FRAUD DETECTION & PREVENTION USING SOCIAL NETWORK ANALYSIS

BY Lekan Omodara
Agenda

• Introduction
• Financial cost of fraud in the UK
• SAS Fraud Framework components
• FCM & SNA
• Steps in FCM & SNA
• Prevention and Detection in Financial sector
Introduction

What is Fraud?
Fraud is a criminal activity and is defined as Abuse of position, or false representation or prejudicing someone’s right for personal gain

Simply: Fraud is an act of deception intended for personal gain or cause a loss to another party

-SFO, UK

There is always a Financial Implication to every fraud attempts in any organisation

• If it is successful, the company will lose money
• If it is not successful, the company may spend money to investigate or redeem their image
Financial Implication

The UK economy lost £52bn from fraud, according to the 2013 report by the National Fraud Authority. The financial and insurance only experience fraud activities of £5.4bn.
SAS Fraud Framework

Fraud Framework consists of software products designed to detect and prevent fraud, waste, and abuse for organisations in banking, government, health care, and insurance.
SAS Fraud Framework

Operational Data Sources
- Customers
- Accounts
- Transactions

Exploratory Data Analysis & Transformation

Fraud Data Staging

Alert Generation Process
- Business Rules
- Alert Administration

Analytics
- Anomaly Detection
- Predictive Modeling

SAS® Social Network Analysis
- Network Rules
- Network Analytics

Learn and Improve Cycle

Alert Management & Reporting

Case Management
The Fraud Framework also contains the following two fraud-specific products:

- SAS Financial Crime Monitor (FCM)
- SAS Social Network Analysis Server (SNA)
## SAS Fraud Framework Users

<table>
<thead>
<tr>
<th>User</th>
<th>SAS Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Administrator</td>
<td>SAS Management Console</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>SAS Data Integration Studio</td>
</tr>
<tr>
<td>Fraud Administrator</td>
<td>SAS Financial Crime Monitor</td>
</tr>
<tr>
<td>Fraud Analyst</td>
<td>SAS Financial Crime Monitor SAS Enterprise Miner SAS Text Miner</td>
</tr>
<tr>
<td>Fraud Investigator</td>
<td>SAS Social Network Analysis Server SAS Web Report Studio</td>
</tr>
<tr>
<td>Management</td>
<td>SAS Information Delivery Portal SAS BI Dashboard</td>
</tr>
</tbody>
</table>
Financial Crime Monitor (FCM)

SAS Financial Crimes Monitor is an administrator interface responsible for the generation and administration of alerts.
Business Rules & Scenario

• Unusual low cumulative lodgment
• Unusual quick succession of Online Outflow
• Inflow with uncorrelated amount (Sudden lodgement)
• Count of outflow in a day greater than the count of outflow in the last 3 months
• Non active account with un-usual inflow
• KYC – account with similar details
• Accident with Around Same area
• Claims with Same doctor or GP
• Claims around same postcode

Alert can also be generated through the enterprise miner model.(Analytics)
## Tasks and Processing

There are four main tasks and processing that need to be perform during the implementation of the FCM

<table>
<thead>
<tr>
<th>Task</th>
<th>Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Tasks</td>
<td>Create and register Prep and enrichment tables</td>
</tr>
<tr>
<td></td>
<td>Create and register an alert table template</td>
</tr>
<tr>
<td></td>
<td>Write SAS programs (scenarios, processing, enrichment, routing, and so on)</td>
</tr>
<tr>
<td></td>
<td>Create the structure of RDB tables using scripts</td>
</tr>
<tr>
<td>Interface Tasks</td>
<td>Enter project information (Fraud detection/Risk, second pass/score,</td>
</tr>
<tr>
<td></td>
<td>suppression and Routing)</td>
</tr>
</tbody>
</table>
## Task & Processing

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-Tasks</td>
<td>Modify the FCM_JOBCALENDAR table Schedule the Alert Generation Process in an application that is not SAS application</td>
</tr>
<tr>
<td>Alert Generation Process</td>
<td>FCMMain.sas with AutoExec.sas is submitted</td>
</tr>
</tbody>
</table>
Alert Generation Process AGP

Data Makes everything clearer? – Do you agree with this?

An Alert is a potential indicator of Fraud - SAS
Alert Generation Process consists of 6 steps

• Fraud Detection and Risk Scenario:
  • First pass Auto type fraud detection and Risk scenario are executed, with respect to a specific table sorted to variable
  • First pass custom type fraud detection and risk scenario are executed

• Second pass scenario:
  • Second pass scenario are executed, if defined against the data from the first pass based on the run order specified at the second pass group level

• Enrichment: Alerts are enriched if enrichment code is specified

• Scoring:
  • Data is further processed. Current fraud detection and risk alerts are combined with active historical fraud detection and risk alerts
  • The combined alerts are scored
Alert Generation Process

- The process of reduction is initiated on the current–day risk alert
  - Any risk alert whose entity exists with a current-day fraud detection
  - If the overall actionable entity score for an entity not currently win a fraud alert exceeds the specified threshold, then those alerts are retained. A new record is created in the current-day alert table for that entity.
  - The remaining risk alerts are dropped because they do not have an entry with a current-day fraud alert and they do not exceed the specified threshold

- Suppression: Alerts are suppressed based on suppression scenario and run order specified, if defined
- Routing: Alerts are routed based on routing scenarios and run order specified, if defined
Financial Crime Monitor
Financial Crime Monitor

Adding a new scenario

Parameter for the Scenario
Summary Implementation steps

This shows the end to end processes for FCM Alert generation
Social Network Analysis

The SAS Social Network Analysis Server is an investigator interface responsible for viewing and managing alerts.

It is made up 3 major parts, they Alert Window, Detail tab and SNA tab.
Alert Window: The alert windows has the alert pane and filter pane. The alert pane displays the entities for which the alert is generated from the search window. The filter pane enable investigator to subset the current alert in the pane.
The details tab is displayed after you click on an alert row in the alert pane.
SNA TAB

SNA Tab : Contains a network diagram for the alert selected from the alerts window
Implementation Task

Pre-tasks
• Create input data tables
• Create configuration RDB
• Update general property values in the configuration manager

Alert Windows
• Implement the get actionableEntities stored process

Details Tab
• Implement the getSubAlerts stored process
• Implement the getAlertTransactions stored process
• Implement the getChartSeries stored process
Implementation Tasks cont....

Social Network Analysis

• Create nodes and links tables with the %sfs_net_main_link_macros macro
• Implement the getSocialNetwork stored process
• Implement the getSocialNetworkNodesDetails stored process
• Implement the growSocialNetworkNode stored process
Implementation Tasks cont ...

PRE-TASKS

Alert Window

Detail Tab

SNA Tab

Template.SPK

getSubAlerts

gtemChartSeries

getSocialNetwork

getSocialNetworkNodeDetails

processAlertResponse

search_config.xml

alert_config.xml
Best practice for SNA input Data

A best practice is to create input data tables with all the needed information before you need the data in the Social Network Analysis interface

- The data should be in desired row order (Sorted)
- The data should be in desired column order
- All dates, times, and datetimes should be unformatted numeric values
- Column values are displayed with stored case
- Sometimes, column names are case sensitive
SNA Diagram

One of the main features SNA is the ability to displays relationship between selected alert and any other related alerts through the link and nodes.
Building SNA Diagram

At a minimum, two data sources are needed to create a Social network analysis diagram.
Macro input Data Sets

The transactional data set contains the data in which the relationships are to determined.

<table>
<thead>
<tr>
<th>Claim_Number</th>
<th>Name</th>
<th>Role</th>
<th>DateOfLoss</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM4207CL0042</td>
<td>Betsy Adams</td>
<td>Passenger</td>
<td>19173</td>
<td>(908) 588-8644</td>
</tr>
<tr>
<td>DM4207CL0042</td>
<td>Edward Hunter</td>
<td>Passenger</td>
<td>19173</td>
<td>(908) 588-1234</td>
</tr>
<tr>
<td>DM4207CL0042</td>
<td>Hostense Pierce</td>
<td>Passenger</td>
<td>19173</td>
<td>(908) 587-3344</td>
</tr>
<tr>
<td>DM4207CL0042</td>
<td>Tom</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM4208CL0346</td>
<td>Edw</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM4208CL0346</td>
<td>Thor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM4208CL0346</td>
<td>Tom</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM4208CL0346</td>
<td>Row</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM4208CL0346</td>
<td>Whig</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>table_name</th>
<th>var_name</th>
<th>attribute_of</th>
<th>begin_date</th>
<th>end_date</th>
<th>to_cluster</th>
<th>to_display</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkData</td>
<td>Claim_Number</td>
<td>Claim_Number</td>
<td>DateOfLoss</td>
<td>DateOfLoss</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NetworkData</td>
<td>Name</td>
<td>Name</td>
<td>DateOfLoss</td>
<td>DateOfLoss</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NetworkData</td>
<td>Phone</td>
<td>Name</td>
<td>DateOfLoss</td>
<td>DateOfLoss</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Attribute_of – From Node
Var_Name - To Node
Methods of creating Nodes and Link

- User-defined logic
- The OPTGRAPH
- The `%SFS_NET_MAIN_MACROS` macro

The SNA make use of the Macro, this is a compiled macro and another macro that synchronise the names and types of variables.

`%SFS_NET_SYNC_NAMES_TYPES` macro
The main macro call other 4 macros they are:

- Sfs_net_create_graph_data
- Sfs_net_find_conn_comp
- Sfs_net_init_link_macro
- Sfs_net_link_one_table
Calling the Macros

The macro contains five positional parameters
%SFS_NET_MAIN_LINK_MACRO(libref,
    metadata,
    nodes,
    link,
    clustersummary)

The macro has four keyword parameter
%SFS_NET_SYNC_NAME_TYPES(nodesin=data-sets,
    linksin = data-sets,
    nodesout = data-sets,
    linksout=data-sets)
Macro Output Data Sets

### Nodes1

<table>
<thead>
<tr>
<th>node_label</th>
<th>node_id</th>
<th>num_links</th>
<th>cluster_id</th>
<th>node_type</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM4207CL0042</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>CLAIM_NUMBER</td>
</tr>
<tr>
<td>DM4208CL0346</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>CLAIM_NUMBER</td>
</tr>
<tr>
<td>DM4209000063</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>CLAIM_NUMBER</td>
</tr>
<tr>
<td>DM4209000064</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>CLAIM_NUMBER</td>
</tr>
<tr>
<td>DM4209CL0049</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>CLAIM_NUMBER</td>
</tr>
<tr>
<td>DM4209CL0156</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>CLAIM_NUMBER</td>
</tr>
<tr>
<td>Betsy Adams</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>NAME</td>
</tr>
</tbody>
</table>

### Links1

<table>
<thead>
<tr>
<th>cluster_id</th>
<th>begin_date</th>
<th>end_date</th>
<th>from_node</th>
<th>to_node</th>
<th>link_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>23JUN12</td>
<td>.</td>
<td>1</td>
<td>7</td>
<td>-1</td>
</tr>
<tr>
<td>3</td>
<td>13SEP12</td>
<td>.</td>
<td>5</td>
<td>8</td>
<td>-2</td>
</tr>
<tr>
<td>1</td>
<td>29JUN12</td>
<td>.</td>
<td>1</td>
<td>9</td>
<td>-3</td>
</tr>
<tr>
<td>1</td>
<td>03MAY12</td>
<td>.</td>
<td>2</td>
<td>9</td>
<td>-4</td>
</tr>
<tr>
<td>1</td>
<td>31JUL12</td>
<td>.</td>
<td>3</td>
<td>9</td>
<td>-5</td>
</tr>
<tr>
<td>3</td>
<td>13NOV12</td>
<td>.</td>
<td>6</td>
<td>10</td>
<td>-6</td>
</tr>
<tr>
<td>1</td>
<td>31JUL12</td>
<td>.</td>
<td>3</td>
<td>11</td>
<td>-7</td>
</tr>
</tbody>
</table>

### Cluster Summary

<table>
<thead>
<tr>
<th>num_clusters</th>
<th>max_num_nodes</th>
<th>min_num_nodes</th>
<th>avg_num_nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>20</td>
<td>4</td>
<td>11.6666666667</td>
</tr>
</tbody>
</table>
The getSocialNetwork stored process is responsible for displaying the social network in the Network Viewing pane.
Conclusion

Fraud analysts and administrator are responsible for the process of implementing the SAS Fraud Framework

- Fraud prevention and detection is the work of everybody
- The rules needs to be evaluated at interval as the fraudster are always looking for ways
- Where model is used, it should be reviewed
THANK YOU