Technology’s Impact On Fraud Schemes: What You Need to Know

IIA / ISACA

December 10, 2019
Introductions

Gene Cahill
Partner,
Advisory - Forensics
Grant Thornton LLP

Mark Sullivan
Principal,
Advisory Leader - Midwest,
Grant Thornton LLP
Today’s Topics

- Introduction, Common Schemes & Impact of Fraud
- Emerging Technologies & Their Impact on Fraud
- Preventing & Detecting Fraud
- Examples & Case Studies

Grant Thornton
Today’s Topics

- Introduction, Common Schemes & Impact of Fraud
- Emerging Technologies & Their Impact on Fraud
- Preventing & Detecting Fraud
- Examples & Case Studies

Grant Thornton
What is Fraud?

Fraud occurs in a variety of fashions but generally is due to three specific factors that make up the Fraud Triangle:

• Motivation (or pressure) – the need for committing fraud (need for money, etc.);
• Rationalization – the mindset of the fraudster that justifies them to commit fraud; and
• Opportunity – the situation that enables fraud to occur (often when internal controls are weak or nonexistent)
Internal Fraud

Internal, also called occupational fraud, can be defined as: The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the organization’s resources or assets. Simply stated, this type of fraud occurs when an employee, manager, or executive commits fraud against his or her employer.

Internal Fraud falls into three categories Corruption, Asset Misappropriation, and Fraudulent Statements and can include:

<table>
<thead>
<tr>
<th>Contract Fraud</th>
<th>Payroll</th>
<th>Financial Statement Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a procurement or contract officer uses their position to inappropriately award a contract or approve contract payments for some type of benefit</td>
<td>Payroll employees can falsify timecards for themselves or other employees, set up &quot;ghost employee&quot; accounts, etc.</td>
<td>When financial statements or financial related information is changed to put the company or agency in a better light than what is actually true</td>
</tr>
</tbody>
</table>
External Fraud

External fraud covers a broad range of schemes, and can include:

- **Contract Fraud**: Dishonest vendors might engage in bid-rigging schemes, bill the company for goods or services not provided, or demand bribes from employees.

- **Third-Party Fraud**: Organizations also face threats of security breaches and thefts of intellectual property perpetrated by unknown third parties. Other examples of frauds committed by external third-parties include hacking, theft of proprietary information, tax fraud, bankruptcy fraud, insurance fraud, healthcare fraud, and loan fraud.

- **Customer Fraud**: Dishonest customers might submit bad checks or falsified account information for payment, or might attempt to return stolen or knock-off products for a refund.
Today’s Topics

- Introduction, Common Schemes & Impact of Fraud
- Emerging Technologies & Their Impact on Fraud
- Preventing & Detecting Fraud
- Examples & Case Studies
Emerging Technologies

- Technological advancements present opportunities for both fraud perpetrators and those trying to stop them.

- As criminals find new ways to exploit technology to commit their schemes and target new potential victims, organizations must ensure they are adopting new technologies that are the most effective in navigating the evolving threat landscape.

But which technologies are most effective in helping organizations manage their fraud risk? Which tools provide benefits that outweigh the costs? How are organizations successfully harnessing the power of data and technology as part of their anti-fraud programs?
Emerging Technologies Impact on Fraud

The ACFE 2018 Report to Nations on Occupational Fraud and Abuse indicates that organizations that used "proactive data monitoring" experienced a 52 percent reduction in the total loss from fraud schemes.

Analytics provide a means of combating fraud that is more effective and more efficient.

- Leverage qualitative assessment-based findings into rules.
- Visualize and explore data to profile, pattern, and detect outliers not associated with logic-checks.
- Analyze and convert big data sets into workable targeted populations
- Build models to identify suspicious transactions and predict likelihood of fraud.
Past Technologies

• Leading technologies from as recently as 7-10 years ago offer a fraction of the capabilities today’s technologies are able to perform, including:
  • Restrictions in the volume of data that could be handled
  • Limits to the complexity of analytical rules that could be applied (i.e. simple formulas, charts, etc.)
  • Need for brute-force

• Given the limits of past technologies, complex trends and anomalies may have been missed, sampling was much more random, and E-Discovery was much more time and labor intensive.
What data analytics techniques are organizations using to combat fraud?

<table>
<thead>
<tr>
<th>Technique</th>
<th>Organizations currently use</th>
<th>Organizations expect to adopt in 1-2 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emotional Tone/Sentiment Analysis</td>
<td>7%</td>
<td>9%</td>
</tr>
<tr>
<td>Artificial Intelligence/Machine Learning</td>
<td>13%</td>
<td>25%</td>
</tr>
<tr>
<td>Geographic Data Mapping</td>
<td>10%</td>
<td>16%</td>
</tr>
<tr>
<td>Text Mining</td>
<td>12%</td>
<td>18%</td>
</tr>
<tr>
<td>Link Analysis/Social Network Analysis</td>
<td>13%</td>
<td>22%</td>
</tr>
<tr>
<td>Predictive Analytics/Modeling</td>
<td>13%</td>
<td>22%</td>
</tr>
<tr>
<td>Data Visualization</td>
<td>12%</td>
<td>30%</td>
</tr>
<tr>
<td>Automated Red Flags/Business Rules</td>
<td>18%</td>
<td>35%</td>
</tr>
<tr>
<td>Exception Reporting/Anomaly Detection</td>
<td>8%</td>
<td>35%</td>
</tr>
</tbody>
</table>

© 2017 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd
What are the most common programs for each data analytics technique?

<table>
<thead>
<tr>
<th>Exception reporting/anomaly detection</th>
<th>Automated red flags/business rules</th>
<th>Data visualization</th>
<th>Predictive analytics/modeling</th>
<th>Link analysis/social network analysis</th>
<th>Text mining</th>
<th>Geographic data mapping</th>
<th>Artificial intelligence/machine learning</th>
<th>Emotional tone/sentiment analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excel</td>
<td>In-house</td>
<td>Tableau</td>
<td>In-house</td>
<td>i2 Analysts Notebook</td>
<td>ACL</td>
<td>In-house</td>
<td>In-house</td>
<td>In-house</td>
</tr>
<tr>
<td>ACL</td>
<td>ACL</td>
<td>Excel</td>
<td>Excel</td>
<td>In-house</td>
<td>Excel</td>
<td>Tableau</td>
<td>Python</td>
<td>SAS</td>
</tr>
<tr>
<td>In-house</td>
<td>Excel</td>
<td>Power BI</td>
<td>ACL</td>
<td>SAS</td>
<td>In-house</td>
<td>Google</td>
<td>SAS</td>
<td></td>
</tr>
<tr>
<td>IDEA</td>
<td>IDEA</td>
<td>In-house</td>
<td>SAS</td>
<td>LexisNexis</td>
<td>Python</td>
<td>Excel</td>
<td>Power BI</td>
<td></td>
</tr>
<tr>
<td>SAP</td>
<td>SAP</td>
<td>ACL</td>
<td>IDEA</td>
<td>Facebook</td>
<td>SAS</td>
<td>Power BI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Today’s Topics

- Introduction, Common Schemes & Impact of Fraud
- Emerging Technologies & Their Impact on Fraud
- Preventing & Detecting Fraud
- Examples & Case Studies
Controls Overview

Fraud internal controls falls into two buckets:
• Preventive controls are designed to prevent errors, inaccuracy or fraud before it occurs
• Detective controls are intended to uncover the existence of errors, inaccuracies or fraud that has already occurred

<table>
<thead>
<tr>
<th>Preventive</th>
<th>Detective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud awareness training</td>
<td>Anonymous tips / hotlines</td>
</tr>
<tr>
<td>Clearly defined policies</td>
<td>Reconciliation</td>
</tr>
<tr>
<td>Policy enforcement</td>
<td>Analysis</td>
</tr>
<tr>
<td>Predictive data analytics</td>
<td>Email notification</td>
</tr>
<tr>
<td>Multifactor authentication</td>
<td>Whistleblowers</td>
</tr>
<tr>
<td></td>
<td>Descriptive data analytics</td>
</tr>
</tbody>
</table>
Leveraging Analytics to Combat Fraud

FRAUD RISK ASSESSMENT

- Rule-Based Analytics
  - Known Patterns: Common Fraud
- Anomaly Detection Analytics
  - Unknown Patterns: Criminal Fraud
- Predictive Analytics
  - Complex Patterns: Organized Fraud
- Network / Link Analytics
  - Linked Patterns
- Text Analytics
  - Text Patterns

Grant Thornton
Rule-Based Analytics

- A transaction level technique to prevent common fraud based on known patterns.

- Focus on transactional data which does not adhere to organizationally accepted rules.

- Example: Using a company purchase card to buy alcohol on a Saturday evening or holiday will be rejected when expensed.
Business Rules

Approach to Solve Fraud Problem

• Apply business rules to transactional data in order to identify transactions that don’t adhere to commonly accepted procedures or rules

Results

• Identify departures from expected procedures for additional investigation

Best Used

• When initiating fraud detection based on qualitative assessments
• When limited historical data exists
• As part of a hybrid-solution combining business rules with algorithms
Anomaly Detection

• Focused on investigating aggregate-level transactions, anomaly detection uses “unsupervised modeling” to identify outliers compared to peer groups based on unknown patterns among common and individual fraudsters.

• This type of analytics technique allows organizations to understand outlier patterns across the data that may suggest fraud and flag for investigation.

Other Considerations -

• Focus on investigating aggregate-level transactions to understand outlier patterns across the data that may suggest fraud or flag for investigation.

• Cluster high risk entities into groups based on similarities for investigation
Network / Link Analytics

- This technique can be useful for uncovering organized fraud and associations between fraudsters by using social network analytics, looking at linked patterns for investigation and discovery.

- For example, an individual may not be suspicious based on their actions alone, yet suspicion may arise when their actions are connected to others through a set of commonalities based on associated attributes, revealing schemes that may have otherwise gone unnoticed.

- Other Considerations –
  - Use social network analysis to assess connections and network size to uncover fraud.
  - Best used when attempting to uncover new fraud or turn up members of organized crime groups.

Mark is under investigation for mortgage fraud.
Text Analytics

- A technique that involves scraping the internet of things (IoT) information into a structured form and parsing strings of text to scan for red flags of fraud.
- The parsing occurs by using natural language processing (NLG) tools that divide the body of text into segments which are analyzed for text patterns and then described in terms of their syntactic roles, resulting in a sentiment or polarity analysis.
Exploring Other Analytic Techniques

- Digital Forensics
- Data Mining
- Machine Learning
- Artificial Intelligence
Digital Forensics

A branch of forensic science focused on recovery and investigation of artifacts found on digital devices

- **Computer forensics** provides tools to collect and preserve legally admissible evidence from one or more computing devices.

- Once data is collected, can apply data mining and analytic techniques to extract and identify patterns and relationships within structured and unstructured data. Can be used in conjunction with data mining and link analysis to discover and evaluate relationships and information for fraud investigations
  
  - Examples of data gleaned from digital forensics: location data, messages sent and received, photos

- Use cases: financial fraud investigations, cyber crimes (breaches, security lapse)
Data Mining ("demonstrate patterns") – Process of discovering patterns in large data sets involving methods at the intersection of machine learning, statistics, and database systems

Machine Learning ("forecasting") – Field of computer science, providing computer systems the ability to "learn" with data through the use of algorithms

Artificial Intelligence ("shape behaviors") – Theory and development of computer systems to perform tasks normally requiring human intelligence (ex: visual perception, speech recognition, etc.)
Data Mining

Use of statistics and other programming languages to discover previously unseen patterns and relationships from large datasets

• Focus on uncovering relationships between two or more variables in a dataset and extracting insights for a particular use case, such as predicting outcomes and prescribing actions

• Covers a large spectrum of data analysis and knowledge discovery tasks, including data characterization, association and correlation analysis, classification, prediction, clustering, outlier analysis, etc.

• Best used to reveal insights for a given point in time rather than an ongoing basis.
Machine Learning

Deploy data mining techniques, as well as other algorithms, to develop models to "learn" from data and improve performance at a task with experience over time

- **Supervised learning** involves models trained on a dataset with properly 'tagged' outputs
  - Commonly used in fraud detection
- **Unsupervised learning** is the deployment of algorithms to infer natural structure present within a dataset (no explicitly-provided labels to learn from).
  - Can be used to spot anomalous behavior that represent previously undetected fraud schemes
Artificial Intelligence

Uses models developed by machine learning and other algorithms to lead to intelligent behavior

Benefits:

✓ Takes into account emerging activities, behaviors, and trends with anomalous data
✓ Can be deployed in real-time to facilitate detection and prevention
✓ Can facilitate business decision-making as to the acceptable fraud threshold
✓ Enables consistency and quality in user experience

Use Cases: Credit Card Fraud Detection, Identity Theft, Generalized Fraud Detection
Today’s Topics

- Introduction, Common Schemes & Impact of Fraud
- Emerging Technologies & Their Impact on Fraud
- Preventing & Detecting Common Fraud Schemes
- Examples & Case Studies
Senior Executive Breaking Code of Conduct

Situation:
- Investigated suspected expense reporting fraud perpetrated by an executive of its foreign based parent company working at the US subsidiary.

Solution:
- Obtained 8 years of detailed electronic expense reports from the client's expense reporting system, and imaged copies of all expense report receipt submissions.
- Analyzed company cell phone records of the suspect for the period in question, performed email review of suspect's client email account, and searched the suspect's social media accounts.

Outcome:
- Reviewed expense reports against receipts to determine legitimate business expenses vs. falsified business trips and non-business expenses.
- Mapped the suspect's purported location per expense reports against their actual location per cell phone tower records over time.
- Identified evidence from the suspect's emails and social media postings to support his actual locations.
- Compiled illegitimate expenses reimbursed to suspect for prosecution and filing of an insurance claim.
Fuel Theft from a Transportation Company

**Situation:**
- The Client’s Internal Audit department identified fuel theft occurring at it’s Mexico operations.
- Engaged to analyze the full population of data to quantify the potential theft and identify trends (e.g. location, time period) related to the theft.

**Solution:**
- Analyzed three years of data for three separate datasets which consisted of over 311 distinct data files.
- Various data analytic tools (e.g. python, visualization software) were used to identify trends, anomalies, and quantify potential fuel theft.

**Outcome:**
- Analyzed millions of rows to quantify the potential loss due to theft which of approximately ~2 million gallons of fuel.
- Specific examples, locations, and trends related to the potential theft were identified in the data.
- Analytic tools were used to quickly analyze a variety of fraud scenarios to evaluate the potential impact and narrow the scope of potential theft.
Manipulation of Inventory in Financial Statements

**Situation:**
- The client identified inventory issues on the books of one of its SE Asia subsidiaries.
- Review the subsidiary’s financials and supply chain / inventory management processes the cause and depth of the overstatement.

**Solution:**
- Loaded all G/L data into full ledger analytics tool. Applied data analytics to identify anomalies and inconsistencies between inventory reports, GL data, and supply chain production and shipping documentation.

**Outcome:**
- Determined that an employee of the subsidiary had been manipulating the inventory costs to match expected margins.
- Analytics found that the employee manipulated the inventory costs simply by moving balances between inventory accounts and a suspense account.
- Further, analytics found that payments were made to vendors using the suspense account balance created by the inventory adjustments to conceal expenses from the P&L, resulting in a wider investigation.
Transactional Reconciliation and Investigation

Situation:
- A financial institution’s new management identified several million dollars in unaccounted cash.
- Asked to analyze and assist in the reconciliation of transaction activity between several information systems.

Solution:
- Reconciled transaction activity across internal MS Excel reports, the internal record keeping system, the accounting system, and bank statements for several clients.
- Utilized Python scripts to automate the reconciliation process, allowing for efficiencies particularly when new information was identified.

Outcome:
- Reconciled over 3 million of line items across several databases for transaction activity over a six year period.
- Under 300 non-reconciled transactions were manually investigated by the GT team. Identify $5.5 million dollars due to / due from (owed clients / clients owed) company’s clients.
For more information

Contact:

Gene Cahill, Partner
Phone: 312 602 8103
Email: Gene.Cahill@us.gt.com

Mark Sullivan, Principal
Phone: 312 602 8110
Email: Mark.Sullivan@us.gt.com