When the Office is the Crime Scene

Margie Reinhart, CPA, CFE
Forensic/Strategic Solutions, PC
Plaza of the Americas
600 North Pearl Street, Suite 2255
Dallas, Texas 75201

The Mystery Novel

• Happy ending – properly structured investigation
• Investigation and remedial action
• Balance employer/employee rights
• 10 considerations

1. Act Quickly
• Dishonesty rarely caught by direct observation
• Schemes likely ongoing
• Financial impact may be material—most likely be more than first suspected
• The employer must move quickly to stop the damage

2. Hire Professional Help
• Attorney who has practiced in this area
• Law firms have white collar crime group
• Coordinate internal & external investigators
• Significant risk to mishandle case
• 2nd loss most painful

Hire Professional Help
• Forensic accountant should be independent
• Yellow tape the crime scene
  – No computer searches
  – No office search
• Preserve incriminating evidence
• Chance of recovery increases dramatically

3. Develop Investigation Plan
• Fraud investigation complex undertaking
• Success sensitive to documentation
• Proper plan will do following:
  – Maximizes efficiency
  – Ensures important steps of the investigation are not overlooked
• Documents compliance with professional standards (e.g. planning, supervision and due professional care)
• Speeds completion of written report at the close of investigation
• Allows the fraud examiner to recall pertinent details of the work at a later date
• Allows greater efficiency on future assignments as a reminder of what works and what did not

Follow Steps of Typical Fraud investigation

• Document examination & computer forensic exam
• Interview neutral, third-party witnesses
• Interview corroborative witnesses
• Interview co-conspirators
• Interview suspect

4. Secure Data & Work Area

• Mirror hard drives of computer used by employee
• Mirror hard drive of server in a network
• Secure copies of all electronic backups
• Secure original data

• Cd’s and thumb drives used to keep selected data off hard drives
• Search desk and office
• Once notified not allowed to touch computers or remove anything other than personal items from office
• Home computer
• Remote access
• Emails and deleted files are wonderful

5. Contact Insurer

• Failure to put insurer on notice can/will void coverage
  – 30 to 60 day notice provision
  – Earlier crime not reported
• Many policies pay investigative costs
  – Approved vendor list?
• Proof of Loss
  – Months after notification
  – Problems with FBI/USA determinations
• Statute of Limitations

6. Deal with “Alleged” Perpetrator

Three courses of action possible
1. Terminate the employee immediately
  – Owners usual preference
2. Place the employee on administrative leave with or without pay
  – Refer to employment agreement
  – Refer to company policy
  – Sufficient predication before action
3. Do not confront the employee until evidence developed
  – Hook the fish and let him swim around
  – Employee’s duty to cooperate
  – Interviews to confront fraudster
Care Is Important

- Avoid exposure to defamation claims
- Was a crime really committed?
- Incompetence may appear to be criminal
- Fraudster may hide behind cloak of incompetence
- Avoid disclosure

7. Know Employer’s Rights and Responsibilities

- Employer has a right to conduct a fraud investigation
  - May be required to investigate
- Actions taken by employer consistently applied to all employees
- Management has responsibility to the stockholders to investigate and seek to recover losses by theft
- May be required to report to agencies

8. Know Employee’s Rights and Responsibilities

- Employee has certain rights to privacy
  - Fair Credit Reporting Act
  - Employee Polygraph Protection Act
- Always read employee handbook
- An employee has the right to sue their employer under certain circumstances
  - Fourth Amendment (unreasonable searches)
  - Fifth Amendment (incrimination)
  - Sixth Amendment (attorney)

State Actions

- Investigations conducted by a private company that are required by state or federal law
- Searches or interrogations conducted by outside investigators who are off-duty state, local or federal authorities
- Sarbanes-Oxley?

9. Perform Background Checks of Suspect

- Background checks and credit checks are a powerful tool
- They allow and can prove identification of “need” and “greed”
- Fair Credit Reporting Act concerns

10. Look for Other Schemes

- Be open – others may be involved in the fraud scheme
- Collusion with others within or outside of the organization
- Any employee with the authority to approve payment of an invoice can perpetrate a scheme
- The admitted fraud likely follows the 10% rule
Conclusion

- Don’t destroy evidence
- This means computer data as well as hard copies
- Failure to preserve may make you just as liable
- Destruction of evidence can lead to
  - Obstruction of justice
  - Conspiracy
- Convictions – prison

Conclusion

- Investigations provide opportunity to assist company and help prevent future instances
- Some recommended areas may involve:
  - Review hiring policies
  - Restrict access to employee master files
  - Restrict access to vendor master files

Conclusion

- Separate the cash/banking function from the accounts receivable function
- Protect check stock and destroy obsolete stock
- Mail vendor checks
- Reconcile bank accounts on a timely basis
  - UCC section 7-4-406
- Rotate personnel or functions in critical financial areas on a regular basis

Recovery of Money and/or Getting a Pound of Flesh

- Most cases – $ gone
- Court ordered restitution
- Civil judgment
- Referral to law enforcement
  - Federal, state, local
  - IRS

Thank you!

Margie Reinhart, CPA/ABV, CFE, CIRA
Forensic/Strategic Solutions, PC
Plaza of the Americas
600 North Pearl Street, Suite 2255
Dallas, Texas 75201

www.forensicstrategic.com