Use of Forensic Data Analytics in Investigations

Gerry Zack, CCEP, CFE, CIA
CEO
SCCE & HCCA
Minneapolis, MN
gerry.zack@corporatecompliance.org

Today’s Agenda
1. A framework for using analytics in compliance investigations
2. Effective design of forensic data analytics
3. What next? Following up on what the analytics tells us
Applications of Analytics

• Three most common applications of data analytics in connection with compliance:
  1. As a monitoring activity
     • Most common use
  2. In response to an allegation
     • To assess credibility of an allegation
  3. As part of an investigation
     • Determine extent of noncompliance
     • Extrapolate findings
     • Identify co-conspirators

PART 1

A Framework for the Use of Data Analytics
The Data Analysis Process

Planning   | Design   | Testing  | Analysis

Framework for Using Data Analytics

• Which data is affected, and how, in each stage of a compliance issue:
  1. Preventive control that should have prevented the act
  2. Perpetration or noncompliance event - the act itself
     • Intentional
     • Unintentional
  3. Concealment – often separate step(s) from the act itself
  4. Detective control that should have detected the act
  5. Effects of the act (if any)
Framework for Using Data Analytics

• Focus on all five elements helps to:
  • Determine who was involved – co-conspirators, etc
  • Identify which controls broke down or were violated
  • Assess whether any key controls were missing or improperly designed
  • Map exactly how the subject did what they did
  • Prove intent
  • Develop a timeline
  • Assess damages to the organization
  • Prepare root cause analysis
  • Develop corrective action plan

Types of Data

**Structured**
- Accounting/financial
- Inventory
- Sales/purchases
- Payroll/H.R./timekeeping
- Security
- Customer service
- System access/use
- Travel, asset use, etc

**Unstructured**
- Journal entry explanations
- Purchase descriptions
- P.O. explanations
- Variance explanations
- E-mails, IMs, etc
- Photo, video, audio files
The Devil’s in the Data

• When fraud or corruption is involved, concealment leaves a digital trail:
  • Deleting electronic records
  • Altering electronic records
  • Adding electronic records
• Sometimes, unintentional noncompliance still leads to concealment
• Don’t overlook “the curious incident of the dog in the night-time”
  • Sometimes the lack of a record is important

Commonly Used Functions

• Aging
• Duplicate searches
• Filter, sort, stratify
• Compliance verification
• Frequently used values
• Join and relate (two sources of data)
• Gap tests
• Unusual times or dates
• Trend analysis
• Regression/correlation
• Text analytics
PART 2

Effective Design of Data Analytics

Identifying Records and Data Needed

- Develop process map of the transaction/activity cycle(s) involved in the area under 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
Identifying Records and Data Needed

- **Example** – For alleged 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.

---

Example Data Sources: Bribery Payment Schemes

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>USES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor master file</td>
<td>Identifies all approved vendors</td>
</tr>
<tr>
<td>Accounts payable ledger</td>
<td>Lists when and to whom payments are due</td>
</tr>
<tr>
<td>Cash disbursements journal</td>
<td>Lists all cash disbursements</td>
</tr>
<tr>
<td>Purchases journal</td>
<td>Reports requests for purchases</td>
</tr>
<tr>
<td>Selected GL accounts</td>
<td>Identifies accounts where payment of a bribe could be hidden</td>
</tr>
<tr>
<td>• Charity/donations</td>
<td></td>
</tr>
<tr>
<td>• Agent/consulting payments</td>
<td></td>
</tr>
<tr>
<td>• Marketing expenses</td>
<td></td>
</tr>
<tr>
<td>Travel and entertainment</td>
<td>Itemized T&amp;E submissions</td>
</tr>
</tbody>
</table>
Go Back to the Framework

• What data is involved in each of the following, and how would an improper transaction differ from a proper one:
  1. Preventive control that should have prevented the act
  2. Perpetration or noncompliance event - the act itself
  3. Concealment
  4. Detective control that should have detected the act
  5. Effects of the act (if any)

Example

• Allegation – that a controller was submitting and being reimbursed for personal travel and other expenses
• First step – learn the process for how expense reports are processed for the organization
• Identify relevant data to confirm understanding and to capture population of data to analyze
• The results:
  • Pulled data for all expense reports for a period of time
  • Noticed an anomaly associated with the subject’s expense reports
    • Every expense report was input by one of two people (based on User IDs) except for the subject, whose reports were processed by someone else
  • Led to a deeper dive of both employees’ time and expense reports
The Results

- The other employee had access to the A/P system used to process expense reports
- The other employee was in collusion with the controller
- Since the other employee also was involved in the payroll function, we analyzed payroll data
- Found that the two employees also perpetrated a payroll fraud that was much bigger than the expense reimbursement fraud

Group Discussion

- **Allegation**: That our company is improperly billing a government agency by (1) charging for certain products we did not deliver and (2) misclassifying certain services provided to the government in order to charge at a higher rate than the contract would allow.
- Using the 5-part process introduced earlier, how might data analytics be used to show:
  - Break-down of a detective control
  - Commission of the act
  - Concealment of the act
  - Break-down of a detective control
  - The effect of the act
Group Discussion

- **Allegation**: That one of our employees is paying bribes in exchange for preferential treatment resulting in sales for our company.
- Using the 5-part process introduced earlier, how might data analytics be used to show:
  - Break-down of a detective control
  - Commission of the act
  - Concealment of the act
  - Break-down of a detective control
  - The effect of the act

Multi-Factor Analytics

- Excellent method of reducing false positives to make analytics more precise
- Involves identifying multiple possible anomalies that are consistent with a particular risk
- Follow up only if a certain number of red flags result
- Might also consider weighing factors differently and using a pass/fail score to determine whether to follow up on transactions/activities
Example

• Factors that could be present in sales transactions in which our company violated FCPA:
  • Customer is a government agency
  • Previously unused subcontractor
  • Lack of key identifying information for subcontractor or third party (e.g. no street address, etc)
  • Address of subcontractor or third party out of range for where work is to be done
  • Portion of contract for services versus hardware is higher than usual range
  • Pricing in final quote is higher than second to last quote
  • Unusual profit margin on contract
  • Service line item in final quote that was not in previous quotes
  • Many others !! Use your imagination !!

PART 3

What next?
Following up on the results of analytics
What Next...

- Anomalies found in performing data analytics rarely prove intentional acts of noncompliance
- What anomalies might identify:
  - That an internal control was not followed as designed
  - That specific transactions/activities should be looked at further
  - That certain documents should be reviewed

Example

- Analysis of data from an online travel expense reporting system found two anomalies:
  - Several supervisors reviewed their workers’ expense reports without ever opening the PDF supporting documents
  - One supervisor (included above) “approved” 17 expense reports while logged into the system for 37 seconds!
- What’s it mean?
  - A critical detective internal control (identifying whether employees with corporate credit cards charged inappropriate items to the cards) is not operating as designed
- What to do?
  - Notify supervisors (or their supervisors)
  - Training
  - Deeper dive to assess whether fraud is occurring? Collusion?
Deeper Dive

• Possible next steps:
  • Review expense reports and supporting documents
  • Additional analytics:
    • Assess correlation with specific salespeople, customers, or supervisors
    • Compare to PTO or timekeeping records
    • Compare to SalesForce or similar customer contact management systems
    • Interviews

“Reverse Proof”

• The concept of considering each of the legitimate (i.e. no compliance problem) explanations for an anomaly/red flag
• If after considering all explanations, each has been ruled out, the only remaining explanation is that a violation occurred
Example – Reverse Proof

- Anomaly: Properties of a PDF document indicate the document is dated 4/15/2018 supporting an expense report and other PDF supporting docs all dated 2/25/2018
- Possible legit explanations:
  - Document was missing from initial submission
  - Initial document was insufficient, supervisor requested better documentation
  - What else?
  - If none can be proven, it might be fraud – subsequent alteration of a document to conceal an improper expenditure

QUESTIONS ??

Gerry Zack, CCEP, CFE, CIA
CEO
SCCE & HCCA
Tel: +1 952.567.6215
gerry.zack@corporatecompliance.org