Case Studies in Occupation Fraud – What went wrong?
A Forensic Accountant’s Perspective

2010 CORRUPTION INDEX
KPMG 2011 ANALYSIS OF GLOBAL PATTERNS OF FRAUD

- Male
- 36 to 45 years old
- Commits fraud against his employer
- Works in finance function or finance-related role
- Holds a senior management position
- Employed by the company for more than 10 years
- Works in collusion with another perpetrator

Exploitation of weaknesses in internal controls by fraudsters increased significantly from 49 percent in 2007 to 74 percent by 2011.

The increased failure to respond to red flags highlights the need for companies not only develop system for identifying red flags, but also acting on them.

Only 23% of the frauds detected were publicly reported
Institute of Financial Operations

- International Accounts Payable Professionals (IAPP), International Accounts Receivable Professionals (IARP), the National Association of Purchasing & Payables (NAPP), and The Association for Work Process Improvement (TAWPI)
- May 15, 2011 - In informal poll of 622 managers, 72% said fraud was on the rise in back office fraud

WHAT IS FRAUD?

*Black's Law Dictionary* - “Fraud is a generic term, and embraces all the multifarious means which human ingenuity can devise, which are resorted to by one individual, to get an advantage over another by false representations. No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trickery, cunning and unfair ways by which another is cheated. The only boundaries defining it are those which limit human knavery.”

**Legal Elements of Fraud**
1. A material false statement
2. Knowledge that the statement was false when it was made
3. Reliance on the false statement by the victim, and
4. Damages as a result
The use of one’s occupation for personal enrichment
The misconduct of employees, managers and executives
Internal fraud
Victim Organizations

As the chart below illustrates, direct deception schemes were much more common at small organizations than at large entities. Recognizing and protecting themselves from common risks at small organizations, these fraudsters would tailor their presentation and opportunity to suit the victim's vulnerabilities. They would also learn to remain untraceable, as the financial resources of small organizations can be depleted more quickly and may not have the same amount of resources available to them as larger organizations.

Methods of Predator Based Victim Organization

<table>
<thead>
<tr>
<th>Method of Fraud</th>
<th>Percent of Cases</th>
<th>Small Organizations</th>
<th>Large Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Median Loss Based on Size of AFA Fraud Victims

<table>
<thead>
<tr>
<th>Size of AFA</th>
<th>Median Loss $</th>
<th>Mean Loss $</th>
<th>Median Loss %</th>
<th>Mean Loss %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>$5,000</td>
<td>$15,000</td>
<td>$10,000</td>
<td>$30,000</td>
</tr>
<tr>
<td>Large</td>
<td>$25,000</td>
<td>$75,000</td>
<td>$50,000</td>
<td>$150,000</td>
</tr>
</tbody>
</table>

Depiction Based on Presence of AFA Fraud Controls

<table>
<thead>
<tr>
<th>Controls</th>
<th>Present</th>
<th>Lost $</th>
<th>Present</th>
<th>Lost $</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-level manager approval</td>
<td>90%</td>
<td>$5,000</td>
<td>80%</td>
<td>$7,500</td>
</tr>
<tr>
<td>Written policies</td>
<td>80%</td>
<td>$10,000</td>
<td>60%</td>
<td>$15,000</td>
</tr>
<tr>
<td>Internal controls</td>
<td>70%</td>
<td>$20,000</td>
<td>50%</td>
<td>$30,000</td>
</tr>
<tr>
<td>Security audits</td>
<td>60%</td>
<td>$30,000</td>
<td>40%</td>
<td>$45,000</td>
</tr>
<tr>
<td>Background checks</td>
<td>50%</td>
<td>$40,000</td>
<td>30%</td>
<td>$60,000</td>
</tr>
<tr>
<td>Good documentation</td>
<td>40%</td>
<td>$50,000</td>
<td>20%</td>
<td>$75,000</td>
</tr>
</tbody>
</table>

* These controls are independently assessed by each organization.
ACFE 2010 REPORT TO THE NATIONS – Other Highlights

- Typical organization loses 5% of revenues to fraud
- Median loss was $160,000
- Nearly 25% involved losses of at least $1 million
- Frauds lasted a median of 18 months before detection
- Asset misappropriation schemes were in 90% of cases
- Financial statement schemes were less than 5% but caused median losses of more than $4 million
- More likely to detected by tip
- More than 80% were committed in accounting, operations, sales, upper management, customer service or purchasing
- More than 85% had never been charged or convicted
- Most common red flags were living beyond means and financial difficulties
**COSO’S FRAUDULENT FINANCIAL REPORTING 1998-2007**

Common Financial Statement Fraud Techniques

- Improper Revenue Recognition 61%
- Overstatement of Assets 51%
- Understatement of Expenses/Liabilities 31%
- Misappropriation of Assets 14%
- Inappropriate Disclosures 1%
- Other Miscellaneous Techniques 20%
- Disguised Through Related Party Trans 18%
- Insider Trading Cited 24%

---

**COSO’S FRAUDULENT FINANCIAL REPORTING 1998-2007**

Improper Revenue Recognition

- Sham sales
- Conditional sales
- Round-tripping
- Loans as sales
- Bill and hold
- Revenue before sale completed
- Improper cutoff of sales
- Improper use of percentage of completion
- Unauthorized shipments
- Consignment sales
COSO’S FRAUDULENT FINANCIAL REPORTING 1998-2007

Asset Accounts Misstated
- Inventory
- Accounts Receivable
- Property and Equipment
- Cash/Marketable Securities
- Loans and Notes Receivable
- Investments
- Prepaid Expenses

FRAUD TRIANGLE

Opportunity

Incentive/Pressure

Rationalization
FRAUD DIAMOND

Opportunity
Incentive/Pressure
Rationalization
Capability

Fraud

RISKS FALLING OUTSIDE SOX

Reputation
Legal
Strategic
Operational
### COMPREHENSIVE ANTIFRAUD PROGRAM

#### Control Environment

<table>
<thead>
<tr>
<th>Fraud Risk Assessment</th>
<th>Antifraud Control Activities</th>
<th>Information and Communication</th>
<th>Monitoring</th>
</tr>
</thead>
</table>

---

### COMPREHENSIVE ANTIFRAUD PROGRAM

#### Control Environment

- **Code of Ethics**
- **Handbooks, Manuals, Memos**
- **Fraud Policy**
- **Whistle Blower Policy**
FRAUD RISK ASSESSMENT GOALS

Provide a map to the fraud schemes and scenarios the company potentially faces with an understanding of existing controls and a list of steps needed to mitigate fraud risk on an ongoing basis.

CONDUCTING A FRAUD RISK ASSESSMENT

- Organize the assessment
- Determine the scope
- Identify universe of fraud schemes and scenarios
- Determine likelihood of identified risks
- Determine assessment significance
- Mapping fraud schemes to mitigating controls
- Evaluate controls for design effectiveness
- Develop risk responses
- Test controls to validate operating effectiveness
- Communicate findings
- Schedule follow up
Preventive Controls
- Separation of duties
- Proper authorization
- Adequate documentation
- Physical control over assets and information systems

Detective Controls
- Reviews of performance
- Analyses
- Reconciliations
- Physical observations
- Information systems
- Proactive fraud detection
Controls which help eliminate risk factors which many lead to fraud

SIX STEP APPROACH TO PROACTIVE FRAUD DETECTION

Step 1 – Understand the Business
Step 2 – Identify the possible frauds that could exist
Step 3 – Catalog possible fraud symptoms
Step 4 – Use technology to gather data about symptoms
Step 5 – Analyze the results
Step 6 – Investigate the symptoms
SIX STEP APPROACH TO PROACTIVE FRAUD DETECTION

Analytical

Step 1: Understand the Business

Step 2: Identify Possible Frauds that Could Exist

Step 3: Catalog Possible Fraud Symptoms

Technology

Step 4: Use Technology to Gather Data About Symptoms

Step 5: Analyze Results

Investigative

Step 6: Investigate Symptoms

Follow Up

TYPICAL ENVIRONMENT IN WHICH FRAUD OCCURS

- Trust is placed in employees
- Employees have detailed knowledge of the accounting systems and their weaknesses
- Management domination subverts normal internal controls
- Management adds pressure to “make the numbers”
- Expected moral behavior is not communicated to employees
- Unduly liberal accounting practices
- Ineffective or nonexistent internal auditing staff.
- Lack of effective internal controls.
- Poor accounting records.
- Related party transactions.
- Incomplete and out of date procedural documentation.
- Management sets a bad example.
RED FLAGS IN FRAUDULENT FINANCIAL STATEMENTS

- Cash flow does not match net income
- Receivables spike relative to sales – Days’ Sales in Receivables
- Management earning tied to performance
- Decrease in the Asset Quality Index – Noncurrent Assets, exclusive of PPE, relative to total assets in given year
- Exceptionally strong sales growth from one year to next
- Significant increase in Gross Margin Index
- High turnover of key management
- Sales allowances, warranties and other reserves out of line compared with others in industry
- Low Total Accruals to Total Assets – Working Capital, less Cash, less Current Taxes Payable, less Current Portion of LTD, less AD and Amortization, divided by Total Assets

EMPLOYEE RED FLAGS

- Employee lifestyle changes
- Significant personal debt and credit problems
- Behavioral changes
- Defensive
- Fraud and Stupid look the same
- High employee turnover
- Refusal to take vacation or sick leave
- Lack of segregation of duties in a high-risk (vulnerable) area
MANAGEMENT RED FLAGS

- Reluctance to provide information to auditors
- Photocopied or missing documents
- Decisions dominated by an individual or small group
- Excessive number of year-end transactions
- Management displays significant disrespect for regulatory bodies
- Excessive number of or frequent changes in checking accounts
- Weak internal control environment
- Unexpected overdrafts or declines in cash balances
- Accounting personnel are lax or inexperienced
- High employee turnover rate
- Compensation is out of proportion
- Decentralization without adequate monitoring
- Frequent changes in external auditors

RED FLAGS IN PAYROLL

- Inconsistent overtime hours for a cost center / department
- Overtime charges for employees who normally would not have overtime wages
- Employees with duplicate Social Security numbers, names, and addresses
- Overtime charged during a slack period
- Budget variations for payroll by cost center / department
- Employees with few or no payroll deductions
RED FLAGS IN CASH OR ACCOUNTS
RECEIVABLE

- Excessive number of voids
- Presence of personal checks in petty cash
- Sudden activity in a dormant account
- Taxpayer complaints that they are receiving non-payment notices
- Discrepancies between bank deposits and postings
- Excessive or unjustified cash transactions
- Large number of account write-offs
- Bank accounts not reconciled on a timely basis
- Unauthorized bank accounts
- Abnormal number of expense items or reimbursement to an employee

RED FLAGS IN BILLING SCHEMES

- Remittance to PO Box
- Telephone does not match physical address
- Consistent billing in round numbers
- Address matches employee address
- Invoices consistently under approval limits
- Use of consecutive invoice numbers
- Invoice numbers and dates do not correspond
- Increasing purchases to same vendor
- Incomplete vendor master information
- Unspecified consulting or other services
RED FLAGS CHECK TAMPERING SCHEMES

- Voided or missing checks
- Invoices posted to inconsistent accounts
- Checks used out of order
- Journal entries to cash
- Duplicate check numbers on bank reconciliations
- Altered or dual endorsements
- Customer complaints regarding payments
- Checks payable to cash
- Altered payee on checks
- Checks payable to employees

RED FLAGS IN PURCHASING OR INVENTORY SCHEMES

- Increasing number of complaints about services
- Vendors without physical address
- Lack of physical security over assets / inventory
- Excessive inventory or slow-moving inventory
- Payments to vendors not included on an approved vendor list
- Vendor address matching employee address
- Abnormal inventory shrinkage
- Purchases that bypass normal procedures
- Charges without shipping documents
- Vendor payments picked up rather than having it mailed
- High volume of purchases from new vendors
SYMPTOMS OR RED FLAGS

Do not ignore a red flag – Studies of fraud cases consistently show that red flags were present, but were either not recognized or were recognized but not acted upon by anyone.

Sometimes an error is just an error – Red flags should lead to some kind of appropriate action, i.e. an investigation by a measured & responsible person, but sometimes an error is just an error and no fraud exists.

RED FLAGS PRESENT IN CORRUPTION SCHEME

[Diagram showing various symptoms and red flags related to corruption, such as kickbacks, analytical symptoms, behavioral symptoms, tips and complaints, lifestyle symptoms, and internal controls.]
The offering, giving, receiving or soliciting any thing of value to influence an official act or business decision:

- Bribery
- Illegal gratuities
- Conflicts of interest
- Economic extortion
Billing Schemes

Perpetrator causes the victim organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices or personal purchases:

- Invoicing via Shell Companies
  - Submitting False Invoices
  - Pass through Entities
- Non-Accomplice Vendor
  - Pay and return
  - Overbilling or duplicate invoices
- Personal Purchases

CASE STUDY #1
Asset Misappropriation - Billing Scheme

- A Large retail company
- Director of IT
- 10-year employee
- Could authorize expenditures up to $15,000
- Computer consultants contract ran out in prior year
- Suspect set up computer consulting in current year budget
- Created shell company and incorporated
- Self approval of invoices
- Losses were $365,000
- Asked AP to hold that check!
CASE STUDY #1
Asset Misappropriation - Billing Scheme

Controls to Prevent or Detect

1. Promote a culture of integrity
2. Provide fraud awareness training
3. Promote the company’s anonymous hotline and protect whistleblower’s
4. Require reporting of management override of controls and procedures
5. Perform necessary due diligence on all new vendors

Check Tampering Scheme

Perpetrator converts an organization’s funds by forging or altering a check on one of the organization’s bank accounts, or steals a check the organization has legitimately issued to another payee:

- Forged Maker
- Forged Endorsements
- Altered Payee
- Concealed Check
- Authorized Maker
CASE STUDY #2
Asset Misappropriation – Check Tampering

• A Medium size manufacturing company
• Suspect was Assistant Controller
• 8-year employee
• Responsible for accounts payable and payroll
• Suspect has purchased new car and traveled each year
• Approximately 7 years prior, suspect has tax lien
• Check numbers and dates out of sequence
• Vendor name on check was different than records
• Losses were $650,000
• Backed up system, produced checks, restored system
• Removed checks/check copies from statement

CASE STUDY #2
Asset Misappropriation – Check Tampering

Controls to Prevent or Detect

1. Obtain a credit report on all employees involved in handling of funds
2. Have someone independent of disbursements receive and review the bank statement and canceled checks each month
3. Have someone independent of disbursements account for all checks, including voided checks
4. Never pre sign checks
5. Have the associate roll forward the GL cash account each month in addition to reconciling the bank statement
CASE STUDY #5
Asset Misappropriation – Skimming Sales

- Chain of 10 drug stores
- 5-year employee of the company and college student
- Was considered a very trusted employee and friend of the family
- Prescription system was not tied to cash register
- Entered “no sale” to open the register for cash sales
- Many times would enter “no sale” for friends and family
- Closed the store and insisted on closing the register for prescription sales
- Bought several cars and boat

Controls to Prevent or Detect

1. Update systems to provide necessary accountability
2. Install surveillance camera in appropriate locations
3. Monitor and review ratio of daily cash sales/deposits
4. Have someone independent of recording sales close out the registers
5. Perform surprise audits
CASE STUDY #3
Asset Misappropriation - Inventory

- Large parts manufacturing company
- Perpetrator was warehouse manager
- 18-year employee
- Was considered very knowledgeable about all inventory in the warehouse
- Never took vacations
- Obtained pass word from wife
- Had product picked up during third shift
- Arrived early and removed inventory and shipping information from system

CASE STUDY #3
Asset Misappropriation - Inventory

Controls to Prevent or Detect

1. Have IT require and document the suspension of passwords when employees change positions or leave the company

2. Have internal audit or another group “audit” the password assignments and review the password capabilities

3. Provide exception reports, by person executing the change, to management for all changes in inventory status

4. Require vacations be taken and consider job rotation
CASE STUDY #4
Fraudulent Financial Reporting

• Large manufacturer of computer components
• CFO was 12-year employee of the company
• Several years before, the company was very profitable
• CFO was very aggressive in setting up loss contingency and other reserves
• When there was a downturn in the economy, company needed additional financing
• Loss contingencies and reserves were reversed into income
• After financing obtained, company subsequently declared bankruptcy

Controls to Prevent or Detect

1. Promote a culture of integrity and adopt ethics policies and training
2. Provide fraud awareness training
3. Promote the company’s anonymous hotline and protect whistleblower’s
4. Do not tie compensation directly to bottom line results
5. Data mine email language for key words
Discussion/Questions

billacuff@decosimo.com