THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING
ADVANCED DATA ANALYTICS, THE FRAUDSTERS WORST ENEMY

Introducing Powerful Tools and Techniques to Uncover Fraud
**Agenda**

- Overview of data analytics in the anti-fraud and fraud investigation context
- Capability limitations of traditional data analytics methods and how to overcome
- The power of combining publicly available information and data visualization technology
- Real world examples of indications of fraud identified using advanced data analytics, public information and visualization technology
Overview of data analytics in the anti-fraud and fraud investigation context
Data Analytics in an Investigative Context

• What is Data Analytics?
• How is it employed in investigations?
• What are the advantages of the use of data analytics versus traditional forensic investigative techniques?
• How can it be used as a tool in an investigation?
• Proactive versus reactive data analytics
Fraud’s Increasing Trajectory

• Typically starts out small

• Increases in complexity and aggressiveness

• Often grows in magnitude and in number of participants

• Will rarely cease on its own
What are we looking for?

What might we find with data analytics?
- Fraud or fraud risks
- Control gaps / failures
- Errors and inefficiencies

Proactive/detective data analytic purposes:
- Generally looking for previously unknown patterns indicative of fraud or loss
- Identification of high risk areas to enhance controls or concentrate further investigative efforts/action

What is different with an investigations context?
- [Often] you know where to begin your focus
  - Process(es), patterns, specific accounts/vendors, etc.
- May analyze more detailed information, such as meta data
- Heavier review of results, including comparing results to social media and/or other publically available information
Fraud Risks/Schemes in Common Processes

Vendors / Accounts Payable (AP)
- Conflict of interest / kickbacks
- Embezzlement/Theft
  - Fictitious/Ghost vendor
  - False invoicing scheme
- Bid rigging
- Anti-corruption

Corporate Expenses/Purchase Card
- Embezzlement/Theft (personal expenses)
- Anti-corruption (entertaining or making payments to government officials)

Employees / Payroll
- Embezzlement/Theft
  - Ghost employee (never or was previously employed)
  - Unauthorized or improper payroll payments
  - Falsified or inflated hours or overtime
- Anti-corruption (in addition to Ghost employee risks)
  - Hiring unauthorized/illegal employees (incl. government)
Fraud Risks/Schemes in Common Processes

Customers / Accounts Receivable
- Embezzlement/Theft
  - Lapping / Re-directing deposits
- Conflict of interest / kickbacks
- Earnings management (inflating assets / revenue)

• Manual Journal Entries (GL)
• Earnings management, most typically:
  - Increase assets, revenue
  - Decrease liabilities, expense
  - Balance sheet gross-up
• Concealment of improper cash disbursements
Broad Category of Routine Groups/Objectives

- Master record matches (ex. Vendor/Customer to Employee)
- Segregation of duties / user access
- Invalid/Missing/Unusual/High-risk record characteristics, including Benford’s Analysis, rounded dollar transactions, etc.
- Numeric sequencing and structure (ex. Invoice references)

- Duplicate records
- Unusual days/times
- External record comparisons
- Change log analysis
- High-level analysis
  - Top X summaries
  - Stratifications
Methodology

Business Environment

• Business & concerns
• Processes & systems

Scope

• Processes to analyze
• Data to collect (tables, time frame)
• Number and types of routines

Tool Selection and Determination of Risk Factors

• What tools will you use
• How will you determine high-risk records
Methodology

- Load Data
  - Import tables
  - Quality checks

- Process Data
  - Run routines
  - Quality check results

- Forensic Review and Reporting of Risk Areas
  - Review findings
  - Report to stakeholders
Data Analysis Flow

- User Interface
  (Risk Scoring and Test Results)

- Repository of Forensic Procedures
  (Classified by Business Process)

- Rules Engine

- Data Aggregator

- Data Loader

- Examples of Client Data
  (Multiple Sources such as SAP,
   Oracle, In-House, etc)
  - Vendor Master List
  - Employee Master List
  - Payments, Invoices, etc.

- Public Information
  External Data Sources
Focus on High Risk and High Value Transactions

- Frequency Anomalies
- Data Anomalies
- Inconsistency in Data Sets
- High Risk & Value

©2016 RSM US LLP. All Rights Reserved.
Capability limitations of traditional data analytics methods and how to overcome
Current Challenges

• Increasingly Complex Regulatory Environment:
  • Foreign Corrupt Practices Act (FCPA)
  • Sarbanes and Oxley
  • Dodd-Frank Whistleblower Provision

• Business processes and controls don’t operate perfectly

• Collusion is difficult to prove

• Compliance resources must be allocated efficiently

• Improper behavior of certain employees may be unavoidable

• Performance pressures may create unintended incentives to achieve metrics
Ongoing Benefits Include…

- Identify compliance failures on a timely basis
- Continually evaluate control environment effectiveness
- Mitigate control weaknesses
- Objective basis for quantifying system-wide risk
- Allocate limited resources efficiently
- Reduce cost by correcting errors
- Eliminate inefficiency and waste in the supply chain
- Uncover high risk relationships
- Improve existing internal audit protocols
- Assess compliance with FCPA books & records
- Monitor compliance and risk of newly acquired businesses
### Other Limitations and How to Overcome

<table>
<thead>
<tr>
<th>Quality assurance</th>
<th>Use of trends rather than transaction-level</th>
</tr>
</thead>
<tbody>
<tr>
<td>− Import issues</td>
<td>− Frequencies</td>
</tr>
<tr>
<td>− Complete population</td>
<td>− Time lines</td>
</tr>
<tr>
<td>− All fields necessary</td>
<td>− Various other visualization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sampling vs. complete population</th>
<th>Time consuming to repeat</th>
</tr>
</thead>
<tbody>
<tr>
<td>− Test 100% of population</td>
<td>− Scripts</td>
</tr>
<tr>
<td></td>
<td>− Normalization</td>
</tr>
</tbody>
</table>
The power of combining publicly available information and data visualization technology
Examples of Public Information

• Utilizing public information can tell you:
  – If an address is invalid or high risk
  – A phone number is invalid or tied to a temporary address
  – An employee address or phone ties to a business
  – Employee SSN belongs to a deceased person
  – Address is a check cashing store
Potential Ghost Employee: Address is a Hotel, SSN Pattern or Other IDs are invalid for Active Payroll Employee
Potential Ghost Vendor: Mail Delivery Address, Temporary Office Location, Mobile Phone and the Vendor Received Payments
Visualization Tools

Benefits of visualizing results:

• Compelling way to tell a story – not just numbers
  – “A picture is worth a million words”

• Useful to risk management

• Dashboards add immediate understanding of data world working with

• Conflict results can be simplified
Example of Risk Management Dashboard

Routines per Module and Risk

Risk Score Dashboard

Risk Ratings Distribution

Vendor Score Distribution

Average Risk Scores Across Vendors per State
Example of Vendor Risk Dashboard

Vendor Dashboard

Vendor Activity by State - Total Count

Vendor Active Status Counts

Vendor Status

Active
No Activity 586
93
Inactive
No Activity 273
30
Active 2
$17,054

Number of Vendors with Activity Inactive

Vendors Count by Type

Employees 367
36.0%

Vendors Amount by Type

Employees $51,481
2.7%

Regular Vendor 720
66.0%

Vendors in Dollar Ranges

Range
Over $500K 0
500K to $500K 1
100K to $500K 1
50K to $100K 0
10K to $50K 1
5K to $10K 1
$1K to $5K 2
$1K to $10K 1
$500 to $1K 2
$100 to $500 4
$50 to $100 77
$0 to $50 41
$1 to $50 61
in $50 110

Number of Vendors with Total Activity in Range
Examples of Social Network Diagram to Visualize Shared Data Elements
Real world examples of indications of fraud identified using advanced data analytics, public information and visualization technology
Case Studies

Conflict of Interest:

• Test identified an employee with the same address as a contractor, but different phone number and last name

• Upon investigation, it was determined the contractor was the son of the employee, and the employee not only supervised the work, but also determined how much the contractor was paid

• Over $20,000 was paid to the contractor and the relationship was not disclosed on the vendor conflict forms (‘no relationships’ was checked by the employee)

Employee Fraud:

• Tests Identified vendor bank account numbers that matched an employee's bank account numbers

• An Accounts Payable clerk used the vendor master change function to change the payable information to his own name during the check run and change it back once the run was completed

• The employee had collected several hundreds of thousands in diverted payments
Case Studies

**Employee Expense Fraud:**

- Whistleblower indicated suspect expense reimbursement requests from a senior executive
- Data analysis routines, coupled with timeline visualization, helped identify over $50,000 in inappropriate spend, including falsified receipts

**Employee Fraud:**

- Ghost Employees - Identified 21 terminated employees that received over $1 million in payroll payments
- Identified an employee whose SSN, according to public records, was issued prior to birth and belonged to a deceased individual. The employee was an active employee on payroll.
This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM US LLP.

© 2016 RSM US LLP. All Rights Reserved.