

Fraud Auditing

Presented by:

Craig L. Greene, CPA/CFF, CFE, MCJ

of

McGovern & Greene LLP



www.mcgoverngreene.com

Occupational Fraudster's Mantra

- Greed, for lack of a better word, is good. Greed is right. Greed works. Greed clarifies, cuts through, and captures, the essence of the evolutionary spirit. Greed, in all of its forms; greed for life, for money, for love, knowledge, has marked the upward surge of mankind.



Control Environment Challenge

- Governments are organized for and *operated to achieve a particular mission or service for its constituency rather than to make a profit* from their operations.
- With a high level of focus on mission or service, administrative functions such as accounting, internal audit, and procurement are often ignored or seen as unnecessary. Therefore, governmental organizations often *lack sufficient staff to implement or administer an effective system of internal accounting controls*. In addition, many small and medium-sized governmental organizations *lack the financial resources to attract qualified accounting and finance personnel*.



OCCUPATIONAL FRAUDSTER STUDY

2012 ACFE Report to the Nations

- Organizations lose approximately 5% of their annual revenues to employee fraud, waste and abuse.
- \$3.5 Trillion in fraud losses globally.
- The median loss in this study was \$140,000. One-fifth over \$1 million.
- Frauds lasted a median of 18 months before being detected.

2012 ACFE Report to the Nations

- Most common fraud is asset misappropriation.
- More than 87% of fraudsters in the study had never been previously charged or convicted for fraud-related offenses.
- Small organizations are disproportionately victimized by occupational fraud – likely due to their less extensive anti-fraud measures.

2012 ACFE Report to the Nations

- More than 77% of frauds in the study were committed by individuals in one of six departments.
 - Accounting
 - Executive/upper management
 - Operations
 - Customer service
 - Sales
 - Purchasing



WHO COMMITS FRAUD?

What Sort of Person Commits Fraud?

- Someone with a shifty appearance?
- In need of a shave & haircut?
- Black shirt, white tie?
- Sneering glare?
- Low cut blouse, too much makeup, big hair?
- Fraud perpetrators tend to be the least suspected.

Perpetrators

- More authority = greater access to resources & ability to override controls.
- More trust = autonomy & authority...and opportunity.
- More frauds are committed by employees and managers than owners/executives.
- The size of the losses increases directly with authority of the perpetrator's position.



WHY DO THEY DO IT?

Cressey's Hypothesis: The Fraud Triangle

Non-sharable Financial Problem



Rationalization

Opportunity

What to Look For?

- Unexplainable wealth or financial difficulties
- Refusal to take promotions
- Refusal to take time off
- Unusual hours and/or taking on additional work
- Doing jobs below their position or taking on others' responsibilities
- Addictive behaviors – alcohol, drugs, gambling
- Close association with vendors/customers



HOW DO THEY DO IT?

Misappropriation of Assets

- Misappropriation of assets is commonly referred to as theft or defalcation and involves the actual theft of an entity's assets. In the consideration of fraud in financial statement audits, the effect of theft results in material misstatements in the financial statements. Individuals involved in the theft of assets belonging or entrusted to a governmental organization may face civil or criminal charges if caught, especially if such assets were purchased with federal government financial assistance.

Fraud – Three Step Process

- The fraud is *committed*.
- Perpetrators *receive the benefits* of the fraud.
- The fraud is *concealed*.
- Typically the auditor detects fraud during the "concealment" step, which most often results from
 - *Discrepancies in the accounting records.*
 - *Conflicting or missing evidential matter.*
 - *Problematic or unusual relationships between the auditor and the client.*

Review Procedures to Identify Misappropriation

- Ascertaining if any *significant budget adjustments* were made at, near, or after year end.
- Determining whether all budget adjustments made at, near, or after year end were properly and timely *approved by the governing body*, if required.
- Reviewing *significant transfers between classes of net assets* made at, near, or after year end.
- Comparing volume of *purchases by vendor for significant increases* from the prior year.
- Reviewing *adjustments to perpetual fixed asset and/or inventory records* based on current year physical counts.

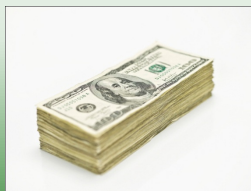
Review Procedures to Identify Misappropriation

- Comparing prior year and current year activity for number and amount of write-offs for
 - Significant *bank reconciling items*.
 - Significant *uncollectible receivables*.
 - Significant *supplies inventory* adjustments.
 - Significant *sales of property, plant, and equipment*.

Cash Frauds

Incoming Cash Frauds

- Skimming
- Altered documents
- Cash Larceny



Fraudulent Disbursements

- Fictitious Vendors
- Check tampering
- Falsified expense reports
- Payroll Frauds
- Credit Card/EFT Frauds



Red Flags for Cash

- Revenue volume drops unexpectedly.
- Customer claims that A/R balances have been paid.
- Employee makes extra effort to be the person to handle/make deposits.
- Lower average cash volume.
- Missing or out of sequence checks
- Significant bank reconciling items without reasonable explanations



Red Flags for Cash

- Second payee or unusual endorsements on checks
- Missing cancelled checks, bank statements and other advices
- Unusual disbursement transactions or transactions lacking sufficient supporting documentation
- Entity with the same initials (and address) as a payables employee.
- New vendor at higher price.
- Expense support is printout of order prior to actual placement.

Suggested Forensic Audit Procedures

- Prepare a Proof of Cash for the Year
- Reconcile receipt documentation to deposits
- Download Expenditures and Sort by:
 - Vendor Name
 - Largest Amounts
 - Look for Round Amounts
 - Look for Escalating Expenditures
 - Unusual EFTS/ACHs
- Confirm all accounts in government name with bank.

Payroll Fraud Red Flags

- Unusual or second-party endorsements on payroll checks.
- Employees without the usual withholdings related to employer provided or offered benefits (i.e., insurance, retirement, savings bonds, etc.).
- Missing, unusual looking, or altered time and attendance records in general or frequently for the same employee(s).
- Time and attendance records signed by someone other than the usual supervisor in general or frequently for the same employee(s).

Suggested Forensic Audit Procedures

- Download Master Employee File
- Sort information looking for:
 - Duplicate Information – Addresses, EFT/ACH Nos., Social Security Nos, addresses, etc.
 - Look for unusual addresses
- Download Annual Employee Earnings
 - Perform a Net Payroll Analysis Net/Gross sorted and looking for outliers
 - Look for Large O/T amounts, excessive or minimal withholdings etc.
- Pass Out Pay Checks

Accounts Receivable Frauds



- Lapping
- Posting improper credits
- Altering internal copies of invoices
- Unjustified credit being offered
- Fictitious refunds



A/R Red Flags

- Examples of red flags in A/R include:
 - Excessive number of voids, discounts and returns
 - Unauthorized bank account in a company name
 - Sudden activity in a dormant banking account
 - Customer receiving notices for non-payment on account
 - Discrepancies between bank deposits and posting to the account
 - Large number of write-offs of accounts

Suggested Forensic Audit Procedures

- Examine underlying documentation for Accounts Receivable
- Confirm activity not just balances with customers
- Look for delayed deposit of customer checks
- Confirm payment of accounts receivable placed with collection agency.
- Confirm all accounts with bank in government name.
- Look for unusual customer address/information

Inventories/Physical Assets

- Small in Size
- High in Value
- High in Consumer Demand
- Easily Convertible to Cash
- Lacking in Ownership Identification



Inventory Tells

- Significant Inventory Shrinkage
- Unusual inventory turnover
- Significant unusual or explained entries to control or subsidiary inventory records
- Significant unusual or unexpected relationships in inventory and inventory related ratios.
- Receiving reports differing from purchase orders, contracts, or vendor invoices.

Equipment/Physical Assets Subject to Personal Use

Equipment

- Cellular Phones
- Digital Cameras
- Computers
- Vehicles
- Tools

Physical Assets

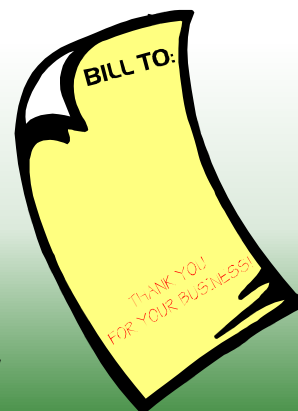
- Unused or out of the way buildings
- Vacant Land
- Obsolete Equipment
- Abandoned Assets

Suggested Forensic Audit Procedures

- Examine physical inventory and reconciliation process
- Review large asset purchases in inventory and/or capital assets
- Examine and/or individual significant capital items
- Review expense accounts for capital item purchases
- Examine disposition of retired and/or scrapped assets

Purchasing & Procurement Fraud

- Forming fictitious vendors
- Pass-through schemes
- Submitting false invoices
- Self-approval of fraudulent invoices
- “Rubber Stamp” supervisor approval
- Double-paying invoices
- Personal purchases through company



Suggested Forensic Audit Procedures

- Download Master Vendor File
- Sort by Address looking for:
 - Duplicate Addresses
 - Residential Addresses
 - P.O. Boxes
- Sort by Names looking for
 - Similar Sounding Names
 - Unusual Vendors
 - Initials of Individuals

Common Indicators

- Unusual vendor names and addresses.
- Copies of invoices, purchase orders, or receiving documents rather than original documentation.
- Orders for materials/supplies already on hand in sufficient quantities or that are scheduled for disposal/discontinued use due to obsolescence.
- Orders for materials/supplies not consistent with the operations and/or mission of the government or not-for-profit organization.
- Delivery addresses different than the purchaser's physical locations.
- Purchases falling just below the threshold for required next-level approval (in quantity or amount).

Common Indicators

- Split purchases using purchase orders, vendor invoices, change orders, etc.
- Payments to vendors not on approved vendor lists.
- Signature of management or supervisory personnel on documents typically signed by subordinate personnel.
- Supplier/contractors receiving significant amounts of business from the organization.
- Prices in excess of market or expected market especially when large quantities are ordered.
- Complaints from vendors/suppliers regarding not being allowed to bid, stringent bid specifications or procedures, or inadequate time allowed for responding to bid requests.

Common Indicators

- Contract award patterns that may indicate bids are being rotated.
- Low quality combined with high prices including high product failure/return rates.
- Sole source procurements in significant number or without adequate justification.



DETAIL ON A PURCHASING FRAUD SCHEME

Fictitious Vendor Schemes

- Most common fraud
- Commonly referred to as a “Shell Company” or just “Shell”
 - Insulates the bad guy
- Also used in corruption schemes, conflict of interest schemes, etc.



Shell Company Schemes: How They Work

- Organization will pay what appears to be a legitimate vendor
- The fraudster forms the Shell using another person's name as the owner ("straw man").
- Typically, the fraudster is in a position to:
 - Authorize the purchase of goods and/or services
 - Approve payment of the goods and/or services
 - Supervise employees who authorize and/or pay for the goods and services

Forming a Shell Company

- Articles of Incorporation –Sub S Corporation or LLC
- "Assumed Name Act" (or D/B/A) Certificate
- Partnership Agreement or LLP
- Or nothing at all



Ways Fraudsters Avoid Detection

- Use another person's name as the owner ("Straw Man")
- Use postal boxes, mail drops, shared offices
- Use their home address
- Use friends, relatives or accomplices



Shell Scheme Red Flags

- Invoice appears to have been hand-typed or from computer template.
- Incomplete vendor information in system.
- Vendor information same as employee information
- Invoice not folded.
- Company not listed in the phone book and has no Internet presence.



CASE STORY – ILLUSTRATE THE POINTS

Ben The Tax Accountant

- Ben was a tax accountant for a subsidiary of a \$7 billion corporation.
- Ben had been with the company for over 28 years – holding the same position after his first 18 months with the company.
- One day the company's General Manager received a call from the fraud unit of the company's bank.

Discovery

- The fraud unit representative told the General Manager that over the past several months the unit had been tracking some unusual deposit activity.
- Company checks payable to the bank in the amount of \$7,500 were being deposited into an account in the name of Emily's Boutique Store.

Discovery

- The General Manager knew that Emily was, in fact, Ben's wife.
- He then proceeded to call Ben to his office, wherein he accused Ben of theft of company funds.
- During the interrogation the General Manager discovered customer checks in Ben's briefcase.

Discovery

- The company found that checks allegedly used to pay a Diesel Fuel Tax were being diverted to Ben.
- An examination of the transactions revealed that the company's checks had been previously deposited into the company's C.O.D. Account.

Ben's Scheme

As Prepared by Accounting		Change	As Prepared by Ben
Cash	\$ 2,874.00	\$ (2,800.00)	\$ 74.00
CLG Const.	3,200.00	(3,200.00)	
B&M Concrete	1,000.00	(1,000.00)	
Woods Contractors	4,650.00		4,650.00
US Construction	500.00	(500.00)	
James Builders	2,750.00		2,750.00
Kyle's Konkrete	<u>1,380.00</u>		1,380.00
<i>Company Check</i>		<u>7,500.00</u>	<u>7,500.00</u>
Total	<u>\$16,354.00</u>	<u>\$ 0.00</u>	<u>\$16,354.00</u>

Profile of Ben

- Unexplainable wealth.
- Very few days taken off for sick or vacation time.
- Refusal to take a promotion.
- Unusual hours.
- Unusual story explaining his circumstances.



Contact Information

Craig L. Greene, CPA/CFF, CFE, MAFF, MCJ

McGovern & Greene LLP

200 W. Jackson Boulevard, Suite 2325

Chicago, Illinois 60606

(312) 692-1000

Office in Las Vegas

Craig.Greene@McGovernGreene.com