Continuous Audit at Insurance Companies

Youngbum Kim, PhD. Student, Rutgers Univ.
Sutapat Thiprungsri, PhD. Student, Rutgers Univ.
Outline

- Objectives
- Scope
- Methods
- Research Framework
  - A Rule-based model for Anomaly Detection
  - Clustering
- Q&A
Objectives

- Creating an architecture for a future continuous audit of the systems in question
- Assisting the audit with analytical support
- Creating system specific filters of eventually preventive nature
Scope

- Historical disbursements & claims data to develop filters that may detect fraud, discrepancies and internal control weaknesses

- Maturity Model
  - Automated Continuous Audit
  - Continuous Control Monitoring
Methods
An evolving continuous audit framework

- Automation
- Sensoring
- ERP
- E-Commerce

Continuous Risk Monitoring and Assessment
Continuous Data Audit
Continuous Control Monitoring

Continuous Audit
Steps in the continuous forensic and audit process

1. Identify system and understand its structure and features
2. Capture relevant data
3. Clean and scrub data
4. Create KPI and extraction models
5. Run models under different scenarios
6. Examine the exceptions found on an interactive basis
7. Decide on profile of risk
8. Place filters in the entrance of processes
9. Create an audit by exception mechanism within the internal audit organization
10. Create interfaces between management continuous monitoring and audit by exception
11. Continue the forensic model development process based also on the filtering results
12. Work on external audit reliance on the process
Framework
A Rule-Based model for Anomaly Detection
Research Question

- Prior Research
  - Focuses on fraud by outsiders such as customers, criminals, and intruders (→ external fraud).
  - Little research on Internal Fraud
  - Highly depends on ‘labeled/classified’ data.
  - Known internal fraud examples are rarely documented and disclosed.
    → Unsupervised method of profiling
- Practicability
  - Rarely considers actual implementation by internal auditors
    → Rule-based indicators and suspicion scoring system

- How can we develop a rule-based model to detect abnormal (internal fraudulent/erroneous) wire transfers?
Obstacles to Anomaly Detection

- Anomaly (including internal fraud) detection
  - When anomaly prevention fails (how to know?).
  - Detects in a timely manner (or at least not too late, especially for internal fraud).
  - Too small number of anomaly cases.

- Continuous Auditing/Monitoring process
  - Unawareness that the anomaly prevention control has failed.
  - Highly adaptive existing fraudsters (=fraud perpetuators) and Newcomers.
  - Cost of undetected anomaly (esp. internal fraud) is significant.
Model Development Process

- Information collection
- Discussion with Internal Auditors for Validation
- Rule Creation (addition/deletion/revision)
- Result Investigation by Internal Auditors
- Model Testing with Data (Re-testing)

Note. (): After the first round
Anomaly Detection Process

A transaction

Anomaly detecting model

Suspicion Score Calculation

Greater than criterion?

Y

Labeled as potential anomaly

N

No Reports

Final Results

Test of detail by internal auditors
Indicators Category

- 21 types (38 indicators) of anomaly indicators.
  - Purport to identify abnormally low or high values, abnormally positive slope, or abnormally different from population norms.

- Conditional tests
  - Pass/Fail or Yes/No types
  - Some of them are directly related to controls.

- Statistical tests
  - PI/CI, Frequency test, Correlation test, or Clustering
  - Developed by using either prediction intervals, correlation, or clustering.
## Anomaly Indicators: Example

(Nota. All the examples are fictitious.)

<table>
<thead>
<tr>
<th>Questions</th>
<th>Possible Filtering rules to test</th>
</tr>
</thead>
<tbody>
<tr>
<td>The payee transactions payment amount is out of the range of payment amounts.</td>
<td>Amount range for each payee (or all payees) &amp; check outliers.</td>
</tr>
<tr>
<td>The payee transaction payment trend line over time has a positive slope.</td>
<td>Correlation between date (or sequence numbers) and payee amounts for each payee</td>
</tr>
<tr>
<td>The payee is an outlier to payee baseline activity. (Send to a payee that normally do not send to)</td>
<td>Payee frequency by each initiator &amp; check the payees that have the least frequencies.</td>
</tr>
<tr>
<td>The transaction amount is out of range of normal activity from this bank account.</td>
<td>The 90, 95, and 99 PI amts for each sending/receiving bank account and check the exceptions.</td>
</tr>
<tr>
<td>The transaction initiator is not a normal sender from this bank account.</td>
<td>First, check the list of sender bank account, then create exception list of initiators by sending bank account.</td>
</tr>
<tr>
<td>The transaction payee is not a normal receiver from this bank account.</td>
<td>A list of payees by sending banks who have least frequency:</td>
</tr>
</tbody>
</table>
# Suspicion Scores

(All the numbers are fictitious.)

<table>
<thead>
<tr>
<th>Statistical score</th>
<th>All wires</th>
<th>Last Qtr only</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>197505</td>
<td>52574</td>
</tr>
<tr>
<td>1</td>
<td>7943</td>
<td>2092</td>
</tr>
<tr>
<td>2</td>
<td>1867</td>
<td>485</td>
</tr>
<tr>
<td>3</td>
<td>762</td>
<td>281</td>
</tr>
<tr>
<td>4</td>
<td>150</td>
<td>92</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conditional score</th>
<th>All wires</th>
<th>Last Qtr only</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>86613</td>
<td>34472</td>
</tr>
<tr>
<td>1</td>
<td>102686</td>
<td>17787</td>
</tr>
<tr>
<td>2</td>
<td>14063</td>
<td>2183</td>
</tr>
<tr>
<td>3</td>
<td>4327</td>
<td>987</td>
</tr>
<tr>
<td>4</td>
<td>402</td>
<td>80</td>
</tr>
<tr>
<td>5</td>
<td>133</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total score</th>
<th>All wires</th>
<th>Last Qtr only</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>81922</td>
<td>32666</td>
</tr>
<tr>
<td>1</td>
<td>101384</td>
<td>18227</td>
</tr>
<tr>
<td>2</td>
<td>17596</td>
<td>2824</td>
</tr>
<tr>
<td>3</td>
<td>5772</td>
<td>1425</td>
</tr>
<tr>
<td>4</td>
<td>1072</td>
<td>266</td>
</tr>
<tr>
<td>5</td>
<td>384</td>
<td>84</td>
</tr>
<tr>
<td>6</td>
<td>83</td>
<td>32</td>
</tr>
<tr>
<td>7</td>
<td>21</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

If Target Flags are between 25 and 30, 5 for Statistical, 6 for Conditional, and 7 for Total scores.
## Examples of Flagged Wires

<table>
<thead>
<tr>
<th>wireID</th>
<th>amount</th>
<th>Statistical score</th>
<th>Conditional score</th>
<th>Total score</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>950,000</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>25</td>
<td>22,600,000</td>
<td>5</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>33</td>
<td>4,000</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>42</td>
<td>11,500,000</td>
<td>5</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>50</td>
<td>8,200,000</td>
<td>2</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>52</td>
<td>600,000,000</td>
<td>3</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>63</td>
<td>85,000,000</td>
<td>6</td>
<td>7</td>
<td>13</td>
</tr>
</tbody>
</table>
Contribution

- Proposes developing a detection model of internal fraud with unlabeled/unclassified data.

- Describes the development process of an anomaly detection model that is implementable by internal auditors.

- Shows that developing process of anomaly detection model can help internal auditors to identify weakly-controlled areas and thus provide additional assurance.
Limitations and Future Study

- **Limitations**
  - False negatives may exist in model development.
  - Some anomaly indicators may not be applicable to the other companies.

- **Future Study**
  - Needs more fine-tuning, that is, specification and customization to consider transactional characteristics.
  - Thus, Next step will examine the relevance of relevant attributes. If relevant and effective, they will improve the current model.
Clustering For Anomaly Detection
Insurance Claims

- Objective
  - To detect potential fraud or errors in the claims process by using clustering techniques

- Steps in Cluster Analysis
  - Selecting attributes
  - Selecting distance measurement
  - Selecting cluster techniques
  - Analyzing the resulting clusters
  - Identifying anomaly and/or outliers
Visualizing combination of attributes, we will be able to see similarity and differences among claims.
Analyzing individual variables, we will be able to see clearly that some claims have rare values.
Contribution

- Clustering can be used to build a model for anomaly detection when the labeled data are not available.
- It may help to discover some hidden pattern or clusters in the dataset.
Limitations and Future Study

- Cluster Analysis always generates clusters, regardless of the properties of the data-set.
- The interpretation of the results might not be clear.
- How to define anomaly could also be a problem.
Thank you for your attention!