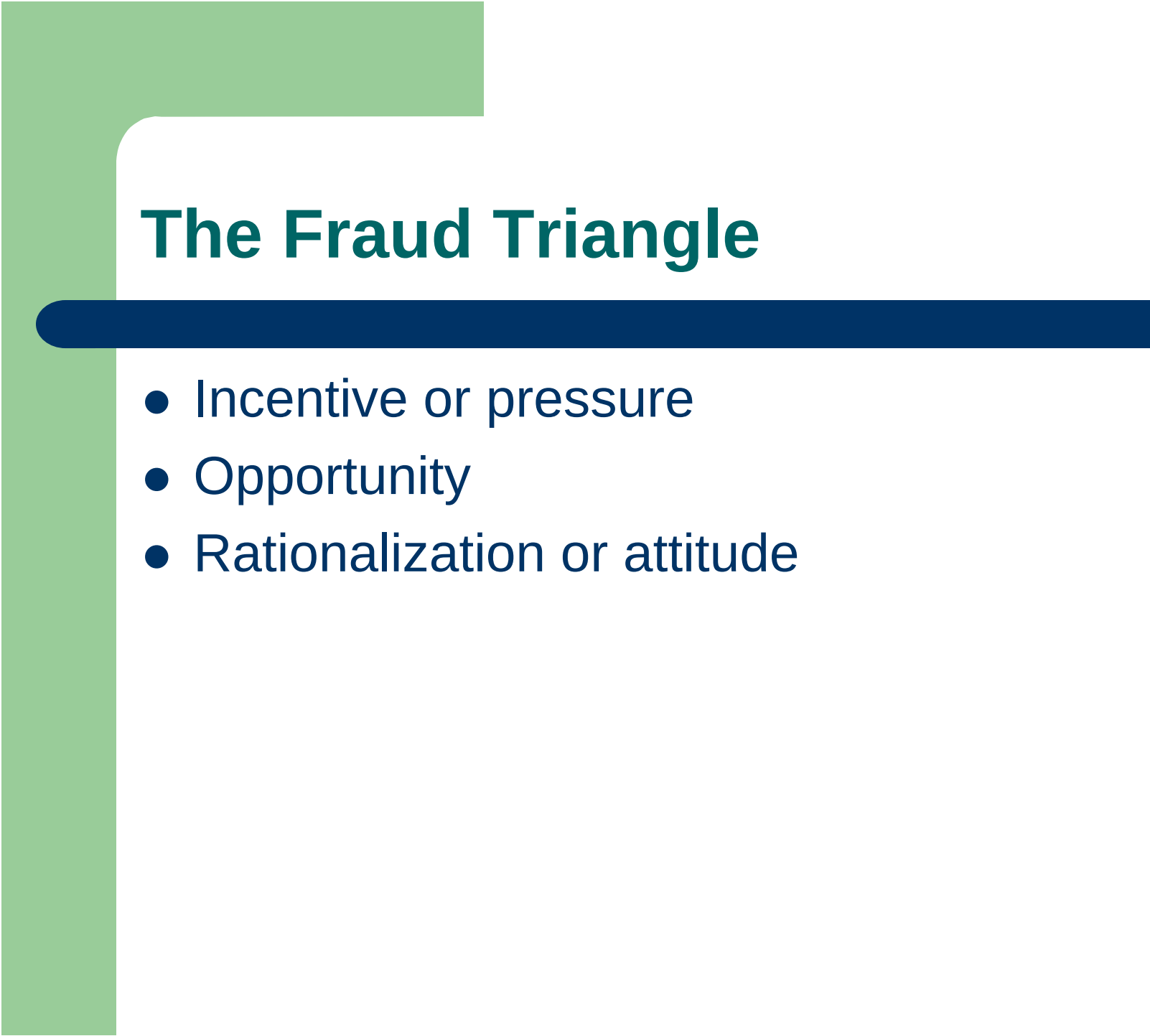
I. Understanding what Fraud is and is not

- Definition of Fraud
- The Fraud Triangle
- The “People Factor”

Definition of Fraud

- “Trickery or deceit aimed at obtaining an unfair advantage”
- SEC Rule 10b-5
- False statements or acts, with INTENT to deceive a victim, resulting in damages to the victim
- Broadly includes wrongdoing, misconduct and corruption

The Fraud Triangle



- Incentive or pressure
- Opportunity
- Rationalization or attitude

Incentive or Pressure

- Management or other employees
- Examples – personal or business
- “Good to Bad” – relative honesty of people
- Outcome: Fraud Risks increase
- Not a reliable predictor of who is likely to commit fraud

Opportunity

- Absence of controls
- Ineffective controls
- Management's ability to override controls
- This is the only variable that can be managed

Rationalization or Attitude

- Individual character
- Set of ethical values
- A “temporary” situation
- Justification of action
- Not a reliable predictor of who is likely to commit fraud

Keeping People Honest

- Personal beliefs, values, ethics
- Attitudes about right and wrong and fairness
- Cultural standards, laws and customs
- Fear of punishment
- “Tone at the Top”
- Lack of opportunity

II. Identifying and Assessing Key Fraud Risk Areas

- Basic realities
- An Antifraud Environment
- A Fraud Risk Inventory
 - Types of Fraud
 - Prevention and Detection

Basic Realities

- Some types of fraud cannot be prevented
- Every fraud is a unique set of circumstances
- Fraud is “hard work” for the fraudster

An Antifraud Environment

- Aggressive prevention
- Early detection
- Leadership in organization
- A positive work environment
- Penalties
- A Reporting Process

Prevention and Detection

- Strong internal controls are essential
- Controls for prevention and detection are related and both are necessary
- Policies and procedures

“Tone at the Top”

- Examples of officers, executives and top management
- Workplace provides fair and equal treatment
- Zero tolerance for wrongdoing
- Written policies – comprehensive Code of Conduct

Code of Conduct includes:

- Compliance with laws and regulations
- Conflicts of interest
- Workplace behavior
- Employee's external activities
- Third party relationships
- Specific activities in specific areas
- Protection of assets and records of the organization

A Positive Work Environment

- Focuses on the rationalization or attitude side of the Fraud Triangle
- Identify factors which would detract from a positive work environment
- Factors may increase the risk of fraud
- Consider unsafe or hostile working conditions specific to the organization or industry

Penalties

- Belief that there are penalties
- There is a fair process to review suspected misconduct
- The process functions in a consistent manner for everyone
- Works within a policy established by the company

A Reporting Process

- A method to safely report concerns and suspicions
- Anonymous hotlines or similar ways to report
- Supported by a Policy applicable to all levels
- May be part of the Code of Conduct or part of a separate Fraud Policy

Fraud Risk Inventory

- Step 1 – Identify Specific Fraud Risks
- Step 2 – Develop Prevention Controls
- Step 3 – Training Employees in Detection

Step 1 – Identify Fraud Risks

“What could go wrong?”

- Use of specialists in controls
- Brainstorming
- Develop for each department
- Employees should participate
- Consider details and technology

Step 2 – Develop Prevention Controls

“What are we doing formally or informally to prevent the identified fraud risk?”

- Analyze each step in the procedure
- Brainstorm how fraud could occur and how to prevent that
- Document the procedure, policy or required behavior

Step 3 – Train Employees

- People must know the “hard controls” covering access, documentation, approval and reconciliation
- People must also be the “soft controls” that support a strong internal control environment
- Fraud awareness training is the key to early detection and starts with the first two steps

Fraud Awareness Training

- General knowledge of fraud risks facing the organization
- Specific examples of what can happen
- What it looks like when it happens (symptoms)
- Specific actions that can prevent fraud
- Specific actions that can detect fraud

Types of Organizational Fraud

Management Fraud -

Financial Statement Fraud:

- Revenue and Inventory-related Financial Statement Fraud
- Liability, Asset and Inadequate Disclosure Fraud

Misappropriation of Assets:

- Larceny
- Skimming
- Theft
- Corruption

Other Types of Fraud

- Consumer Fraud
- Bankruptcy, Divorce and Tax Fraud
- Money Laundering
- E-commerce

Management Fraud

- Misstated Financial Statements and “cooking the books”
- Inappropriate executive loans and corporate looting
- Insider trading
- Excessive executive compensation and perks
- Loans and other transactions

Why These Frauds Occur

- Back to the Fraud Triangle
- Other factors:
 - The economy
 - Decay of moral values
 - Misplaced incentives
 - High analysts' expectations
 - High debt levels
 - Focus on accounting rules rather than principles
 - Lack of auditor independence
 - Greed
 - Poor education

Fraud Detection Strategy

1) Think like a thief

- What could go wrong?
- What are indicators?
- Where are the weaknesses?
- How would it be detected?

2) Use Discovery Techniques

- Signs of wrongdoing – yes or no?
- Use of discovery sampling
- Failure of preventive controls
- Use of interviews and inquiries of management and others
- Body language and other signs
- Monitoring for fraud indicators

3) Determine the cause of all fraud indicators

- Investigate all causes, even errors
- Use professional skepticism
- Have a plan for follow-up
- Continue inquiry, use technology as appropriate and call on a fraud specialist if needed

Fraud Prevention

- For every fraud risk identified, develop preventive and detective control steps and behaviors
- Prevention controls should be aimed at each step in the scheme
- Consider “hard” and “soft” controls

Prevention Steps

- 1) Have specific authorization, access and transaction recording procedures (the control environment)
- 2) An accounting system should ensure transactions are valid, authorized, complete, properly valued, recorded & classified, summarized properly and secure from manipulation
- 3) Consider security and access company-wide

III. Developing a Comprehensive Fraud Policy

- What is a Fraud Policy?
- Requires high level sponsorship and a positive introduction
- Outlines communication, policy and responsibilities and procedures concerning fraud

A Comprehensive Fraud Policy

- Is a critical part of an antifraud business environment
- States requirements for all employees with respect to their daily fraud prevention, detection and handling responsibilities
- Should be in writing and acknowledged by the employee
- May require specific training

Positive and High-level Sponsorship

- Part of the “Tone at the Top”
- “We need your help to fight fraud!”
- Training is essential and across the entire organization.
- Training should be specific to the individuals and their duties – *what does fraud look like?*

Policy includes:

- **Goal** is to establish and maintain a business environment of fairness, ethics and honesty.
- **Purpose** of the policy is to communicate the procedures for deterrence and investigation of suspected misconduct and dishonesty and to provide specific instruction re: appropriate action.

Definition of Misconduct and Dishonesty

- Acts which violate the Code of Conduct
- Theft or other misappropriation of assets
- Misstatements or other irregularities in company records
- Wrongdoing
- Forgery or alternation of documents
- Fraud or other unlawful acts
- Any similar acts

Policy and Responsibilities

- It is the responsibility of every employee to immediately report *suspected* misconduct or dishonesty.
- Be specific to whom it should be reported.
- Reprisal against anyone reporting this in good faith, is strictly forbidden.
- Effective professional follow-up is critical.

Follow-Up and Investigation

- Identify who has primary responsibility for all investigations involving the company.
- Identify designated members of the investigative team
- General procedures for follow-up and investigation should insure that suspected individuals are not alerted and that statements that could adversely affect the company, employee or others are avoided.

General Response Action Plan should include:

- Early referral of issues to those authorized to investigate
- A Response Team organized BEFORE there is a need
- A planned response by that team
- Coordination with law enforcement and others
- A planned public response (publicity)
- Consideration of employee morale issues

The Response Team

- Lawyers skilled in criminal matters
- Investigative team (fraud examiners & forensic accountants and investigators)
- Internal auditors
- Information technology and computer forensics experts
- Human resources
- Insurance company personnel

CONCLUSION AND SUMMARY

- Fraud is intentional and harmful
- The “tone at the top” and employee awareness and training are the primary ways to deter fraud
- Prevention and Detection Strategies are required as part of a comprehensive plan to minimize fraud risk
- The development of a Fraud Policy is essential to being adequately prepared before and after fraud is discovered

Resources Available

- AICPA Antifraud & Corporate Responsibility Center (www.aicpa.org)
- SAS No. 99, *Considerations of Fraud in a financial Statement Audit* – Management Antifraud Programs and Controls
- COSO – *Internal Control – Integrated Framework* (www.coso.org)
- ACFE – www.acfe.org
- PCAOB – Auditing Standard 2, *An Audit of Internal Control over Financial Reporting...*