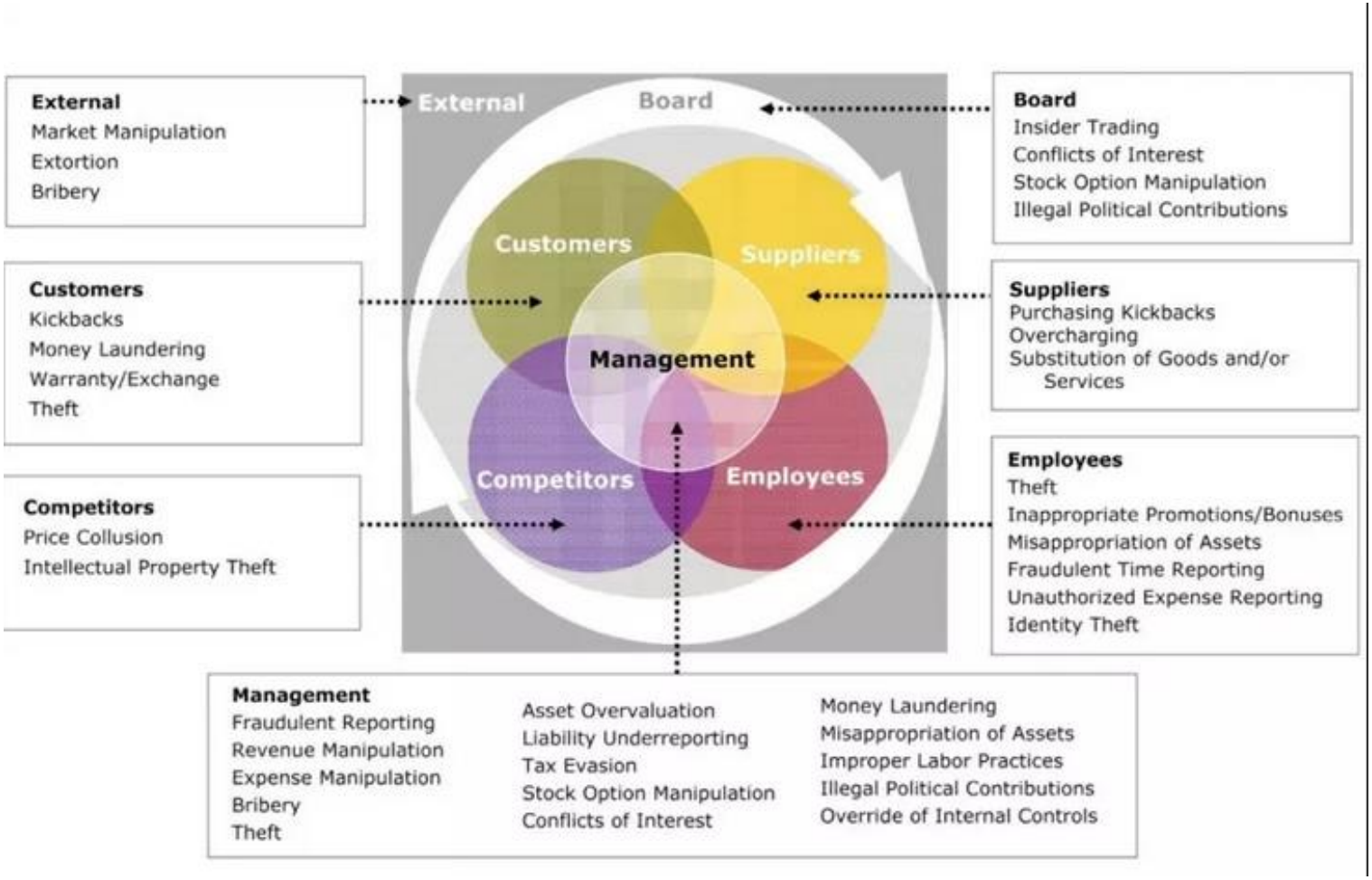
Fraud Detection: Red Flags and Targeted Risk Assessment

The Fraud Prompt

"If you make it easier for auditors by saying 'One of the symptoms of fraud is cognitive dissonance, so keep that in mind as you listen to this real-world recording of an earnings call with an executive and when you assess if there's deception,' that's where they're able to perform substantially better than chance at predicting fraud."

– Mark Peecher

The Fraud Risk Universe



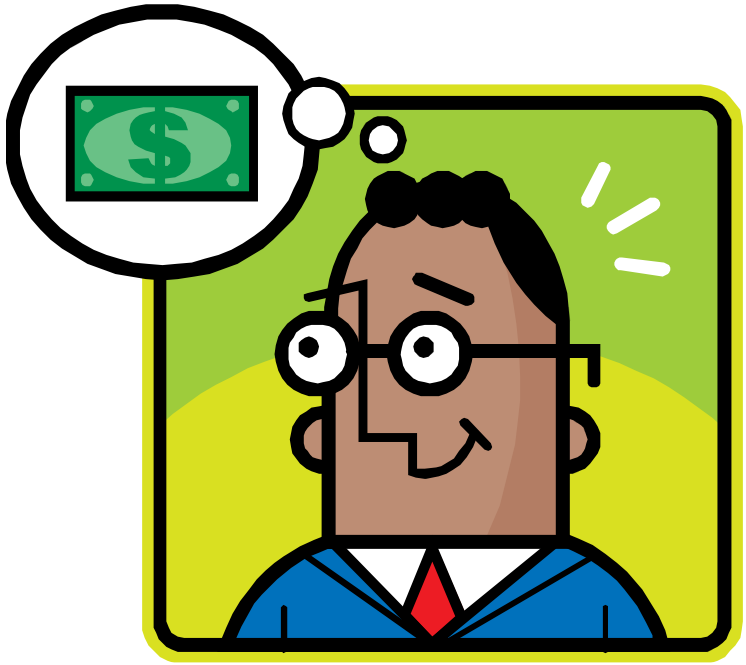
Organizational Governance and Fraud

- Management's Responsibility
  - The Risk of Management Override and Collusion
- The Role of the External Auditor
  - SAS No. 99
  - Materiality
  - Earnings Management and Fraud
- Boards of Directors & Audit Committees
- Internal Auditors

Management Responsibility

- Meet strategic, operational and performance objectives
- Measure performance
- Communicate results
- SAS No. 1
- Internal controls
- Fair representation of financial statements
- Provide information to independent auditors

The Risk of Management Override and Senior Management Collusion



- Internal controls can't control management override
- Prevention not possible in collusive environment
- Fear of detection

The Risk of Management Override and Senior Management Collusion

- 3 procedures to identify breakdowns in internal controls due to override and collusion
  - Journal entries recorded in the books and records
  - Review significant accounting estimates
  - Scrutinize “one-time” transactions

The Role of the External Auditor

- Reasonable assurance
- Material misstatement
- Analytical procedures
- "Expectations gap"
- Attest fairness of management's presentation of financial information
- Audit report

The Role of the External Auditor

Types of audit opinions

- Unqualified
  - Explanatory paragraph
- Qualified
- Disclaimer
- Adverse

Statement on Auditing Standards (SAS) No. 99/No. 113

- Consideration of Fraud in a Financial Statement Audit
  - Enhanced professional skepticism
  - Pre-audit fraud brainstorming
  - Interviews with management
  - Audit test design
- Intent

Statement on Auditing Standards (SAS)

Nos. 99 and 113

8 steps in considering the risk of fraud

1. Staff discussion
2. Obtain information needed to identify risks
3. Identify risks
4. Assess identified risks and potential schemes after considering internal controls
5. Respond to the result of the risk assessment
6. Evaluate the audit evidence
7. Communicate about fraud
8. Document procedures undertaken in steps 1 to 7

Materiality

- FASB 2 definition
- Auditor must apply judgment
- Materiality is a relative concept
- Illegal acts have no materiality threshold
- Qualitative versus quantitative aspects
- SAS No. 111 limits tolerable misstatement

Determining Materiality: Relativity and Professional Judgment

- Judgment and Expectations
  - Anticipate potential readers of information
  - Public expects CPA to be a financial cop
- The Problem with Quantification
  - Auditing Standard No. 5
  - Focus on minutiae when assessing risk
  - Encourages consistency
  - Doesn't provide quantitative value

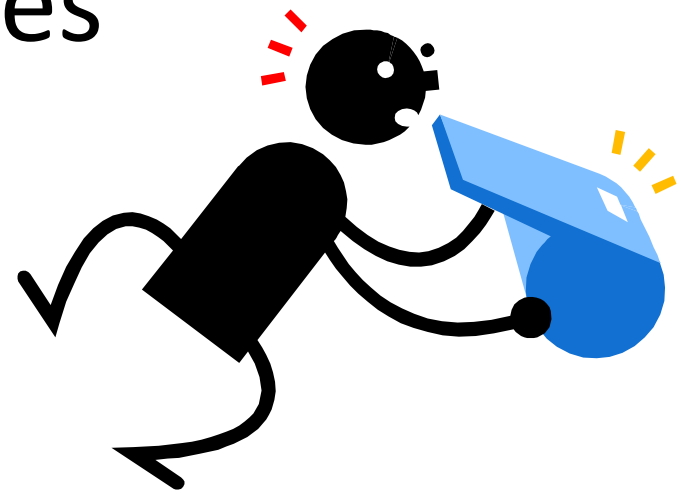
Earnings Management and Fraud

- Deliberate actions by management to meet specific earnings objectives for private gain
- Materiality threshold
- Accounting principles and policies provide some-degree of choice
- May lead to fraud
- Clear and convincing evidence

Boards of Directors and Audit Committees

- Primary responsibility
  - oversee management
  - direct internal audit
  - direct external auditor
- Internal controls over financial reporting and the company's internal control processes
- Assure - management has adequately assessed the risk of management override or collusion among top-level managers and executives

Boards of Directors and Audit Committees



- "tone at the top"
- Anti-fraud programs
- Ethics training
- Instituting a zero tolerance policy toward fraud
- Proactively investigate whistleblower tips
- Protect whistleblowers

Fraudster's Perspective

- "Packaged" and "process oriented audits"
  - "Fill in the blanks"
  - "Check the boxes"
- Many audit committee members receive compensation in stock options
- Audit Committees not prepared
  - Many members lack proper background

Internal Auditors

- Increased perception that fraud perpetrators will be detected
- Operations
  - Evaluate segment, product line and division profitability
  - Improve internal productivity
- Financial reporting
  - Evaluation of internal controls
- Institute of Internal Auditors (IIA)
- Statement on Internal Auditing Standards (SIAS) No. 3

Fraud Detection

- Go beyond mere existence of documents
- Sheer size of fraud often brings “house of cards” down
- Internal control environment has been violated or circumvented
- Professional skepticism
- Possibility of concealment
- 2 major approaches to fraud detection
  - Identification of red flags
  - Targeted risk assessment

Social Media as a Tool for Fraud Detection

- Big data analysis using text sources, such as social media, shows promise for improving fraud detection efforts.

Understanding the Business

- Understand the organization and the environment in which it operates
- Assessment of the industry
  - Is organization following trends?
- Comparison of competitors
- Evaluation of trends within an organization
  - Horizontal
  - Vertical

The Internal Control Environment

1. Commitment to integrity and ethical and core values
2. Commitment to competence
3. An independent board of directors and audit committee that participates in the internal control processes and oversees the process
4. Management's attitudes, philosophy and operating style concerning important internal controls and operational issues
5. Organizational structure, including lines of responsibility and authority, particularly as it relates to the control environment and operational expectations
6. Communications about the importance of control-related matters, ethics, anti-fraud awareness and commitment, organizational and operating plans, employee job descriptions and related policies
7. Human resource policies and practices

The Use of Red Flags to Detect Fraud

- Does the anomaly have supporting documentation?
- Does the documentation appear to be falsified, altered, or fictitious?
- Does the transaction and its reflection in the financial statements make sense?
- Does the transaction make sense in light of the company's operations, goals and objectives?
- Does the totality of this and similar transactions make sense analytically when evaluated in comparison to the economy, the industry, key competitors and other related accounting numbers within the organization?
- Does the transaction have proper approval and the proper authority levels?
- Does anything else about the transactions or its nature make it appear suspicious?

Tips and Complaints

2022 ACFE Report to the Nations

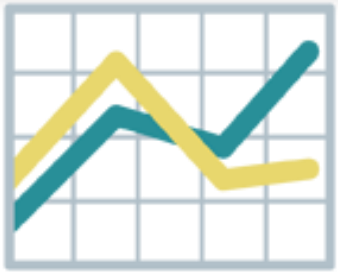
- Tips most common detection method
- Stark variation between small & large organizations regarding fraud detection via tips
  - 47% of frauds detected by tips in small orgs
  - 56% of frauds detected by tips in large orgs
- Tips and accidental discovery, combined, account for >50% of all frauds detected

Tips and Complaints (cont'd)

- Many times, tips and complaints are false.
- Employees may not report for fear of getting someone in trouble
- Whistleblower or fraud hotline
  - Easy and anonymous
  - Tipster must provide sufficient detail

Behavioral Red Flags

- Lifestyle symptoms
  - Living outside of means
  - Easy to observe
- Unusual behaviors
  - Fear causes fraudster to act differently
  - Stress changes fraudster's behavior
  - Difficult to discover fraud from these clues alone
  - Should be combined with other red flags



Analytical Anomalies

- Transaction or financial statement relationships that do not make sense
- Transactions that are too small or too large when compared to normal activity
- Patterns or breaks in patterns
- Analytical anomalies are common and should be pursued until fraud is discovered or ruled out

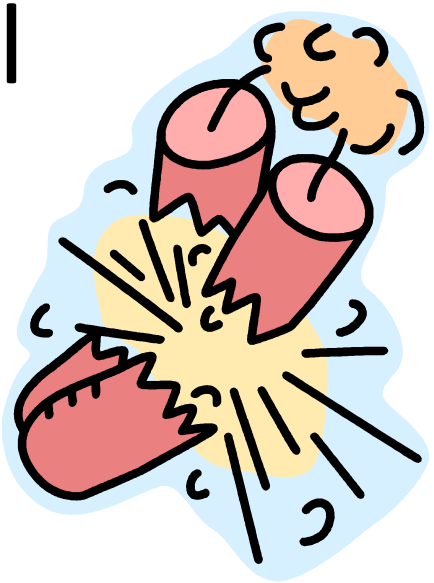
Accounting Anomalies

- Unusual activities that seem to violate normal expectations for the accounting system
- Irregular or undocumented journal entries
  - Entries that reduce liability while simultaneously increasing a revenue account should be red flagged
  - Unusual or problematic entries should be closely scrutinized
- "Cooking the books"

Internal Control Irregularities and Weaknesses

- Internal controls should prevent, deter and detect fraud
- Normal internal control environment
  - Adequate separation of duties
  - Proper authorization of transactions and activities
  - Adequate documents and records
  - Physical control over assets and records
  - Independent checks on performance

The Power of Non-financial Numbers



- Make use of data from surrounding operational systems
- Break sums down to quantity and prices
- Correlate with numbers represented in financial statements and tax returns
  - Start with data generated outside of financial accounting system

Using Red Flags as a Basis for Further Investigation

- Each fraud has unique attributes
- Consider red flags in context of the circumstances
- What causes transaction to seem unusual or irregular?
- Use evidence to develop other reasons for the suspicious activity
- Consider possible motivations of who might be involved

Evidence-Based Decision Making & Documentation

Each of the following should be considered:

- The Elements of Fraud

✓ Are cash or other assets missing (i.e., has a fraud act or financial crime possibly been committed)?

✓ Are the financial statements materially misstated?

✓ What are the concealment possibilities?

✓ What are the conversion possibilities and have any conversion symptoms (e.g., lifestyle anomalies) been observed?

Evidence-Based Decision Making & Documentation (cont'd)

- The Fraud Triangle

✓ Which individuals have opportunity?

- ❖What are the key internal controls in this area?
- ❖Are key internal controls deficient or have they been violated?

✓ Have any individuals demonstrated signs of pressure?

✓ What potential rationalizations might be offered and is there any evidence of rationalization by particular individuals?

Evidence-Based Decision Making & Documentation (cont'd)

- M.I.C.E.
  - ✓ What might motivate the fraudster: money, ideology, coercion, or ego/entitlement?
- Other considerations
  - ✓ What are the most promising investigative techniques?
  - ✓ What methods and approaches will most likely result in a successful investigation?
  - ✓ Have any other related symptoms been observed?
  - ✓ How do the red flags observed in one area relate to red flags observed elsewhere?

Targeted Fraud Risk Assessment

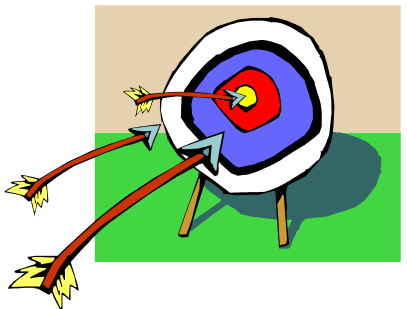
1. Identify, understand and evaluate the company's operating environment and the pressures that exist
2. Identify the business processes and consider differences in those processes
3. Identify the "process owner" for each of the identified significant processes
4. Review past fraud experience within the company for the process being evaluated
5. Identify how fraud may occur in each process and at each location using brainstorming techniques

Targeted Fraud Risk Assessment

6. Identify the parties who have the ability to commit the potential fraud
7. Evaluate the likelihood that each of the identified frauds could occur and be significant as well as the persuasiveness of the potential fraud without consideration of controls
8. Consider the likely methodology to commit and conceal the fraud to determine the level of mitigation to prevent, detect, and deter the fraud
9. Investigate the characteristics of potential fraud manifestations within each process identified
10. Remediate fraud risk schemes by designing control activities to mitigate the unmitigated fraud scheme risk

Targeted Fraud Risk Assessment in a Digital Environment

- Electronic environment captures millions of transactions annually
- Targeted risk assessment process yields highest probability of frauds
- Computer aided auditing tools and techniques (CAATT) to prevent and deter fraud
  - Data extraction
  - Analysis



Digital Evidence

- Information is captured electronically and is available to monitor fraudster's activities
- Electronic storage is relatively inexpensive
- Fraudster risks detection during the fraud act and as long as the data is stored
- Stored data can be used to
  - Trace transactions
  - Document approvals and exceptions
  - Provide evidence of system override

Detection and Investigation in a Digital Environment

- Value of information systems
  - Generate red flags for further investigation
  - Reconstruct actual data flow
  - Provide strong evidence trail
- Potential for overwhelming number of fraud symptoms
- Targeted approach
  - Must have sense of what could or did go wrong
  - How might it manifest itself in the information systems

Reference & Contact

- Forensics Accounting and Fraud Examination 2nd edition Mary-Jo Kranacher & Richard Riley

  2019 / John Wiley & Sons, Inc.

- https://www.nacva.com/search.asp?type=basic&keywords=knott&search=

  Volume 13: Issue 2, July-December 2021

  Volume 14: Issue 1, January-June 2022

Cedric Knott, Ph.D., CFE

clknott@wayne.edu

313-401-1906

Any Questions?

Thank You

Executive & Professional Development
(313) 577-4665
www.ExecEd.wayne.edu

These Weights Didn't Measure Up!

By Joseph R. Dervaes

Richard Langley was a party-hearty political activist in his community. As a rising political star, he worked on voter registration projects and was the campaign manager for an unsuccessful gambling initiative. He also made donations to many political campaigns in the state.

Richard was a self-promoter who loved to name-drop. Known as a high roller, he threw large and lavish parties at his rented home on a lake near a major metropolitan city. Richard frequently entertained judges, mayors, ex-governors. lawyers, and councilpersons at his home. Valet service was provided for all who attended these gala events. Once inside, guests enjoyed the extensive display of autographed sport memorabilia that adorned the walls of his elegant home. But the primary purpose of these events was to provide a forum for the principal dignitaries to network with other participating in political activities.

When Richard needed money to fuel his extravagant lifestyle, he first formed a trucking business. Over time, he used his political contacts to secure a lucrative freight contract the state's liquor control agency, referred to as simply the Agency. The Agency's decision to hire Richard as a contractor remains a mystery to this day. When examined later, his contract file was found to be unimpressive and practically empty. Of the two records in the file, one was a memorandum by a staff member indicating Richard had dropped the name of an agency executive when he first approached them for a job. The other letter of resignation. The Agency selected Richard as a contract vendor for one of its 14 liquor delivery routes.

Upon accepting the contract, Richard did not know how to complete invoices to be paid promptly, as he lacked accounting skills. The remedy this condition, he began to cultivate a relationship with Gerry Sparkle, an employee in the Accounts Payable (AP) Department at the Agency. She had been a fiscal technician at the company for five years. Gerry was 42-year-old single mother with two teenage children. She had just ended a relationship with her domestic partner of four years. Due to her personal life and poor financial situation, she was vulnerable. Financial security was a major concern in her life, but the reality of being alone again scared her even more.

The AP Department was located at the Agency's headquarters in the state capital. One of Gerry's jobs was to process invoices for freight vendors that delivered liquor products in the statewide distribution system. It was a time-consuming job that involved processing about 1,400 invoices totaling $420,000 in payments every month. After Richard was hired as a contractor, she was required to process his invoices, as well. Invoices were first batched for review and approval. The data were then entered into the computer accounting system. Finally, invoices were processed for payment. While performing these duties, Gerry was required to verify information from vendor invoices to the Agency's computer database for all freight shipments from the central warehouse.

Richard pleaded for help. Gerry decided that it would be easier to prepare his invoices herself rather than to fix them every time. They agreed to change procedures. Richard provided her with the freight transaction information. Gerry prepared his invoices, which allowed her to spend less time working on the accuracy of the transactions, and Richard began receiving his payments more promptly. Even with Gerry's help, things began to go away. One of Richard's payments was lost in the mail. Another payment was mailed to the wrong company.

When Gerry was transferred to another department, she continued to help Richard prepare invoices. Once her review had been completed, she gave the invoices to the AP staff for further processing. Since she had already verified the information, the staff simply entered the information into the computer accounting system using their own password.

It wasn't long before Richard began to exploit his relationship with Gerry for his own personal and business advantage. Ultimately, he conducted a scheme to defraud the state of almost $840,000 over a three-year period. Gerry got wind of Richards' inappropriate activities and begged him to stop.
"I will, eventually," he promised. "If you get fired because of my actions, I'll pay for a defense attorney for you, give you a job at my firm, and provide for your needs during the ordeal." The meeting ended abruptly. Gerry did nothing further to disclose Richard's scheme to the Agency's officials.

Gerry was devastated. She decided to determine the extent of Richard's fraudulent billing scheme. Gerry knew he was supposed to make about $144,000 per year but soon found that he had been paid about $685,000 in 2001. Horrified, she knew now that she would have to become a whistle-blower and report Richard's activities to the Agency. She decided to meet with him one more time to resolve the matter. At the meeting, she was surprised to be met by Richard and his attorney.

"I'll hire an attorney for you, too, if the Agency finds out what we've been doing," he promised.

BAD PAPER

Richard's firm submitted false invoices to the Agency and received unauthorized payments for services he did not provide. He received $839,706.90 in unauthorized payments during the three-year period. The fraudulent transactions are summarized next:

Inflated weights on legitimate deliveries	$123,161.12
Deliveries that did not occur	$600,527.84
Double billings	$116,017.94
Total losses	$839,706.90
Unbilled legitimate deliveries	($67,843.31)
Net loss	$771,863.59

1. Inflated weights on legitimate deliveries. Payment for deliveries was determined by multiplying the weight of the freight load by the rate established in a contract between the Agency and all freight vendors. Richard made 1,103 freight deliveries during the audit period. He inflated 600 of these deliveries by over 5,000 pounds (i. e., 54.39% of all deliveries).
2. Deliveries that did not occur. Richard submitted 1,100 invoices reporting 1,370 deliveries that never occurred.
3. Double billings. Richard submitted 238 invoices requesting payment for 273 deliveries that had been previously billed to and paid by the Agency.
4. Unbilled legitimate deliveries. Richard did not bill the Agency for 382 legitimate deliveries valued at $67,843.31. The auditors gave him credit for this oversight, thus reducing the total loss.

Richard sent invoices to the Agency for transactions totaling $1,100,000 during his five years as an employee. Almost 76% of these invoices were bogus. When the state patrol visited Richard's home to arrest him, he had already fled the state to avoid prosecution. Since this was such an outrageous crime, the state formed a regional fugitive apprehension task force to track him down. Richard remained on the lam for six months. Acting on a tip, United States marshals traveled to another state and arrested him without incident at a friend's home. He was temporarily held in a county jail. After he waived extradition, he was escorted back to his home state and placed in jail to await the trial. "Richard doesn't have anything left but memories. He's penniless. The proceeds from the scheme have been squandered," the county prosecutor declared.

LESSONS LEARNED

At the completion of this case, the auditors learned a great deal about fraudulent billing schemes. In the future, managers will look for a "straight line" from the initiator requesting payment for the transaction, to accounts payable for review and production of the checks, and then to the individual making distribution of the checks. The risk of fraud increases when a check from any transaction makes a U-turn in the AP or Check Distribution department and is returned to the initiator. These transactions automatically become exceptions to the internal control structure and require intense scrutiny and monitoring by managers. Any compromise of the AP system will now be documented on a manual exception log to identify all transactions that have been processed outside normal parameters. These compromises include the use of any type of written communication, including Post-it Notes, or any verbal communications. employees make with the accounts payable or check distribution staff. It also includes picking up checks after issuance when it is not the organization's normal procedure.

What are recommendations to prevent future occurrences?

Source:

Wells, J. T, (2007), Fraud Casebook Lessons from the Bad Side of Business, pages 624, John Wiley & Sons, Hoboken, New Jersey, ISBN: 978-0-470-13468-9