

Internal Fraud Risk Assessment Best Practices

By Tom Holland, CFE



The Threat Within



- Internal fraud is an ongoing concern and by many indications is growing
- There are a number of factors contributing to the increase



The True Cost of Fraud

Losses from fraud are more than just the money that “walks out the door”, other factors to consider include

- Investigation costs
- Other departments involvement
- Business disruption
- Cost of hiring a replacement
- Reputational issues



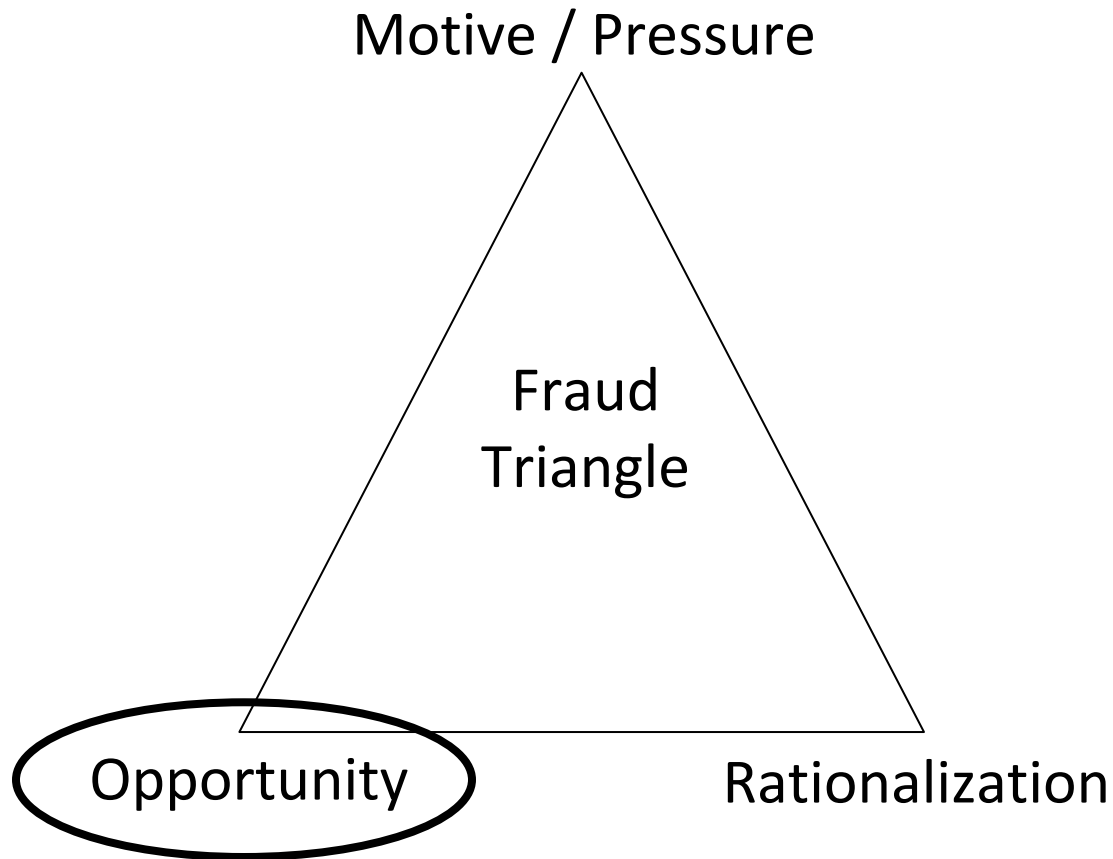
Regulatory Requirements

There are a number federal regulations, depending on the type of company and its businesses, that require organizations to monitor their employees for criminal activity

- Sarbanes-Oxley Act
- Federal Sentencing Guidelines
- Foreign Corrupt Practices Act
- Bank Secrecy Act



Components of Internal Fraud



Purpose of a Fraud Assessment

- Conducting a risk assessment allows you to mitigate associated risk by **understanding the opportunity** for fraud and the **effectiveness of related controls** to prevent and/or detect the unauthorized activity
- A risk assessment should ask the following questions
 - What areas are susceptible and how
 - Who can commit the fraud and how
 - What is the impact
 - What controls are in place, or should be in place



Approach and Participants

- At the enterprise level review
 - Fraud prevention programs
 - Controls related to frauds not unique to a department
- Assess major business and administrative groups separately
- Participants should include
 - Management
 - Internal Audit
 - Compliance
 - Management in tangent businesses
 - Corporate Security
 - Legal
- Timing, annually or as significant changes occur



Enterprise-wide Programs

- Tone from the top
 - Strong and comprehensive code of ethics
 - Strong system of internal controls
- Employee background checks
 - Criminal
 - Previous employment
 - Education
- Channels for reporting suspicious activity
 - Fraud / ethics hotline
 - Intranet, internal phone lines, emails
- Fraud awareness programs



Code of Ethics

- A code of ethics must detail expected behavior in general terms
- An effective code should require
 - Reporting of known or suspected fraudulent activity
 - Cooperation in the investigation process
 - Penalties for failure to cooperate
- Employees should affirm their understanding and compliance upon initial employment and again on an annual basis



Reporting Suspicious Activity

- The Sarbanes – Oxley Act requires publically traded companies to have the ability to receive complaints related to unethical accounting and audit activities
 - An ethics hotline should
 - Be accessible 24 x 7
 - Provide for anonymity, if desired
 - Allow for direct reporting to the Board of Directors, if desired
- Requirements of the Sarbanes- Oxley Act
- Other reporting channels should be made available
 - Reporting channels should be promoted periodically



Fraud Awareness Programs

- Fraud awareness programs should be developed to assist employees, particularly management
 - Understand the signs (i.e. “red flags”) of internal fraud
 - What to do when they identify red flags
- Red flags can be classified into two groups
 - Operational ... examples include
 - Poor internal controls or disregard for internal controls
 - Increasing expenses without a corresponding increase in sales
 - Behavioral ... examples include
 - An employee living beyond their apparent means
 - Change, often dramatic, in an employee’s personality



Automated Fraud Monitoring Programs

- Risk assessments should be utilized to identify need, type, and frequency of internal fraud monitoring programs
- Automated solutions should be considered in departments with large volumes of transactions and high potential for fraud
- An effective software solution should be able to detect unusual transactions and operator behavior
 - Transactional analysis identifies suspicious transactions regardless of who owns the account
 - Behavioral analysis identifies suspicious activity of an individual when compared to pre-defined peer groups such as call center representatives or cashiers



Proactive Reviews

Proactive reviews should be performed in areas where the likelihood of fraud is high and software solutions are not used

- Accounts payable
 - Duplicate payment
 - Multiple payments in the same billing cycle
- Payroll
 - Non-existent (i.e. “ghost”) employees
 - Unusually high salary given the position
- Travel expense
 - Altered or no receipts
 - Receipts from businesses not associated with travel



Investigation Program

The risk assessment should also include a review of your company's internal investigation program particularly if you don't have a dedicated department to perform internal investigation

- Are procedures current
- Are investigation team members familiar with procedures, roles, and responsibilities
- Are contact lists current



Overview of a Crime Insurance Policy: ***“Underwriting and Coverage Details”***

Joe Kacsanek

Chubb Specialty Insurance Manager

Richmond, VA Office



Disclaimer

The views, information and content expressed herein are those of the author[s] and do not necessarily represent the views of any of the insurers of The Chubb Group of Insurance Companies. Chubb did not participate in and takes no position on the nature, quality or accuracy of such content. The information provided should not be relied on as legal advice or a definitive statement of the law in any jurisdiction. For such advice, an applicant, insured, listener or reader should consult their own legal counsel.



Current Crime Insurance Environment

- Marketplace & Capacity
- Increase in Claims Activity
- Increase in Underinsured & Un-Insured Losses
 - Survey Says....32% had a loss over past 5 years
- Evolution of Crime & Cyber Exposures
 - *336,655 Complaints in 2009 (+22.3% over 2008)**
 - *\$559.7 Million in Losses**

*Used with Permission. ©2010. NW3C, Inc. d/b/a the National

White Collar Crime Center. All rights reserved.

Executive Protection Practice



Underwriting the Exposures

Underwriting Considerations

- Class of Business, Annual Revenues, Total Employee Count, Number of Locations
- Policies and Procedures
 - Segregation of Duties
 - Audited Financial Statements
 - Internal Control Audit with Management's Response
- International Exposures, Precious Metals, Cash On Hand
- Prior Loss History
- Policy Structure – Limits and Retentions



Crime Coverage Overview

Typical Insuring Agreements

- Employee Theft / Dishonesty
- Premises
- Transit
- Forgery
- Funds Transfer Fraud
- Computer Fraud
- Money Orders & Counterfeit Currency Fraud
- Credit Card Forgery
- 3rd Party Coverage or Client Coverage
- Expense Coverage



Crime Coverage Overview

Key Policy Definitions

- **Employee** – natural person in regular service of Insured Organization, including D&O's, temp, leased, volunteers
- **Theft** – unlawful taking of money, securities or property to detriment of Insured...
- **Money & Securities, Property**
- **Third Party** – Person other than Employee or Insured



Crime Coverage Overview

Insuring Clauses

Employee Theft / Dishonesty Clause -

- Coverage for **DIRECT LOSS** resulting from Theft or Forgery Committed by an Employee
- Overwhelming majority of all losses stem from employee theft insuring clause
- Loss Scenarios
 - “Winchester Woman admits Church Embezzlement”
 - “Chesterfield Man Faces Embezzlement Charges”



Crime Coverage Overview

Insuring Clauses

Premises Clause-

- resulting from robbery, safe burglary, or unlawful taking of money or securities by a **THIRD PARTY** within or from the **premises**
- Or actual destruction or disappearance of money or securities

Transit Clause-

- resulting from robbery or unlawful taking of money or securities by a **THIRD PARTY** while **in transit**
- Or actual destruction or disappearance of money or securities



Crime Coverage Overview

Insuring Clauses

Forgery Clause-

- resulting from **forgery** or alteration of a financial instrument committed by a **THIRD PARTY**

Funds Transfer Fraud Clause-

- resulting from **funds transfer fraud** committed by a **THIRD PARTY**
- Written, telegraphic, telephone... to a financial institution...without Insured's consent



Crime Coverage Overview

Insuring Clauses

Computer Fraud Clause-

- resulting from **computer fraud** committed by a **THIRD PARTY**
- Unlawful taking of money or securities through unauthorized entry or deletion of data through a computer system

What about damaged or destroyed data or computer programs?



Crime Coverage Overview

Insuring Clauses

Money Order and Counterfeit Currency Clause-

- resulting from **MO & CC Fraud** committed by a **THIRD PARTY**
- Good faith acceptance in exchange for merchandise, money or services

Credit Card Fraud Clause-

- resulting from **Credit Card Fraud** committed by a **THIRD PARTY**
- Resulting from forgery or alteration in connection with...



Crime Coverage Overview

Insuring Clauses

Third Party / Client Clause-

- **Third Party/Client** stemming from theft or forgery committed by an Employee, not in collusion with a Client's employees
- Care, Custody and Control?

Expense Clause-

- Coverage for investigative expenses and computer violation expenses



Crime Coverage Overview

Common Policy Exclusions

- Loss of Trade Secrets or confidential information
- Loss committed by a Partner/Owner
- Indirect Loss, except expense coverage
- Loss sustained following the termination of employee
- Any loss after Insured becomes aware of a prior loss while employed by the Insured
- Knowledge of loss prior to employment – subject to threshold




Crime Coverage Overview

Key Coverage Details

- Loss Sustained vs Loss Discovered
- Subrogation & Right of Recovery
- Prosecution required?
- Policy Aggregate
- ERISA Bond Requirement





Legal Perspective: Conducting the Internal Investigation/Pursuing the Employee

**John S. West, Partner,
White Collar and Government Investigations
Troutman Sanders LLP**



Company Is Alerted To Incident Of Embezzlement Or Other Fraud

- Tip From Management / Employees
- Anonymous Report
- Internal or External Review/Audit
- Other (e.g., Customer, Vendor)

Initial Response After Becoming Aware Of Fraud

- Identify Who Within the Organization Should be Notified
- Identify Who Outside the Organization Should be Notified

Initial Response After Becoming Aware Of Fraud

- Determine Whether Criminal Activity is Ongoing or has Ended
- Make Initial Determination of Number of Employees and/or Third Parties Involved
- Preserve evidence

Planning the Investigation

Fundamental Goals

- Determine what happened
- Determine who was involved in the suspected activity (possible collusion?)
- Determine whether the company is responsible for that activity

Planning the Investigation

- Who within the organization should oversee the investigation?
- Who should conduct the investigation?
- Who should be interviewed immediately?
- Who should gather documents?
- Will Company's computer system or other electronic media be used?

Planning the Investigation

- What timeline should be imposed on the investigation?
- Are there company actions or operations that should be suspended pending the investigation?
- If identity of suspected perpetrator(s) is known:
 - Make decision on whether or not to place suspected employees on leave during conduct of investigation
 - Restrict access of suspected employees to office, records, computer system

Conducting the Investigation

- Conduct interviews and review of documents/data
- Limit discussion regarding suspected activity
- Determine whether facts indicate a possible material effect on the company's financial condition

Conducting the Investigation

- The “Fraud Triangle”
 - Motivation of perpetrator
 - Rationalization of perpetrator
 - Opportunity – How was fraud perpetrated?
- Concealment – How Was the Fraud Concealed?
- Conversion – How Were the Funds Expended?
- Tracing of Assets (“Follow the Money”)
- Recovery
- Reporting of Results

Contacting Law Enforcement

Whether To Do So:

- Company under no obligation (misprision of felony).
- Factors influencing decision:
 - Amount of money involved
 - Number of employees or third parties involved in illegal scheme
 - Whether any government funds or contracts are connected to illegal activity
 - Whether or not there is a risk law enforcement will take possession of company records and length of time before they will complete any investigation

Contacting Law Enforcement

When To Do So:

- Immediately
 - If criminal activity is still ongoing
 - If scope of activity extends beyond primary company (e.g. -kickback scheme involving third party service providers)
 - Threat of ongoing harm or violence
- After Internal Investigation Has Concluded
 - If criminal activity is over
 - If criminal activity is limited to within organization

Private Settlement With Employee

- Complete Internal Investigation Before Presenting Offer of Settlement
 - Initial scheme or impact of fraud is often the tip of the iceberg
- Confront Person Alleged to Have Committed Wrongdoing:
 - Record admissions or response
 - Propose payment obligation with short deadline
 - Do not negotiate amount of payment
 - Prepare settlement and release agreement

Private Settlement With Employee

- Other Considerations:
 - Insurance company may only cover claim if employee is prosecuted
 - If there is a private settlement, employee may perpetrate the same crime again at an unsuspecting new employer

Participation in Prosecution

- Substantial Assistance of Company will be Required
 - Factual development
 - Preparation of documents
 - Testimony of key employees
- Process will be Lengthy
- Company Will Not Control Final Outcome

***“Partnering with your
Insurance Carrier at the time
of loss”***



Loss Notification

“I’ve discovered something, now what?”

- **Contact your Insurance Broker**
- **Understanding your Obligations under the contract**
 - What constitutes KNOWLEDGE or DISCOVERY?
 - What are your NOTICE requirements?
 - Furnishing a proof of loss
- **What to expect from your Insurance Carrier**
 - Explains requirements for an affirmative proof of loss – forward a proof request letter.
 - Discusses any potential coverage issues.



Proof of Loss Process

- **Proof of loss details**
 - Proof of loss due date (timeframe)
 - Discovery, Timeline of the loss, Background information, Structure of business, Organizational chart
 - Documentation or records, spreadsheets outlining theft, receipts, reconciliations, personnel records, checks, etc.
 - Other insurance
 - Police reports or regulatory proceedings
 - Invoices for Investigative Expenses



The Often Forgotten Investigation Objective ...

Identifying the Causative Factors

By Tom Holland, CFE



Investigation Objectives

In general, there are two investigation objectives

- Determining culpability of those named in allegation
- Identifying causative factors that allowed the fraud to occur and/or go undetected



Analysis of Investigation Activity

Analysis of investigation activity should be performed on a regular basis to identify

- Emerging trends
- Systemic issues not readily identified in individual investigations
 - Consider performing as part on the annual internal fraud risk assessment



Questions & Comments

