Digital Forensic and Data Analytics in Forensic Audit

Presented by:
Payal Agarwal,
Perspective of Fraud in India

58% respondent believe that incident of fraud will rise in the next two years

Source: Deloitte India Fraud Perception Survey 2018
India perspective - usage of technology for fraud detection

Advanced Technology awareness and usage in fraud detection

Source: Deloitte India Fraud Perception Survey 2018
Overview of Digital Forensic

Digital Forensic is the application of the scientific principles to the process of discovering information from a digital device.

Result Verification: Result of research need to be validated.

Test the Hypothesis: Testing helps in fine tuning the results for analysis.

Purpose of Research: It is important to define the purpose of research.

Defining the Hypothesis: Defining hypothesis helps in understanding measures to be taken for the research.

https://youtu.be/ZUqzcQc_syE
Need for Digital Forensic

Factors Impeding Fraud Controls

Information Silos:
Can provide an incomplete picture.

Can’t always compete with fraudsters:
Reliance on manual processes and ad-hoc data analysis coupled with lack of resources and skills.

Reliance on Rule Based Testing:
Sophisticated schemes can be missed.

Unstructured Data:
It is difficult to analyze, access and integrate data.
Digital forensic and its role in fraud risk management

**Proactive**
- Setting up a forensic lab and/or fraud risk management system
- Evaluating standards of an existing lab/process reviews

**Reactive**
- Investigations
- Evidence management
Analytics Driven Fraud Investigation

Dimensions for defining analytics driven fraud investigation

**Mature Analytics:**
Including tools employed, frequency of analysis and whether it is conducted in silos or enterprise manner

**Integrated Data Marts:**
Including structured and unstructured data for risk modelling

**Risk Scoring at entity rather than transaction:**
Transaction don’t commit frauds, employees, vendors, customers and others do..

**Advance Analytics:**
Including advance analytics such as machine learning, cognitive computing can enable finding associated bad actors
Data considerations during data discovery

**Familiarity/Ownership**
It is important for senior management to understand the data owners who are fluent at and acquainted with various data systems which are part of their organization’s structure.

**Location**
Knowing where the data is stored is as critical as knowing the sensitive nature of different data sets themselves. Data maps help in understanding the landscape of a firm’s digital storage infrastructure.

**Volume**
The amount of data that a firm holds must be in line with the understanding of the senior management as well as aligned with the applicable regulatory requirements.

**Data type of discovery**
Regulatory requirements do not permit cracking passwords to documents or personal email accounts that may be identified as part of the review. Open documents can be reviewed.

**Preservation requirements**
Regulatory requirements on retention and preservation schedules of data sets are significant to the firm in times of litigation, and for geographical and jurisdictional privacy compliance.
Reactive Digital forensic: Investigation and data management

- Assessment of complaint and problem at hand
- Stakeholders involved
- Accused involved
- Permission levels
- Access strategy
- Doability assessment
- Nature of IT assets to be reviewed
- Server data + on-asset data identification for each user
- Imaging assets
- 4-24 hour timeframe per asset depending on the security level of asset and type
- Chain of custody procedures
- Raw data collection and storage on hard drives
- Data processing
- Indexing
- Keyword identification based on scope
- Run queries
- Review number of size of results
- Index and transfer data for review
- Review data using review tools like Relativity
- Identify hot, medium, low hits
- Level 1,2,3 reviews for story construct
- Evidence arrangement as per scope and delivery
- Data storage per investigation for 5-7 years as per regulatory requirement
Stages in Advanced Fraud Analytics

**Data Collection Strategy**

- Electronic Transactions
- Contract Documents
- Open Source Information

**Data Ingestion**

- Transformation
- Digitization
- Data Input

**Data Cleansing**

- Data Hosting Platform

**Anomaly Testing Strategy**

- Payment Records
- Contracts Data
- Supporting Docs
- Open-Source Info

**Performance Tests**

- Forensic Accounting
- Financial Intel
- Capital Projects
- Valuation

**Review**

- Risk-scored results
- False-positives

**Result Management**

- Recover Improper Payments
- Mitigate Control Deficiencies
- Support Audits & Investigations
- Enhance Transparency Accountability

**Information Processing**

Multiple data sources are considered for collection, including electronic records, paper documents, and open-source research.

**Advance Analytics**

Review may be performed on payment data to risk-score potentially anomalous behavior.

**#The methodology helps to provide the ACTIONABLE RESULTS that will provide enhanced transparency and accountability.**
Fraud Detection – Advanced Analytics Solution Approach

**Static Rules**
- Known common patterns

**Supervised Learning**
- Data labels in past data available for training
- Standard classification techniques to construct the predictive model

**Unsupervised Learning**
- Data labels not available or not used
- To uncover new and unknown fraudulent patterns

**Clustering**
- Model the ‘normal’ behavior of events and hence detect deviations from the modelled ‘normal’ behavior
  - Eg. Claims Data

**Markov Chain Modelling**
- Measure the probability of a sequence of events happening and use to that to detect any rare sequence
  - Eg. Credit Card Transactions

**Association Graph Analysis**
- It locates the associations among the users to identify suspicious connections
  - Eg. Invoicing, Transfers

**Domain Expert Insight**

**Identify Fraudulent events**
Anomaly Detection
Unsupervised Learning to identify new or emerging fraud patterns, such as buyers that are behaving very differently from their peers.

Buyer A – Normal Behavior

Buyer B – Outliers Identified

Analyzed normal purchasing activity for buyers within the organization

Identified buyers making anomalous purchases of certain materials
Illustrative Sample: Invoice Keywords (Anti-Bribery and Corruption Perspective)

Drilling on the keyword provides transaction details.
## Illustrative Sample: Conflict of Interest Amongst Vendors

### Vendor to Vendor Conflict of Interest

Dashboard representing different vendors having the same Account Number, PAN and telephone numbers. 

**Currency:** INR

### Vendor to Vendor Relationship Summary

<table>
<thead>
<tr>
<th>No. of Groups</th>
<th>No. of Vendors</th>
<th>Similar Name</th>
<th>Different Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6</td>
<td>156</td>
<td>7,145</td>
</tr>
<tr>
<td>21000001081</td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21000001089</td>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Summary of Invoice and Payment Count

<table>
<thead>
<tr>
<th>Vendor Name Match</th>
<th>Invoice Count</th>
<th>Payment Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Similar Name</td>
<td>250.0</td>
<td></td>
</tr>
<tr>
<td>Different Name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Vendor to Vendor demographic details

<table>
<thead>
<tr>
<th>Group Id</th>
<th>Vendor Id</th>
<th>Vendor Name</th>
<th>Account Number</th>
<th>Vendor Name</th>
<th>Account Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>100000000941</td>
<td>ULHASPRABHAS GRAPHTHE INC</td>
<td>00640110</td>
<td>00640110</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000001405</td>
<td>ULHASPRABHAS GRAPHTHE INC</td>
<td>00640110</td>
<td>00640110</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00001000307</td>
<td>TECHNOPLAST TIME INC. UNIT-PANOLI</td>
<td>00010330</td>
<td>00010330</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00001000308</td>
<td>TECHNOPLAST TIME INC. UNIT -</td>
<td>00010330</td>
<td>00010330</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000008851</td>
<td>TECHNOPLAST TIME INC.</td>
<td>2563983</td>
<td>3437300</td>
<td>00010330</td>
</tr>
<tr>
<td></td>
<td>2100015083</td>
<td>TECHNOPLAST M/S</td>
<td>00010330</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2100016421</td>
<td>TECHNOPLAST TIME INC.</td>
<td>00010330</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>21100001091</td>
<td>TECHNOPLAST TIME INC.</td>
<td>00010330</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000002592</td>
<td>ULHASPRABHAS QUEST2TRAVEL.COM PVT INC</td>
<td>0541256</td>
<td>0541256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000006340</td>
<td>ULHASPRABHAS QUEST2TRAVEL.COM PVT INC</td>
<td>0541256</td>
<td>0541256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1100000131</td>
<td>COM QUEST2TRAVEL ULHASPRABHAS PVT INC</td>
<td>0541256</td>
<td>0541256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000002592</td>
<td>ULHASPRABHAS QUEST2TRAVEL.COM PVT INC</td>
<td>0541256</td>
<td>0541256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000006340</td>
<td>ULHASPRABHAS QUEST2TRAVEL.COM PVT INC</td>
<td>0541256</td>
<td>0541256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1100000132</td>
<td>NEW THE ULHASPRABHAS ASSURANCE CO.,INC</td>
<td>220204424306</td>
<td>220204424306</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000002194</td>
<td>NEW THE ULHASPRABHAS ASSURANCE CO.,INC</td>
<td>220204424306</td>
<td>220204424306</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000007084</td>
<td>NEW THE ULHASPRABHAS ASSURANCE CO.,INC</td>
<td>220204424306</td>
<td>220204424306</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000003147</td>
<td>NEW THE ULHASPRABHAS ASSURANCE CO.,INC</td>
<td>220204424306</td>
<td>220204424306</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000003147</td>
<td>ULHASPRABHAS NEW ASSURANCE COMPANY</td>
<td>220204424306</td>
<td>220204424306</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000003147</td>
<td>ULHASPRABHAS NEW ASSURANCE COMPANY</td>
<td>220204424306</td>
<td>220204424306</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21000003147</td>
<td>ULHASPRABHAS NEW ASSURANCE COMPANY</td>
<td>220204424306</td>
<td>220204424306</td>
<td></td>
</tr>
</tbody>
</table>

### Account Information

<table>
<thead>
<tr>
<th>Account Number</th>
<th>Pan No</th>
<th>Phone No</th>
<th>Invoice Count</th>
<th>Invoice Amount</th>
<th>Payment Count</th>
<th>Payment Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>0143011006917</td>
<td>0120-4573453</td>
<td>00640110</td>
<td>0120-4573453</td>
<td>0120-4573453</td>
<td>0120-4573453</td>
<td>0120-4573453</td>
</tr>
</tbody>
</table>
Illustrative Sample: Vendor Risk Profile

Drill down to understand which vendor has what risk and why.
Illustrative Sample: Travel and expense—Claim approved and paid within 24 hours

Drill down to obtain details of these claims for further scrutiny.
Illustrative Sample: Duplicate Journal Entries

Duplicate Journal Entries
Duplicate Journal Entries are identified based on the Account ID and the Absolute General Ledger Amount.

Summary by Entry type
Non-Standard
Standard

Drill down by account ID for detail breakup

Summary by Account ID

Duplicate Journal Entries
Duplicate Journal Entries are identified based on the Account ID and the Absolute General Ledger Amount.

Effective Date: 4/1/2013
Company ID: (AS)
General Ledger Amount: 1,842,957.8

Summary by Entry type

Duplicate Journal Entries
Duplicate Journal Entries are identified based on the Account ID and the Absolute General Ledger Amount.

Effective Date: 4/1/2013
Company ID: (AS)
General Ledger Amount: 6,106,000.0

Summary by Account ID

Private and Confidential
### Illustrative Sample: Order to Cash - Exceeding credit limit - Customer wise

#### Exceeding credit limit - Customer - wise

<table>
<thead>
<tr>
<th>Customer ID</th>
<th>Open Amount in Local</th>
<th>Credit limit</th>
<th>Credit limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>671,867</td>
<td>100,000</td>
<td></td>
</tr>
<tr>
<td>1033</td>
<td>274,286</td>
<td>100,000</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>511,292</td>
<td>100,000</td>
<td></td>
</tr>
<tr>
<td>1174</td>
<td>2,827,795</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1175</td>
<td>3,341,745</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Drill down to customer level details

<table>
<thead>
<tr>
<th>Customer ID</th>
<th>Invoice Ent.</th>
<th>Open Amount in Local</th>
<th>Credit limit</th>
<th>System Invoc.</th>
<th>Entered Date</th>
<th>Invoice Date</th>
<th>Gross Amount F</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>ZECHER</td>
<td>671,865</td>
<td>100,000</td>
<td>5/30/2005</td>
<td>5/30/2005</td>
<td>625,133</td>
<td></td>
</tr>
<tr>
<td>1033</td>
<td>MAASSBERG</td>
<td>274,286</td>
<td>100,000</td>
<td>10/30/2005</td>
<td>10/30/2005</td>
<td>623,305</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>MUELLER</td>
<td>511,292</td>
<td>100,000</td>
<td>3/30/2005</td>
<td>3/30/2005</td>
<td>544,986</td>
<td></td>
</tr>
<tr>
<td>1174</td>
<td></td>
<td>2,827,795</td>
<td></td>
<td>7/30/2005</td>
<td>7/30/2005</td>
<td>333,639</td>
<td></td>
</tr>
</tbody>
</table>
Thank You

Payal Agarwal