Compliance Investigations

Lessons from the Trenches

February 12, 2019

Gerry Zack, CCEP, CFE, CIA

CEO

Society of Corporate Compliance and Ethics

Minneapolis, MN, United States

gerry.zack@corporatecompliance.org

An Improperly Performed Investigation Creates More Risk Than it Mitigates
Today’s Agenda

1. Initial phases of an investigation
   • Scoping and risk assessment
   • Key steps in commencing an investigation
2. Use of third parties to assist with investigations
   • Under what circumstances
   • How to manage
3. Collection and use of data and other digital evidence
   • Types of digital evidence
   • Methods and tools used for collection
   • Use of forensic analytics

PART 1

The Initial Stages of an Investigation
What Triggered the Investigation?

- Allegation/tip
  - Anonymous v. known
  - Internal v. third party
  - Level of specificity
- Internal audit
- Other auditing/monitoring activity
- External process (government auditors, etc)
- How serious is the alleged or possible act?
  - Escalation issues?

Allegations

- Perform preliminary assessment to determine whether an investigation is warranted
- Consider whether it is necessary to perform without subject’s knowledge Covert v Overt
- Data analytics
  - Consider this – If the allegation is true, what impact would the act have on electronic data? How would the digital trail of the act differ from that of a valid transaction or act?
  - Data analytics is often the most practical method of establishing credibility of an allegation
- Document analysis
  - Look for red flags, characteristics that support or refute the allegation
What Next?

- What type of compliance issue?
  - Bribery, conflict of interest, employee theft, fraud, privacy, data breach, environmental, financial reporting fraud, etc

- What level within the organization is implicated?

**Possible next steps:**
- If there is an allegation, assess credibility
- Notify/engage legal counsel
- Assemble team; Determine who investigates
- Is subject currently employed with us?
  - Consider whether it is necessary to investigate without subject’s knowledge

Scope Considerations

- How specific/vague is the allegation or concern/red flag?
- Could additional individuals be involved?
  - Internal
  - Third parties (individuals or organizations)
- What other acts could the subject(s) have perpetrated?
  - Very common that if someone is engaged in wrongdoing, there are multiple schemes/acts
  - Perform role-based risk assessment
- How far back might the activity have been occurring?
- Are violations/losses potentially still occurring?
- How likely is it that other individuals may have witnessed the alleged wrongdoing?
What are the Goals of the Investigation?

• Terminate employee?
• Stop the bleeding?
• Civil litigation to recover damages?
• Refer for criminal prosecution?
• Keep it quiet?

Goals as Compliance Professionals

• Investigate processes, not people
• Ultimate goal is to find and fix the problem
Identifying Records & Data Needed

- Develop process map of the transaction/activity cycle(s) involved in the target of the investigation
  - MUST understand how the transaction cycle operates in order to identify relevant records/people needed
- Based on this process map, identify:
  - People involved in each step
  - Internal controls
    - Preventive
    - Detective
  - Documents and forms
    - Received
    - Created
  - Electronic records
  - Systems and databases affected

Example – For corruption in the purchasing cycle:
- Identification and documentation of need
- Development of specifications, if necessary
- Solicitation of bids or negotiation with alternative vendors
- Selection of vendor
- Contract, statement(s) of work, etc
- Purchase orders
- Change orders, subcontracts, etc
- Receipt of goods or services
- Submission, review and approval of invoice
- Payment
- In addition, what other internal records would we expect along the way? E-mails, electronic approvals, etc.
PART 2

Use of Third Parties to Assist with Investigations

Why Use Third Party Assistance?

- Independence
- Specialized Expertise
- Capacity or Geographic Reach
When/Why Use Third Parties?

• **Independence**
  • For example, certain investigations of C-level execs, board members, etc
  • Relationships – family, financial, etc
  • Past history with subject/department

  • Appearance/reputation also matters, not just independence in fact
  • Certain critical/public investigations
  • However, make sure the third party is independent
  • In larger organizations and larger third party firms, this isn’t always obvious
  • Independence checks should be performed

When/Why Use Third Parties?

• **Specialized expertise**
  • eDiscovery
  • Data extraction and analytics
  • Case management
  • Interviewing
  • Subject matter expertise (e.g. accounting fraud, )
When/Why Use Third Parties?

• **Capacity or geographic reach**
  • We have talented people, but not enough time
  • Remote location, impractical for us to investigate

Policy Consideration

• Among the policies that should be in place pertaining to investigations, the issue of when to use third parties should be included
  • Authority to hire third parties
  • Under which circumstances
Understanding the Goals

- What are the goals of the investigation?
  - Determine who did it?
  - Determine how they did it?
  - Determine damages?
  - Terminate guilty employees?
  - Take legal action to recover?
  - Criminal charges?
  - Minimize organizational liability?
- This may drive some of the decisions surrounding the use of outside experts

Outside Experts – Two Types

- Consulting experts
- Testifying experts

  - Subject to U.S. Federal Rule of Evidence 702 and Daubert challenge - A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
    a) The expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
    b) The testimony is based on sufficient facts or data;
    c) The testimony is the product of reliable principles and methods; and
    d) The expert has reliably applied the principles and methods to the facts of the case
Using Third Parties – Engagement Phase

- Key issues before engaging:
  - Background check
    - Firm
    - Individuals working on your engagement
  - Clarification of scope
  - Fee structure (fixed price, hourly, etc)
  - Engagement letter, proposal, professional standards

Third Parties & Privilege

- Use of third party consultants, retained by legal counsel, reinforces privileged status of investigation
  - Underscores that investigation not a routine business function
  - Facilitates legal counsel control of third parties’ work product
  - Controls distribution of third parties’ work product to protect privileged information
Privilege Issues with Third Parties

- Keeping legal counsel “in the loop” with third party consultants
- Risk of waiving privileges when third party consultants communicate exclusively with non-lawyers
- Third party consultants using subcontractors

Using Third Parties – Work Phase

- How should you deal with each of the following key issues?
  - Introduction, integrating into the “team”
  - Supervision of third party contractors
  - Responsibility for their work product
  - Third parties communicating with third parties
  - Managing the investigation
  - Scope creep
  - Reports from outside experts
  - Closeout of engagement
PART 3

Use of Digital Evidence
And Data Analytics

Preserving/Collecting Electronic Evidence

- Issue a document/record hold notice based on process map explained earlier
  - Identify relevant records
  - Identify relevant record custodians (may include third parties, cloud storage, etc)
- Negative implications of information being lost/altered
- ESI (electronically stored information):
  - What ESI is relevant?
  - What format is it in?
  - Where is relevant ESI stored?
  - How do we ensure we collect it all?
  - Proper collection (use forensically recognized technologies)
Tools

• Forensic imaging
• Hand-held devices
• eDiscovery
• Link analysis
• Data analytics
• Graphic depiction of data

Uses of Data Analytics & Forensic Tools

• To assess credibility of an allegation or concern
• To determine which documents and records should be inspected
• To identify additional individuals who may have been involved
• To prioritize or identify suspect transactions
• To determine where internal controls broke down or were intentionally violated
• To assess whether noncompliance was intentional or accidental
• To estimate the full extent of the problem
Data Analytics to Assess the Allegation

- Data analytics can be used to assess the credibility of an allegation, helping to determine whether to launch an investigation.
- If the allegation is true:
  - What data would be created or touched in the processes involved?
  - How would characteristics of the data associated with noncompliant activities differ from data involved with compliant activities?
  - Perform data analytics to see if these characteristics are present, consistent with noncompliant activity.
  - Data analytics does not prove fraud, corruption, noncompliance, etc; But it can provide evidence of characteristics that are consistent with such improper activity.

Framework for Using Data Analytics

- Which data is affected, and how, in each stage of a compliance issue:
  - Preventive control that should have prevented the act
  - Perpetration/violation - the act itself
  - Concealment – is often separate from the act itself
  - Detective control that should have detected the act
  - Effects of the act (if any)
- How would data associated with an improper transaction/activity differ from that of a legitimate one?
QUESTIONS ??

Gerry Zack, CCEP, CFE
CEO
Society of Corporate Compliance and Ethics
Tel:  +1 952.567.6215
gerry.zack@corporatecompliance.org