Fraud Detection and Internal Controls

Presented to State of Vermont
September 5, 2019
Presentation Objectives

• Define fraud
• Recognize how frauds are detected
• Identify the components of the fraud triangle
• Define the types of fraud, the profile of a fraudster, and common red flags
• Relate fraud risks to internal controls
• Identify examples of why internal controls fail
• Apply internal control best practices within their organization or department
Fraud Defined
Fraud Defined

"Fraud is any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and/or the perpetrator achieving a gain."
Source: "Managing the Business Risk of Fraud: A Practical Guide

“Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.”
Source: IIA’s International Professional Practices Framework (IPPF)
Fraud or Error

• What is the difference?

INTENT
Two Types of Intentional Misstatements

- Fraudulent Financial Reporting
- Misappropriations of Assets
ACFE Report to the Nations 2018

- Report to the Nations on Occupational Fraud and Abuse, 2018 Global Fraud Study
- Bi-Annual Report
- Analysis of 2,690 cases of occupational fraud across 125 countries

Seven Key Facts from the *Report to the Nations* and Our Experience

I. *Loss To Organizations*

- Typical organizations lose 5% of revenue in a given year as a result of fraud
- Occupational Fraud:
  - The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets
  - The key to occupational fraud is that the activity:
    - Is clandestine
    - Violates the employee's fiduciary duties to the organization
    - Is committed for the purpose of direct or indirect financial benefit to the employee
Key Facts from the \textit{Report to the Nations} and Our Experience

\textbf{II. Fraud Exists in Every Industry and Organization Type}
II. Fraud Exists in Every Industry and Organization Type
Key Facts from the *Report to the Nations* and Our Experience

**III. Prominent Organizational Weakness – Lack of Internal Controls**

![Diagram showing how internal control weaknesses vary by scheme type.](image)
Key Facts from the *Report to the Nations* and Our Experience

**IV. Misappropriation of Assets**

- Most common form of occupational fraud

![Bar chart showing percentage and median losses of different types of fraud](image)

- Asset misappropriation: 89% of cases, median loss $114,000
- Corruption: 38% of cases, median loss $250,000
- Financial statement fraud: 10% of cases, median loss $800,000
FIG. 4 Occupational Fraud and Abuse Classification System (the Fraud Tree)
Key Facts from the *Report to the Nations* and Our Experience

**IV. Misappropriation of Assets**

Billing schemes and check tampering present the greatest risk to organizations.
Key Facts from the *Report to the Nations* and Our Experience

V. First Time Offenders

**FIG. 36** Do perpetrators tend to have prior fraud convictions?

- Never charged or convicted (89%)
- Charged but not convicted (6%)
- Had prior convictions (4%)
- Other (1%)
Key Facts from the *Report to the Nations* and Our Experience

**VI. Origin – Accounting Department**

*Fig. 28 What departments pose the greatest risk for occupational fraud?*

- Executive/upper management: $729,000 11%
- **Accounting**
- Information technology
- Warehousing/inventory
- Facilities and maintenance
- Purchasing
- Finance
- Administrative support
- Sales
- Operations
- Customer service
- Other
Profile of a Fraudster
What does a fraudster look like?
Who Can Commit Fraud?

ANYBODY is capable of committing FRAUD

Report to The Nations – Some Statistics on Perpetrators

• Perpetrator’s level of authority has been strongly correlated with the size of the fraud
  – Employees and managers were much more likely to commit occupational fraud, but, the losses in these schemes were much lower—though still substantial

• Correlation between the fraudster’s level of authority and the duration of the occupational fraud scheme
  – The typical fraud committed by an employee lasted 12 months before it was detected, whereas the typical fraud committed by an owner/executive lasted 24 months. Frauds committed by managers had a median duration of 18 months.
The Fraud Triangle

Understanding the Fraud Triangle is critical to:

- Minimize the risk of abuse
- Minimize the risk of fraud
- Develop strong internal controls
The Impact of Collusion

Figure 87: Number of Perpetrators—Frequency and Median Loss
Behavioral Red Flags Observed

- Living Beyond Means: 45.8%
- Financial Difficulties: 30.0%
- Unusually Close Association with Vendor/Customer: 20.1%
- Wheeler-Dealer Attitude: 15.3%
- Control Issues, Unwillingness to Share Duties: 15.3%
- Divorce/Family Problems: 13.4%
- Irritability, Suspiciousness or Defensiveness: 12.3%
- Addiction Problems: 10.0%

© 2016 Association of Certified Fraud Examiners, Inc. All rights reserved
Non-Fraud-Related Misconduct

Breakdown of Non-Fraud-Related Misconduct (% of All Cases)

- Bullying or intimidation: 18.0%
- Excessive Absenteeism: 11.6%
- Excessive Tardiness: 10.2%
- Excessive Internet Browsing: 7.0%
- Visiting Inappropriate Internet Sites: 3.2%
- Other: 3.1%
- Sexual Harassment: 3.2%
How are Frauds Detected
Maintaining Professional Skepticism

- Acknowledge that fraud risk exists
- Encourage open and candid discussion – Know your employees
- If I were to try to commit fraud, how would I do it?
- Continuously assess the risk of management and control override (think about collusion)
- Openly display your skepticism to set the tone at the top and spread awareness
- Take swift action when fraud event occur and make the response action (not the details) known internally
Sources of Tips

- Employee: 51.5%
- Customer: 17.8%
- Anonymous: 14.0%
- Vendor: 9.9%
- Shareholder/Owner: 2.7%
- Competitor: 1.6%
- Other: 12.6%
Responsibilities of the Auditor
Consideration of Fraud

- AU-C Section 240: Consideration of fraud in a financial state audit
- Auditor is not responsible for detecting fraud but is responsible for the Consideration of Fraud
- Expansion of:
  - Section 315: Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement
  - Section 330: Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained
Responsibilities of the Auditor

“Responsible for obtaining reasonable assurance that the financial statements as a whole are free from material misstatement, whether caused by fraud or error.”
Objectives of the Auditor

• Identify and assess the risk of material misstatement due to fraud
• Obtain sufficient appropriate audit evidence regarding the assessed risk due to fraud, through designing and implementing appropriate responses
• Respond appropriately to fraud or suspected fraud identified during the audit
Requirement for the Auditor

• Maintain professional skepticism
• Discussion among the engagement team (assessing risk)
  – Known external and internal factors
  – Risk of management override of controls
  – Consideration of circumstances indicative of earnings management
  – Importance of maintaining professional skepticism
  – How to respond to the susceptibility of the FS to material misstatement due to fraud
Requirement for the Auditor

• Inquire of management about risk
  – Most effective when performed in person
  – Useful for identifying risks of employee fraud or other managers
  – Make inquiries of others: non-management; non-accounting
  – Corroborate management’s responses with other information
  – Listen and respond accordingly

• Plan audit to detect material misstatements

• Document auditors assessments of risks and responses
Internal Controls – Your Best Defense
Preventive Controls

Designed to prevent misstatements / fraud before it has occurred

• Provide employees fraud awareness training
• Implement policies and procedures
• Segregate Duties
• Establish passwords and physical safeguards to restrict unauthorized access
• Ensure alignment of responsibilities, authority and incentives
Detective Controls

Designed to detect misstatements / fraud after it has occurred
- Establish a fraud reporting system (i.e. whistleblower hotline)
- Use reconciliations, independent reviews, physical inspections/counts and analysis
- Review exception reports and ensure that they are cleared by persons with appropriate authority
- Utilize technology to perform data analysis and comparison and continuous auditing techniques
- Perform surprise audits
Control Types

• Authorization
• Management review
• Reconciliations
• Segregations of Duties
• System access
• Exception and edit reports
• Key performance indicators
Controls – Segregation of Duties

Smaller organizations or departments with limited resources can still have effective segregation of duties controls.

- Focus on preventive controls rather than detective controls.
- Alternate sequential tasks, so that no one person has complete responsibility for the entire transaction.
- Functions to separate:
  - Authorization,
  - Payment,
  - Custody, and
  - Recording.
- Consider outsourcing if there simply are not enough people to separate the necessary functions.
Segregation of Duties Illustration

"Until we implement a complete segregation of duties solution the auditor said we will need to press the 'enter' key together"
Best Practices
FRAUD PROGRAM BEST PRACTICES

Management ethical commitment.

Fraud Hotlines, reporting procedure and protection.

Fraud awareness training.

Zero tolerance policy and Code of Conduct (recommend a specific senior management code of conduct).

Completion of a fraud risk assessment.

Conflict disclosure process.

Key Human Resources policies and procedures (e.g. background checks).

Investigation Process.

Key Policies and Procedures
Why Controls Fail

- Management override
- Lack of management or governance involvement
  - No conceptual understanding of control
  - Reliance on others (auditors, service providers, etc.)
- Tone at the top is not set appropriately
- Resources needed are not provided
- Collusion
Questions To Consider

• You and your team should consider the following questions:
  – What could go wrong? (WGCW)
  – If I was to commit fraud how would I do it?
  – Do risks exist that encourage fraud?

• Individuals involved in the day to day operations and processes should be involved as well as management
Entity Wide Fraud Risk Considerations

• Financial stability (budget crisis, declining revenue)
• Excessive pressure exists for management to meet requirements or expectations of third parties
• Ineffective monitoring of management
• Complex or unstable organizational structure
• Deficient internal controls
• Lack of formalized policies and procedures
Consideration of Opportunities

• Large amount of cash on hand
• Government-issued credit cards
• Assets that can be easily converted to cash
• Inadequate record keeping
• Lack of reconciliations or timely preparation
• Inadequate oversight of employees
Attitude Matters

- Lack of ramifications in the past
- Lack of promotion of ethical standards
- History of audit findings
- Failure to correct issues timely
- Low morale
- Hiring of unqualified employees or changing qualifications to hire specific individuals
FRAUD DETECTION PROCESS
RED FLAGS

Red Flags for Corruption
- An organization paying more than the best price available.
- Very specific requirements that tend to favor one bidder.
- Projects that are broken into two contracts to circumvent review limits or approval authority.
- A too-successful bidder who is consistently winning bids.
- Social contact between the bid solicitors and bidders.
- A procurement officer living beyond their means.

Employee Red Flags
- Employee lifestyle changes: expensive cars, jewelry, homes, clothes, etc.
- Significant personal debt and credit problems.
- Behavioral changes indicating possible drug, alcohol, gambling addiction, or fear of losing job.
- High employee turnover, especially in areas vulnerable to fraud.
- Refusal to take vacation or leave.
- Lack of segregation of duties.

Work Environment
- Executive management does not appear to care about or reward good behavior.
- Negative feedback and lack of recognition for job performance.
- Perceived inequities in the organization.
- Low organizational loyalty or feelings of ownership.
- Poor training and promotional opportunities.
- Lack of clear organizational responsibilities.
- Poor communication practices or methods within the organization.
Team Approach

• Work with your teams
• Hold a team discussion of WCGW
  – Ask the team how could someone commit fraud or circumvent the control process
• Consider rotating duties
• Look at back-up/vacation procedures
• Involve those that oversee the IT operations/controls
Evolution and Change

- Processes and technology are evolving
- Efficiency is a driving force
- Are your internal controls evolving?
  - How often are your meeting to review the controls?
  - Are your people evolving?
  - Do they understand the new process and/or technology?
How Data Analytics Can Be Useful Tools
Cash disbursement analytics

• Understand vendor relationships
  – Identify key vendors (top 10 or 20 paid)
  – Identify new/unapproved vendors
  – Identify related party vendors (comparison of vendor list to employee list)
  – Identify vendors receiving suspicious recurring or one-time payments

• Identify duplicate payment

• Identify multiple payments just below approval threshold

• Identify out of sequence payments

• Analyze and trend disbursements by name, vendor type, etc.
Payroll Analytics

- Trend and analyze payments over time (total, department, geographic location, job function, employee)
- Compare HR employee listing to actual paid employees
- Compare approved pay rate per HR to pay rate in payroll system
- Identify payments made before hire date or after term date
- Identify large or unusual payments (bonuses, extra pay)
- Analyze overtime payments
- Identify manual adjustments to payroll
Travel and Expense Reimbursement Analytics

- Group payments by meaningful classifications, such as hotel, airfare, meals, mileage, transportation, etc.
- Group payments by meaningful classifications, such as department, location, function, etc.
- Group payments by employee
- Identify duplicate submissions. This can be run on invoice number, amount, employee, month, or description.
- Identify payments made outside of understood business hours
Current Trends in State & Local Governments
Frauds in State & Local Government

• It’s happening!!!
• ACFE has identified government and public administration as one of the top three industries for fraud
Fraud in State & Local Government: Most Common Fraud Schemes

1. Fictitious & Dormant Vendor Fraud
2. Employee Expense Reports Fraud
3. P-Cards Fraud
4. Disbursement Fraud
5. Cash Receipts Fraud
6. Payroll/Time Card Fraud
7. Conflicts of Interest
8. Procurement
1. Fictitious & Dormant Vendor Fraud

Red Flags & Risk Areas:

- Poor controls over vendor master list
  - AP personnel can add/revise vendors
  - Employees can request/submit changes to vendor information
  - Vendor master list not cleaned up regularly
  - Dormant vendors not made inactive
- One-time (temporary vendor) number
- Employees can request that checks be routed back to themselves
- Employees can pick-up checks from accounting
- Payments to individuals (consultants), new vendors, unknown vendors
- Round dollar payments, payments just below approval thresholds
### Victim | School District

#### FICTITIOUS & DORMANT VENDOR FRAUD

<table>
<thead>
<tr>
<th>Org. Size</th>
<th>Annual Budget = $300 million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perpetrator</td>
<td>Director; male; no known personal of family issues</td>
</tr>
</tbody>
</table>

#### Scheme
- Submitted to purchasing a name and address change for an existing vendor (via a forwarded email that appeared to be from the vendor)
- Approved a new contract be executed with the vendor, and he made changes to vendor information on the draft contract
- He approved and submitted invoices from the vendor for payment
- Payments were mailed to new address (mail center)
- Wife created a DBA in the revised vendor name, opened a bank account, and deposited check
- Bank put a hold on the check and called the district

#### Results of Investigation
- Employee resigned when he was notified of administrative leave (declined to be interviewed)
- Through background checks, original vendor appeared to be related to employee (conflict of interest)
- Payments totaled over $480,000 (31 payments) from FY2011/12 to FY2017/18
- No current employees in department were familiar with vendor
- Initial 2 years – invoices based on specific services provided ($112,000 – believed to be legitimate)
- Last 5 years – changed contract to fixed fee, no detailed invoices ($369,000 – believed to be fictitious invoices)

#### Possible Detection Methods
- Review vendor change reports for unusual changes (name change, tax ID change, etc.) and who made changes
- Inquire with personnel (particularly staff) about most frequent or common vendors used
- Use of data analytics
2. Employee Expense Reports Fraud

Scheme:

• Employee submits fictitious, duplicate, or personal expenses on expense report

Red Flags & Risk Areas:

• Executive level expense reports not reviewed at the appropriate level (higher level executive; Board)
• Frequent missing receipts
• Lack of detailed receipts
• High frequency/dollar amount of expenses compared to others
• Employee with p-card also has high frequency/dollar amount of expenses
2. Employee Expense Reports Fraud

Possible Audit Detection Methods:

- Summarize expenses by employee and department and identify employees that have significantly more expenses than people at similar level
- Compare P-card purchase detail with expense report detail (by employee)
- Inquire about the approval process for executive level employees
3. P-Cards Fraud

Scheme:
- Employee uses P-Card for personal purchases

Red Flags & Risk Areas:
- Executive level P-Card expenditures are not reviewed at the appropriate level (higher level executive; Board)
- Frequent missing receipts or lack of detailed receipts
- High frequency/dollar amount of expenses compared to others
- Does not complete monthly P-Card reconciliation
## Victim | Charter School

<table>
<thead>
<tr>
<th></th>
<th>P-CARD / CREDIT CARD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org. Size</td>
<td>$38 Million in annual revenues and $21 million in assets</td>
</tr>
<tr>
<td>Perpetrator</td>
<td>Founder and CEO; female, mid-50s; no known financial or personal issues</td>
</tr>
<tr>
<td>Scheme</td>
<td>CEO used school P-card (credit card) for personal purchases</td>
</tr>
<tr>
<td>Results of Investigation</td>
<td>• Missing supports for multiple expenses</td>
</tr>
<tr>
<td></td>
<td>• Gasoline charges while having an auto allowance</td>
</tr>
<tr>
<td></td>
<td>• No approval or incorrect approval of credit card statements</td>
</tr>
<tr>
<td></td>
<td>• Extravagant purchases (high-end clothing and accessories, luxury hotel stays, first class international flights)</td>
</tr>
<tr>
<td>Possible Detection Methods</td>
<td>• Analytics on P-card expenditures</td>
</tr>
<tr>
<td></td>
<td>• Review of P-Card limits and assess for reasonableness</td>
</tr>
<tr>
<td></td>
<td>• Identify unusual Merchant Classification Codes (MCC)</td>
</tr>
<tr>
<td></td>
<td>• Review process for review of expenditures made by high-level individuals (is the board reviewing the CEO’s expenditures?)</td>
</tr>
</tbody>
</table>
4. Disbursement Fraud

Scheme:

- Employee prepares fictitious A/P check requests
  - Fictitious vendor payments
  - Fictitious refunds to customers
- Employee knowingly processes or approves payment on inflated invoices
- Employee steals outgoing checks and deposits them into a personal account
- Employee issues checks to self or for personal expenses and forges authorized signature
- Employee requests and has approved vendor payments for personal services (small construction, supplies, credit cards, fuel cards, etc.)
4. Disbursement Fraud

Red Flags & Risk Areas:

- Route back requests (not directly mailed to vendors)
- One-time vendor accounts or temporary vendor accounts
- Complaints by vendors of late payments
- Expenses exceed budget or are increasing over time
- Multiple payments to vendors that should be paid only monthly (utilities, credit cards, office/home supplies, construction)
- Excessive use of one account type by a single employee
- Vendor used by only one employee
<table>
<thead>
<tr>
<th></th>
<th>DISBURSEMENT FRAUD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Org. Size</strong></td>
<td>$1.5 million department budget</td>
</tr>
<tr>
<td><strong>Perpetrator</strong></td>
<td>Long-term, trusted employee; female; late 40s; divorced; family medical issues; drug addiction</td>
</tr>
</tbody>
</table>
| **Scheme**             | Department accountant handled deposits, payment requests, journal entries, account reconciliations  
                          • Employee created and approved fictitious refunds to “customers” (8 accomplices)  
                          • Created falsified supporting documentation  
                          • Payments mailed to accomplices for deposit into bank accounts  
                          • More recent years, issued refunds to a local non-profit for which she was the Treasurer  
                          • Marked the checks for pick-up from Accounting (used supervisors log-in to approve)  
                          • Deposited checks into account in non-profit name |
| **Results of**        | Prepared and approved fictitious refunds totaling $1.8 million (240 checks over 8 years)  
                          • Approved disbursements to a fictitious vendor totaling $290,000 (42 checks/ACH over 3 years)  
                          • Used 16 different payee names/addresses  
                          • Processed using a temporary vendor number that allowed manual entry of payee name and address  
                          • Checks to accomplices were mailed; checks to non-profit were processed for pick-up  
                          • Funded the theft by misapplying operational revenue deposits to agency funds (where customer deposits were originally recorded) |
| **Possible Detection**| Analytics on payments made via temporary vendor number  
                          • Identification of round dollar payments  
                          • Trending analytics by department (operational revenue continued to decline despite increased workload) |
Other Red Flags of Possible Check Tampering

- Missing, out-of-sequence, out-of-range, or duplicate check numbers
- Excessive or unexpected voided checks
- Unexpected, unexplained, or unusual number of checks payable to “cash.”
- Check recorded for zero dollars
- Voided checks that are not documented and destroyed
- Non-payroll checks made payable to or endorsed by an employee
- Unusual, altered, or dual endorsements on canceled checks
- Canceled checks that appear to have been prepared, signed, and endorsed in the same handwriting
- Signature on a canceled check by an authorized signer who was out of the office on the date of the check
- Checks lacking supporting documentation
5. Cash Receipts

**Scheme:**

- Employee or volunteer takes incoming cash or checks for personal use
- Checks made out to any payee can be deposited into a bank account without suspicion or question
- Unexpected receipts are particularly susceptible to theft (donations, fundraising activity, refunds, facility use contracts/fees, etc.)
- Use of an “unknown” bank account in organization name
5. Cash Receipts

Red Flags & Risk Areas:

- Poor controls over cash collection processes
  - Insufficient or no segregation of duties
  - No reconciliation of sales
- Decentralized collections of cash/checks (organization does not know what is being collected and where)
- Insufficient training of employees
- Poor controls over bank account management
  - Process for opening a new bank account
  - Are unused accounts closed when no longer in use?
- Old A/R aging
- Complaints by customers of delayed application of payments
<table>
<thead>
<tr>
<th><strong>CASH RECEIPTS FRAUD</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Org. Size</strong></td>
</tr>
<tr>
<td><strong>Perpetrator</strong></td>
</tr>
</tbody>
</table>
| **Scheme** | • Used a dormant bank account on which he was the only signer to deposit incoming checks made payable to the district (state refunds, donations, fundraising, proceeds from vending machine vendor)  
• Bank account was originally opened (with permission of the Superintendent) to deposit and track funds related to a summer international field trip  
• Used funds for mostly personal use (paid federal income taxes, local hotels, local restaurants, gift cards, hot tub)  
• Bank statements were mailed to him at the district (no one was allowed to open his mail) |
| **Results of Investigation** | • Deposited almost $700,000 into the “dormant” bank account over approximately 5 years  
• Largest deposit was a check for approximately $56,000  
• Upon discovery, only approximately $70,000 was left in the account  
• Discovered when new Controller went to bank to add his name to the district accounts and bank rep inquired about the account  
• Always giving gift cards to employees and parent volunteers (sign of guilt)  
• Some potentially legitimate district purchases; however, they were included in the loss because they did not go through the proper procurement process |
| **Possible Detection Methods** | • Inquire about all accounts with organization tax ID at banks on a periodic basis  
• Segregation of duties or rotation of duties  
• Trend miscellaneous revenue activity |
6. Payroll/Timesheet Fraud

Schemes:

- Reporting inflated or fictitious hours
- Not reporting vacation, sick, PTO
- Inappropriate bonus/extra pay
- Inappropriate or excessive vacation payout
- Ghost employees
- Unauthorized pay rate changes
6. Payroll/Timesheet Fraud

Red Flags & Risk Areas:

- Poor processes related to input and approval of time entry
- Manual tracking of vacation, sick, PTO (or separate system that does not interface with time entry/payroll system)
- High level and/or salary employees that are never around
- Full administrative rights of payroll personnel
- No segregation between HR and payroll functions
- Employees that never report vacation, sick, PTO (ghost employee; failure to accurately report time off)
- Employees paid that are not on HR’s employee list, organization director, departmental listings
**PAYROLL FRAUD**

<table>
<thead>
<tr>
<th>Org. Size</th>
<th>Annual budget of $300 million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perpetrator</td>
<td>Superintendent; male; late 60s; financial difficulties</td>
</tr>
</tbody>
</table>

**Scheme**
- District allowed employees to cash out vacation time as long as it did not go below 40 hours (no written policy)
- Employee often failed to report vacation time taken; accumulated a high balance of vacation time
- Submitted several vacation payout requests over the course of two years (largest payout was approx. $70k)
- Payroll used manual process to track vacation time; payroll failed to record 3 of his vacation payouts
- Employee never notified payroll of the oversight

**Results of Investigation**
- Overpayments on vacation payout totaled over $100,000
- Review and approval relied on employee to report available vacation time
- Subordinate employee approved vacation payout and did not independently verify balance
- Board was unaware of unwritten vacation payout policy or requests made by Superintendent
- No process in payroll to track when vacation adjustments were entered/recorded
- In one instance, used Revolving Cash Funds (petty cash) to pay a vacation payout

**Possible Detection Methods**
- Trending payroll data by employee or department (regular pay, vacation/sick/PTO pay, extra or other pay)
- Trending vacation data
- Mandatory vacation

---

Victim | School District
7. Conflicts of Interest

Scheme:
- Employee has undisclosed personal interest in a transaction or contract and uses position to influence a decision which results in personal financial gain
  - Direct relationship and/or financial interest
  - Indirect relationship and/or financial interest (e.g., family member works for vendor)

Red Flags & Risk Areas:
- Unusual delays in providing requested information
- Undue time pressures imposed by management to resolve complex issues
- Tips of complaints about fraud, including whistleblowers inside the organization
- Prior complaints or civil actions
7. Conflicts of Interest

Red Flags & Risk Areas (cont.):

- Frequent use of exceptions to policy
- Frequent failure to follow required processes/policies
- Unusually close relationship between employee and vendor
- Significant volume of work going to one vendor
- Excessive change orders on a construction job
- Projects with one vendor consistently coming in over budget
- Little detail on invoices
<table>
<thead>
<tr>
<th>Victim</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONFLICTS OF INTEREST</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Org. Size</strong></td>
<td>Annual department budget of approximately $50 million</td>
</tr>
<tr>
<td><strong>Perpetrator</strong></td>
<td>Director; male; mid-50s; no known financial or personal issues</td>
</tr>
<tr>
<td><strong>Scheme</strong></td>
<td></td>
</tr>
<tr>
<td>• Director’s son worked for one of the vendors that submitted bids on 2 RFPS</td>
<td></td>
</tr>
<tr>
<td>• Director attempted to influence the RFP processes</td>
<td></td>
</tr>
<tr>
<td>‒ Instructed staff to combine the two RFPS into one even though different specialties</td>
<td></td>
</tr>
<tr>
<td>‒ Initial round of RFPS son’s company failed to submit a bid on time; Director asked Purchasing if they could</td>
<td></td>
</tr>
<tr>
<td>‒ Accept the late proposal then instructed staff to reject bids received and re-open RFPS</td>
<td></td>
</tr>
<tr>
<td>• Did not disclose relationship to anyone in his department or at the City until after the winning vendor was selected</td>
<td></td>
</tr>
<tr>
<td>• and one of the other bidders submitted a protest letter</td>
<td></td>
</tr>
<tr>
<td><strong>Results of Investigation</strong></td>
<td></td>
</tr>
<tr>
<td>• Son lived at home with Director</td>
<td></td>
</tr>
<tr>
<td>• Upon receiving bid protest, Purchasing initiated an internal investigation and consulted with the City Attorney’s Office</td>
<td></td>
</tr>
<tr>
<td>• City Attorney concluded that a conflict existed because son was living at home</td>
<td></td>
</tr>
<tr>
<td>• CLA investigation (retained by Internal Audit department) ran concurrently with Purchasing’s investigation (there were other matters being investigated by CLA)</td>
<td></td>
</tr>
<tr>
<td>• Purchasing rejected all bids and implemented procedures to keep Director out of process</td>
<td></td>
</tr>
<tr>
<td><strong>Possible Detection Methods</strong></td>
<td></td>
</tr>
<tr>
<td>• Conflicts of interest are almost impossible to identify/prove without an admission and/or via background checks</td>
<td></td>
</tr>
<tr>
<td>• Inquire with employees information reported on conflict of interest/ethics reporting forms</td>
<td></td>
</tr>
<tr>
<td>• Analysis to identify payments just below approval thresholds</td>
<td></td>
</tr>
</tbody>
</table>
8. Procurement Fraud

Scheme:
• Bid rigging (leaking information from bidders, accepting late bids, and re-bidding)
• Purchasing thresholds are exceeded (bid splitting)

Red Flags & Risk Areas:
• No public opening of bids
• Deadlines are not enforced, or are extended unnecessarily
• The late bidder happens to be the lower bidder
• Qualified bidders are disqualified for unclear reasons
• Contracts that should have gone out to bid did not
# PROCUREMENT FRAUD

## Victim | School District

<table>
<thead>
<tr>
<th>Org. Size</th>
<th>Annual budget of approximately $62 million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perpetrator</td>
<td>Collusion: Superintendent &amp; Assistant Superintendent</td>
</tr>
<tr>
<td>Scheme</td>
<td>Superintendent and Assistant Superintendent hired a construction company to complete a project over summer. Did not include the Facilities Department, which is responsible for handling all non-bond construction projects. Did not put the project out for a public bid (in California, required for all construction projects over $15,000). Project was completed over approximately two months and cost over $100,000. Vendor submitted 6 invoices that broke down total amount in smaller increments and over a longer period of time than the project lasted.</td>
</tr>
<tr>
<td>Results of Investigation</td>
<td>No contract was signed related to the construction job. No inspections as required by state law. No verification with ADA compliance. A separate PO was issued for each invoice. Payments were questioned by County Treasury, but they allowed payment to occur because work was done. No indication of personal benefit to Superintendent or Assistant Superintendent. Email review showed that employees were aware of California bidding requirements. Currently being reviewed by the District Attorney’s Office.</td>
</tr>
<tr>
<td>Possible Detection Methods</td>
<td>Analyze purchase orders or payments by vendor and amount (identify multiple POs just under bidding/approval requirements). Calculate change orders as a percentage of original contract amounts (separate case where new construction jobs were given to the same vendor as change orders).</td>
</tr>
</tbody>
</table>
What Went Wrong – Recent Example

• County Government:
  – P-cards used for personal expenses
  – Bonuses were given to key members of management
  – Life insurance policies issued to members of management
  – Fraudulent wire transfers to over-pay policies
  – Inappropriate budget amendments/transfers
  – Kickback scheme
  – Violation of procurement policies
  – Fraudulent expense reimbursement
  – Fraudulent time reporting
  – Disbursement of capital and economic development funds to unproved projects
What Allowed These to Happen

- Management override of controls
- Key members of management were long term trusted employees
- Lack of oversight by governance
- Employees failed to report the circumventing of controls due to a fear of retribution
- Tone at the top was not set
Summary – Key Take Aways
SUMMARY - KEY TAKE AWAYS

- Fraud continues to grow in today’s environment and there is an increased focus on addressing fraud.
- A successful fraud program has many aspects, especially a commitment by Governance and Management to the process.
- Completion and updating of a formal Fraud Risk Assessment analysis is an important part of having a successful fraud program.
- Internal controls are key and need to be reviewed and updated frequently.
- Technology is a powerful tool that can be used as a control and to detect and investigate frauds.
- How you respond to a fraud is an important component of fraud program.
- Tone should be set at the top.
Open Discussion and Q&A

Bill Early, Principal
Bill.early@claconnect.com
410-453-5590