



SAS® FORUM
UNITED KINGDOM 2015

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

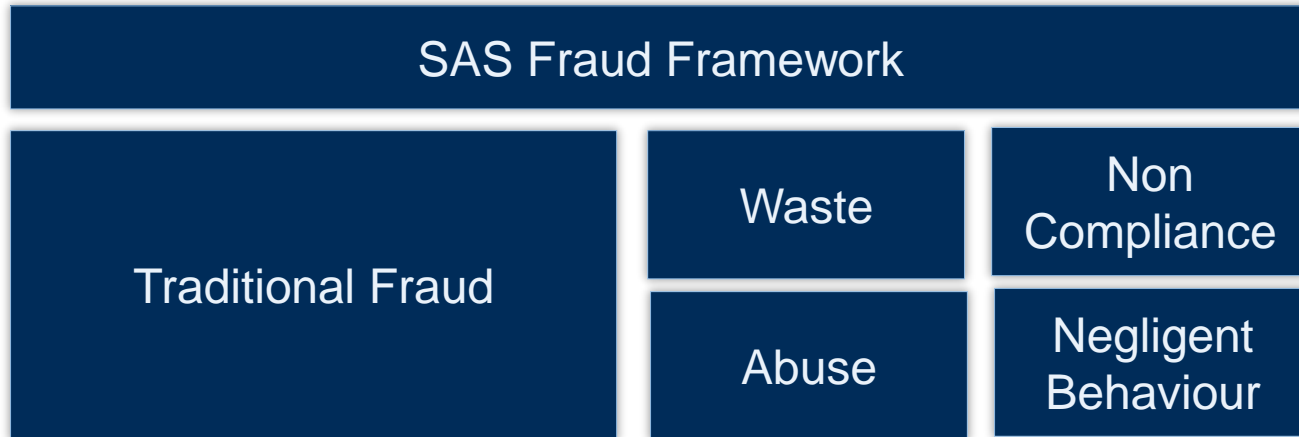


The UK economy lost £52bn from fraud, according to the 2013 report by the National Fraud Authority.

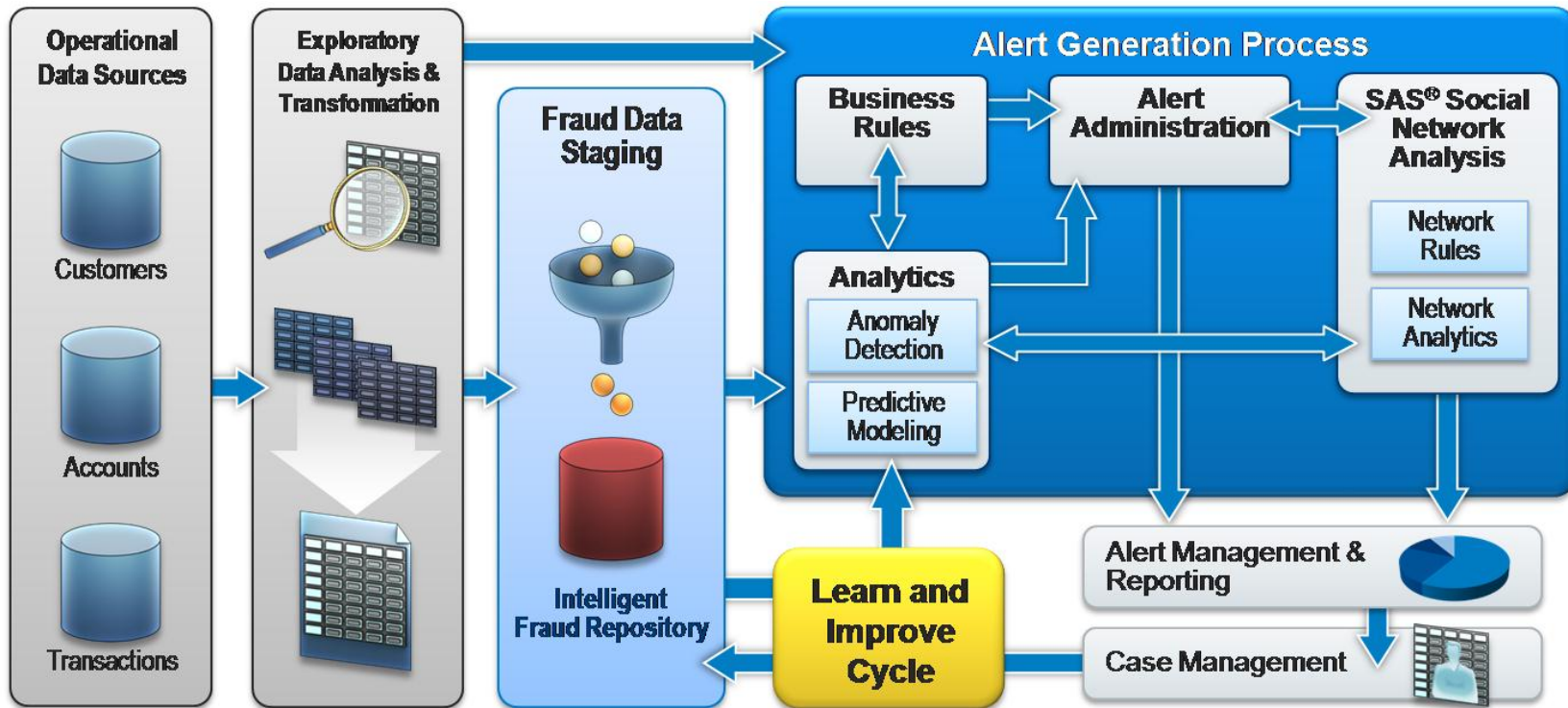
The financial and insurance only experience fraud activities of £5.4bn.

SAS Fraud Framework

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



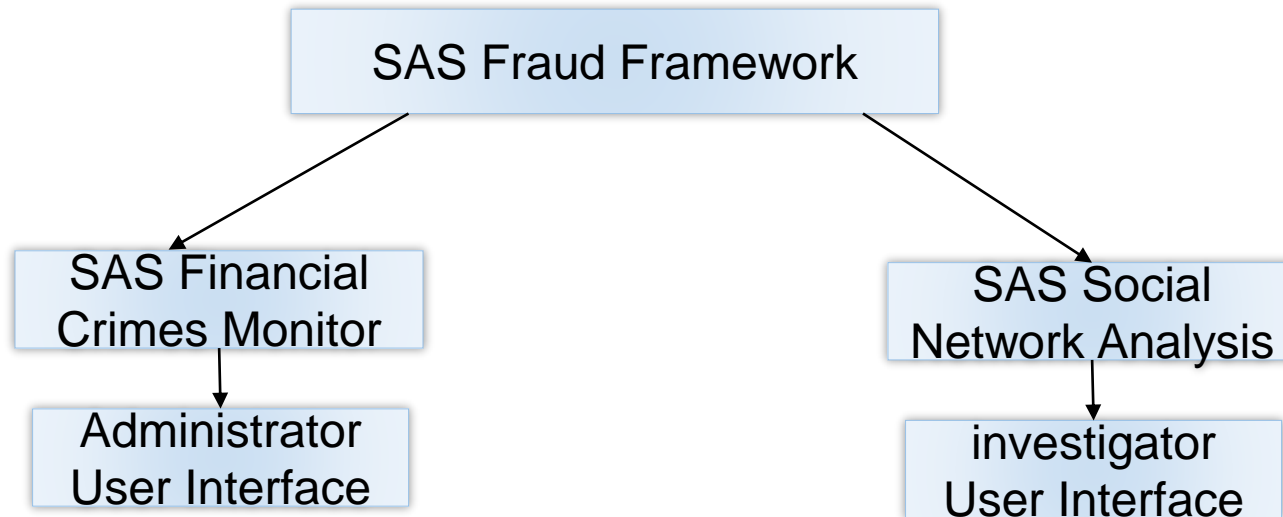
SAS Fraud Framework



SAS Software Product – Fraud Specific

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

User	SAS Products
Platform Administrator	SAS Management Console
Database Administrator	SAS Data Integration Studio
Fraud Administrator	SAS Financial Crime Monitor
Fraud Analyst	SAS Financial Crime Monitor SAS Enterprise Miner SAS Text Miner
Fraud Investigator	SAS Social Network Analysis Server SAS Web Report Studio
Management	SAS Information Delivery Portal SAS BI Dashboard

Financial Crime Monitor (FCM)

SAS Financial Crimes Monitor is an administrator interface responsible for the generation and administration of alerts

The image displays two screenshots of the SAS Financial Crimes Monitor (FCM) interface. The left screenshot shows the 'Log On to SAS' login page with fields for 'User ID:' and 'Password:', and a 'Log On' button. The right screenshot shows the 'SAS Financial Crimes Monitor' main interface. It features a 'Project Tree' on the left with a 'Configured Projects' list, including 'Rule 3 Inflow Fraud Scenario Group'. The main area is titled 'Scenario Group' and contains 'Scenario Group Information' and 'Routing' sections. The 'Scenario Group Information' section includes fields for 'Scenario group name' (Rule 3 Inflow Fraud Scenario Group), 'Purpose' (Fraud), 'Description', 'Group type' (Custom), 'Preprocessing code' (Rule3InflowPreScenario.sas), 'Post-processing code', and 'Status' (Inactive). The 'Routing' section includes a 'Recipient' dropdown (Use default from the Project: (Group) Social Network Analysis Investigator) and a 'Routing rule group' dropdown (Use default from the Project: Online OutFlow Routing Scenario Group).

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 performed during the implementation of the FCM

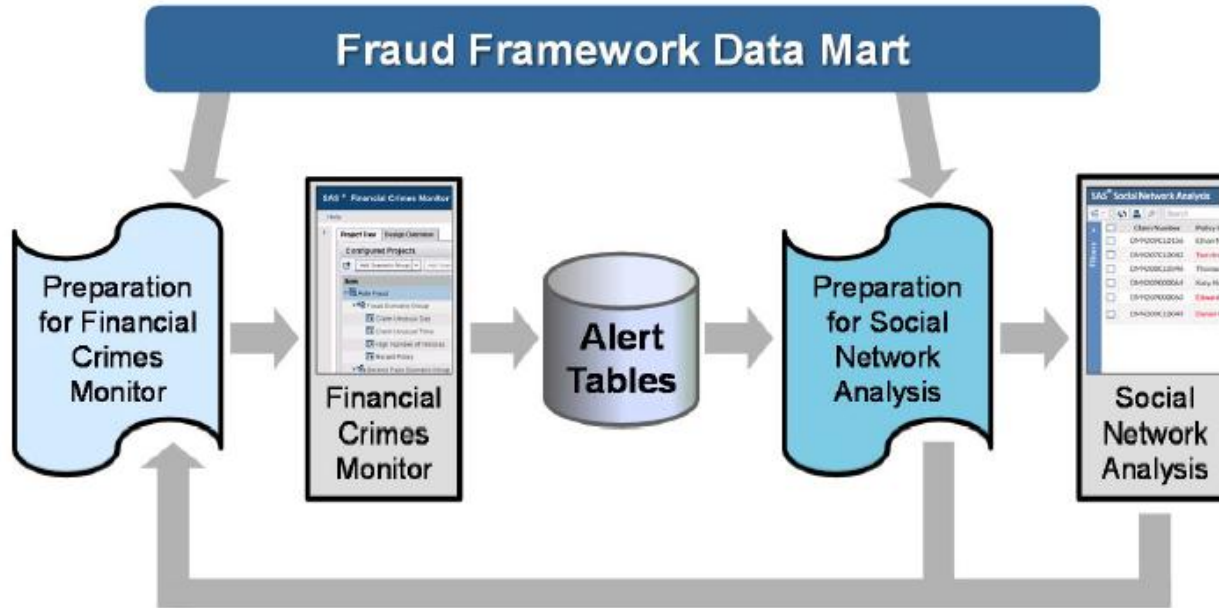
Task	Processing
Pre-Tasks	<p>Create and register Prep and enrichment tables</p> <p>Create and register an alert table template</p> <p>Write SAS programs (scenarios, processing, enrichment, routing, and so on)</p> <p>Create the structure of RDB tables using scripts</p>
Interface Tasks	<p>Enter project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

Task & Processing

Tasks	Processing
Post-Tasks	Modify the FCM_JOB_CALENDAR table Schedule the Alert Generation Process in an application that is not SAS application
Alert Generation Process	FCMMain.sas with AutoExec.sas is sbmitted

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

The screenshot displays the SAS Financial Crimes Monitor interface. The top navigation bar includes the SAS logo and the text "SAS® Financial Crimes Monitor". Below the navigation bar, there are tabs for "Project Tree" and "Design Overview". The "Project Tree" tab is active, showing a list of "Configured Projects" including Tax Fraud, test Entity, Transaction Monitoring, and various Inflow and Outflow Fraud Scenario Groups. The "Scenario Group" configuration page is open, showing the "Scenario Group Information" section. The "Scenario group name" is "Rule 3 Inflow Fraud Scenario Group", the "Purpose" is "Fraud", and the "Group type" is "Custom". The "Preprocessing code" is "Rule3InflowPreScenario.sas" and the "Post-processing code" is empty. The "Status" is "Inactive". The "Routing" section is also visible, showing options for "Recipient" and "Routing rule group".

SAS® Financial Crimes Monitor SAS

Help Log Off

Project Tree | Design Overview

Configured Projects

Add Scenario Group | Add Scenario

Item

- Tax Fraud
- test Entity
- Transaction Monitoring
 - Online Inflow Fraud Scenario Group
 - Online Outflow Fraud Scenario Group
 - Rule 1 Inflow Fraud Scenario Group
 - Withdraw Outflow Fraud Scenario Group
 - Trans Monitor Outflow Second Pass Scenario Group
 - Online Inflow Routing Scenario Group
 - Online OutFlow Routing Scenario Group
 - Rule 1 Routing Scenario Group
 - Withdraw Outflow Routing Scenario Group
 - Online Inflow Suppression Scenario Group
 - Online Outflow Suppression Scenario Group
 - Rule 1 Suppression Scenario Group
 - Withdraw Outflow Suppression Scenario Group
 - Rule 3 Inflow Fraud Scenario Group

Scenario Group

Scenario Group Information

Scenario group name: Rule 3 Inflow Fraud Scenario Group

Purpose: Fraud

Description:

After Group Type is selected and saved, it can be changed only when there are no dependent scenarios in the group.

Group type: Custom

Preprocessing code: Rule3InflowPreScenario.sas

Post-processing code:

Status: Inactive

Routing

Individual and group recipients are defined in SAS metadata and selected from the Recipient option below. A default group is configured during solution installation, and other groups can be defined in SAS metadata. Routing rule groups are created and configured on project-specific Routing Group forms through SAS Financial Crimes Monitor. The routing rule groups must be defined before the list below is populated.

Recipient: Use default from the Project: (Group) Social Network Analysis Investigator

Choose one:

Routing rule group: Use default from the Project: Online OutFlow Routing Scenario Group

Choose one:

Financial Crime Monitor

Adding a new scenario

The screenshot shows the SAS Financial Crimes Monitor interface. On the left, the 'Project Tree' is visible, showing a hierarchy of 'Configured Projects' including 'Transaction Monitoring' and 'Rule 3 Inflow Fraud Scenario Group'. The 'Scenario Group' configuration panel is open, showing fields for 'Scenario group name', 'Purpose', 'Description', 'Group type', 'Preprocessing code', 'Post-processing code', and 'Status'. The 'Routing' section is also visible, with options for 'Recipient' and 'Routing rule group'.

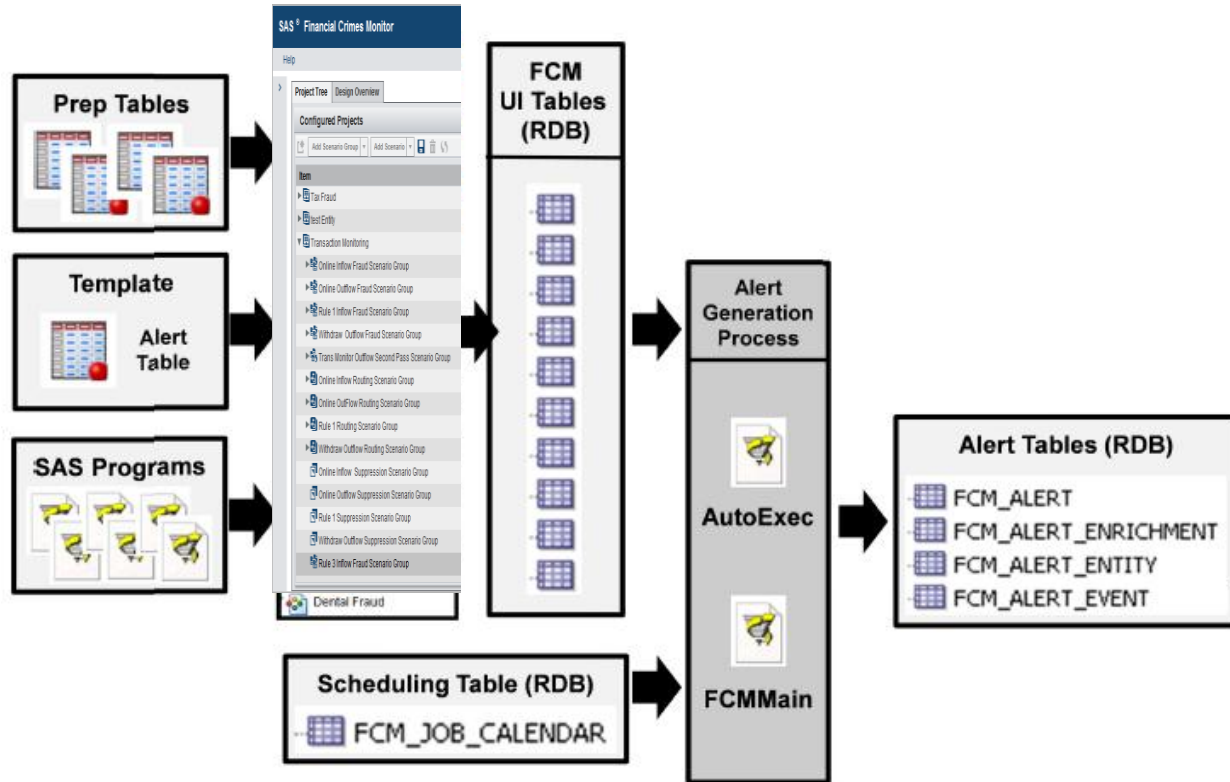
The screenshot shows the SAS Financial Crimes Monitor interface. The 'Scenario' configuration panel is open, showing fields for 'Purpose', 'Scenario type', 'Run frequency', 'Status', 'SAS code', 'Entity', 'Severity score', and 'Weight'. The 'Parameters' section is visible, showing a table with columns for 'Name', 'Value', and 'edit'. The 'Routing' section is also visible, with options for 'Recipient' and 'Routing rule group'.

Name	Value	edit
input_table	Rule3InflowPrep	edit
input_lib	FCMPrep	edit
Rule3_inflow_threshold	10000	edit

Parameter for the Scenario

Summary Implementation steps

This shows the end to end processes for FCM Alert generation



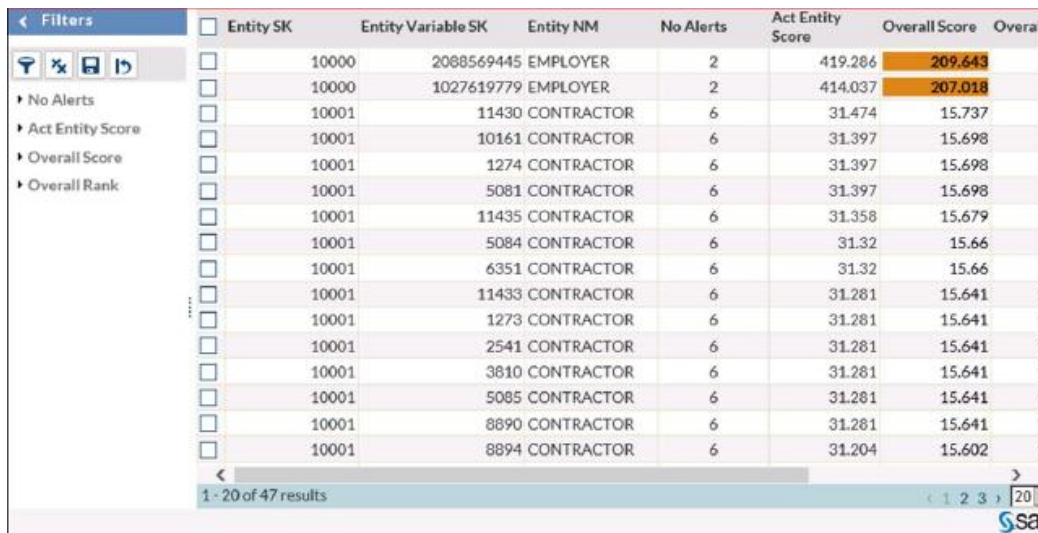
Social Network Analysis

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

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 screenshot displays the Alert Window interface. On the left, there is a 'Filters' pane with a search icon and a list of filter categories: 'No Alerts', 'Act Entity Score', 'Overall Score', and 'Overall Rank'. The main area shows a table of entities. The table has the following columns: Entity SK, Entity Variable SK, Entity NM, No Alerts, Act Entity Score, Overall Score, and Overall Rank. The first two rows are highlighted in orange, indicating they are the top results. The table shows 20 of 47 results.

Entity SK	Entity Variable SK	Entity NM	No Alerts	Act Entity Score	Overall Score	Overall Rank
10000	2088569445	EMPLOYER	2	419.286	209.643	
10000	1027619779	EMPLOYER	2	414.037	207.018	
10001	11430	CONTRACTOR	6	31.474	15.737	
10001	10161	CONTRACTOR	6	31.397	15.698	
10001	1274	CONTRACTOR	6	31.397	15.698	
10001	5081	CONTRACTOR	6	31.397	15.698	
10001	11435	CONTRACTOR	6	31.358	15.679	
10001	5084	CONTRACTOR	6	31.32	15.66	
10001	6351	CONTRACTOR	6	31.32	15.66	
10001	11433	CONTRACTOR	6	31.281	15.641	
10001	1273	CONTRACTOR	6	31.281	15.641	
10001	2541	CONTRACTOR	6	31.281	15.641	
10001	3810	CONTRACTOR	6	31.281	15.641	
10001	5085	CONTRACTOR	6	31.281	15.641	
10001	8890	CONTRACTOR	6	31.281	15.641	
10001	8894	CONTRACTOR	6	31.204	15.602	

DETAIL TAB

The details tab is displayed after you click on an alert row in the alert pane.

The screenshot displays the SAS Social Network Analysis interface. The 'Details' tab is active, showing information for a specific alert. The alert title is 'High ratio of BI vs. APD: \$25,000 in BI vs. \$850 in APD'. The alert score is 250. Other details include Policy Holder: Ethan Mitola, Policy Number: DM1_PAU_0005, Claim Number: DM4209CL0156, Score: 895, Reserve: \$44,350.00, and Reserve Severity: 3.

The 'Key Performance Indicators' section shows a bar chart with the following data:

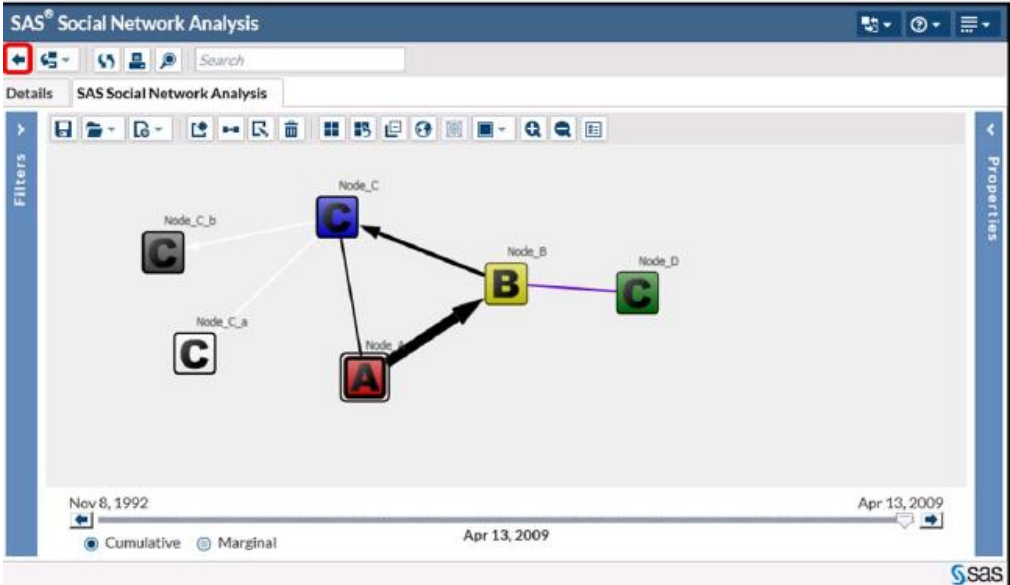
Alert Type	Alert Score
Total Alert Score	895
High ratio of BI vs. APD	250
All injuries are soft tissue	175
Homogeneous behavior	150
High induced accident score	120

The 'Related Alerts' section shows a table of related alerts:

Timeoffloss	Alert Id	Alert Score
November 13, 2012 10:00:00 PM	7	250
November 13, 2012 10:00:00 PM	37	175
November 13, 2012 10:00:00 PM	6	150
November 13, 2012 10:00:00 PM	36	120
November 13, 2012 10:00:00 PM	38	100
November 13, 2012 10:00:00 PM	5	100

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

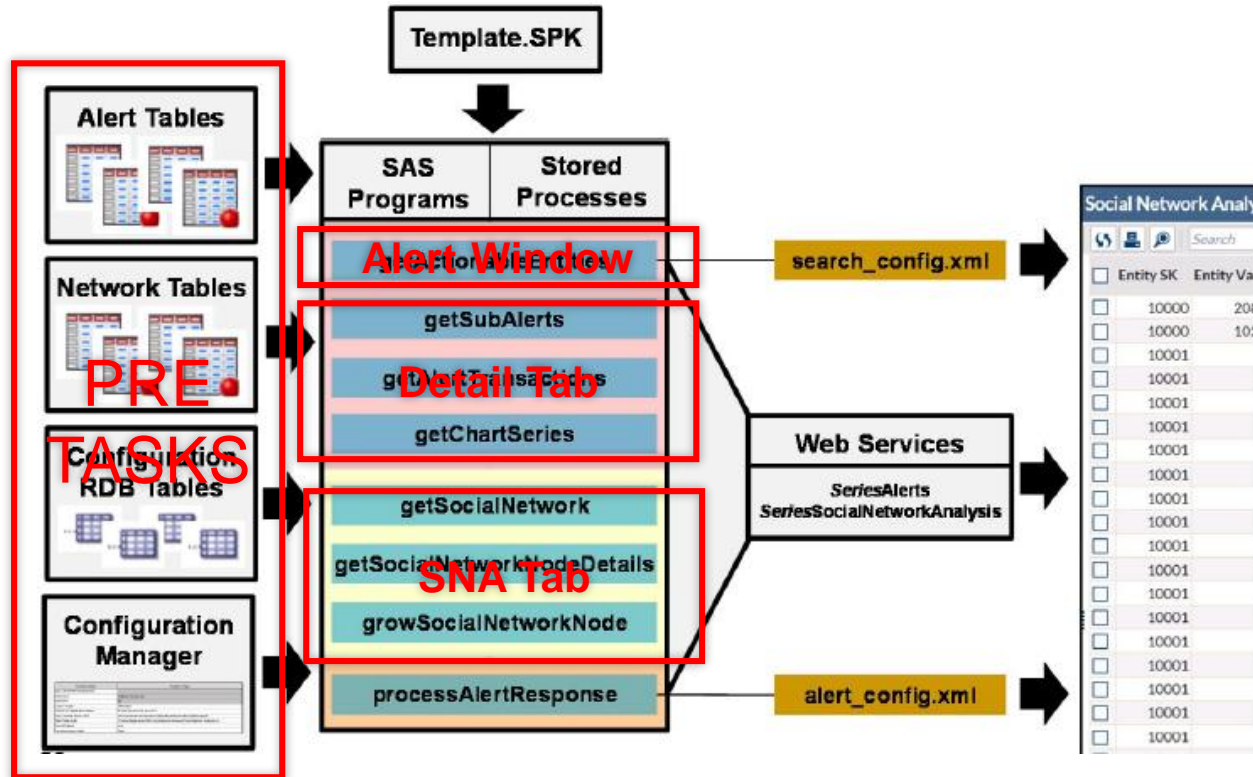
- Implement the getSubAlerts stored process
- Implement the getAlertTransactions stored process
- Implement the getChartSeries stored process

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 ...



Best practice for SNA input Data

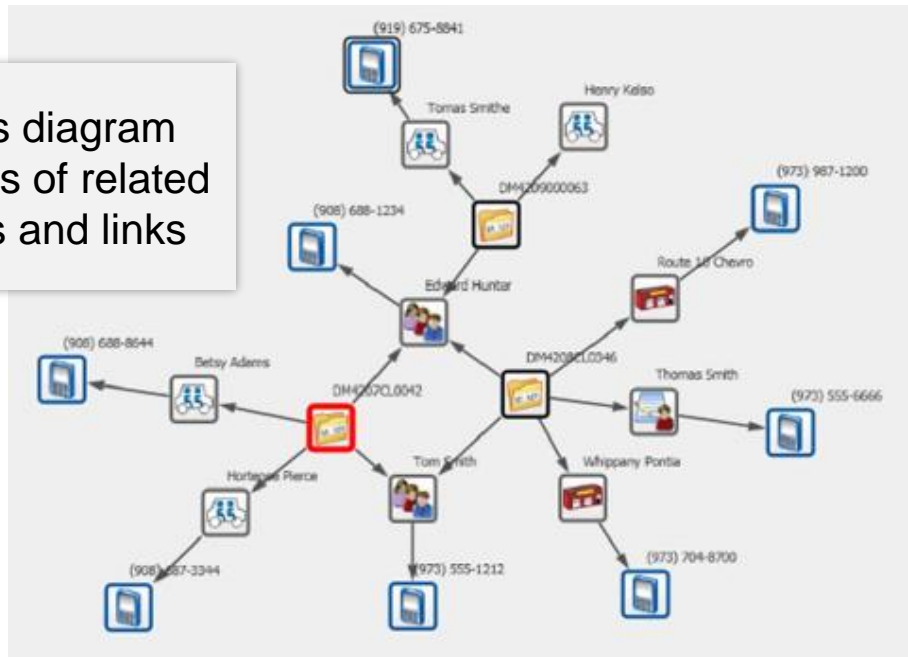
A best practice is to create input data tables with all the needed information before you need the data in the Social Network Analysis interface

- 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

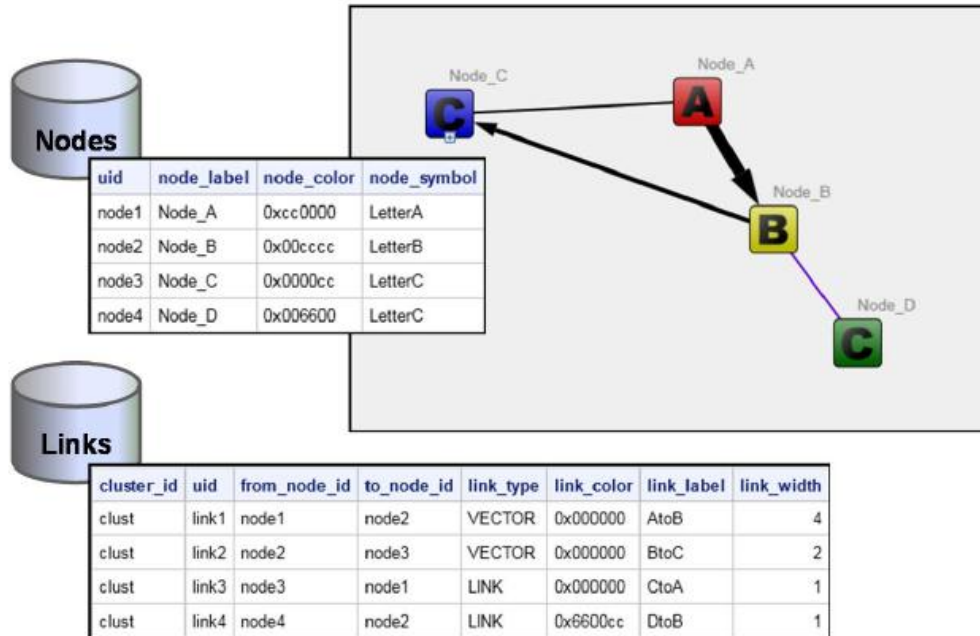
One of the main features SNA is the ability to displays relationship between selected alert and any other related alerts through the link and nodes.

Alerts diagram consists of related nodes and links



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

Claim_Number	Name	Role	DateOfLoss	Phone		
DM4207CL0042	Betsy Adams	Passenger	19173	(908) 688-8644		
DM4207CL0042	Edward Hunter	Passenger	19173	(908) 688-1234		
DM4207CL0042	Hortense Pierce	Passenger	19173	(908) 687-3344		
DM4207CL0042	Tom					
table_name	var_name	attribute_of	begin_date	end_date	to_cluster	to_display
DM4208CL0346	Edwa	NetworkData	Claim_Number	DateOfLoss		
DM4208CL0346	Thon	NetworkData	Name	DateOfLoss	1	1
DM4208CL0346	Tom	NetworkData	Phone	DateOfLoss	1	1
DM4208CL0346	Rout	NetworkData	Name	DateOfLoss	1	1
DM4208CL0346	Whip					
DM4209000063	Edward Hunter	PolicyHolder	19205	(908) 688-1234		
DM4209000063	Henry Kelso	Passenger	19205			
DM4209000063	Tomas Smithe	Passenger	19205	(919) 675-8841		
DM4209000064	Jason Marks	Passenger	18992			
DM4209000064	Katy Hunter	PolicyHolder	18992	(773) 561-0976		

Metadata

Network Data

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

%SFS_NET_MAIN_MACROS 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

node_label	node_id	num_links	cluster_id	node_type
DM4207CL0042	1	4	1	CLAIM_NUMBER
DM4208CL0346	2	5	1	CLAIM_NUMBER
DM4209000063	3	3	1	CLAIM_NUMBER
DM4209000064	4	2	2	CLAIM_NUMBER
DM4209CL0049	5	2	3	CLAIM_NUMBER
DM4209CL0156	6	3	3	CLAIM_NUMBER
Betsy Adams	7	2	1	NAME
Deniel Mitch	8	2	2	NAME

Nodes1

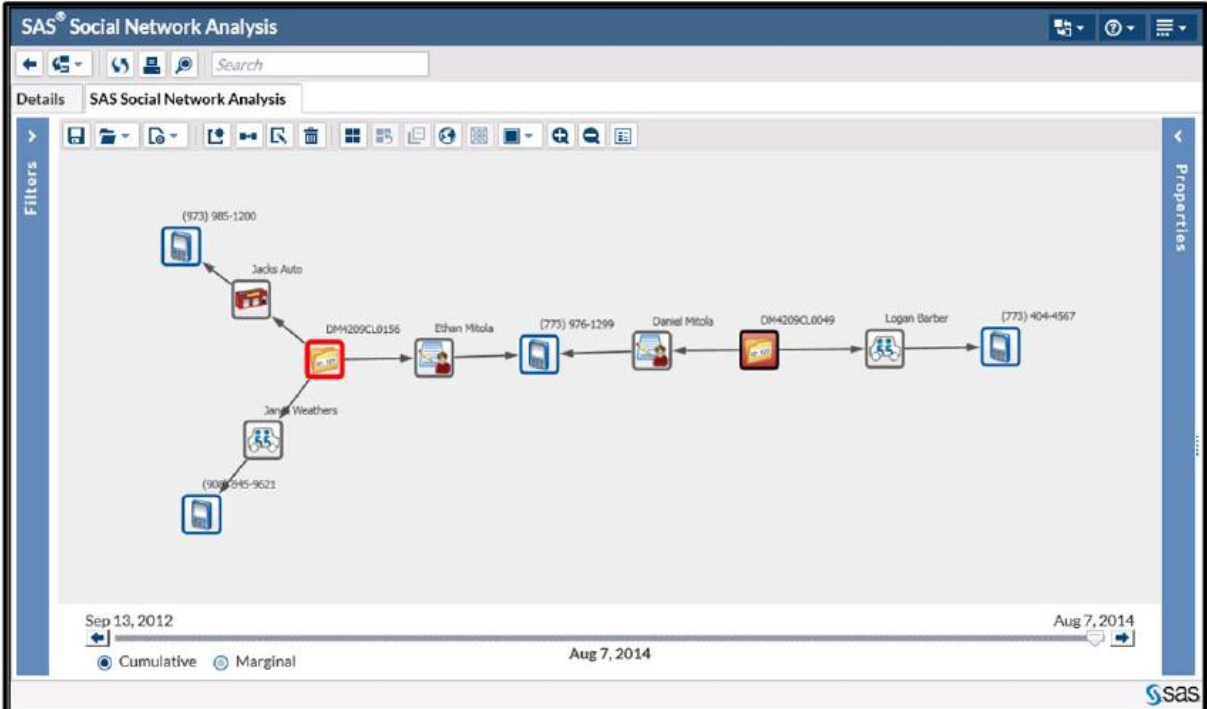
cluster_id	begin_date	end_date	from_node	to_node	link_id
1	29JUN12	.	1	7	-1
3	13SEP12	.	5	8	-2
1	29JUN12	.	1	9	-3
1	03MAY12	.	2	9	-4
1	31JUL12	.	3	9	-5
3	13NOV12	.	6	10	-6
1	31JUL12	.	3	11	-7
1	29JUN12	.	1	11	-8

Links1

num_clusters	max_num_nodes	min_num_nodes	avg_num_nodes
3	20	4	11.666666667

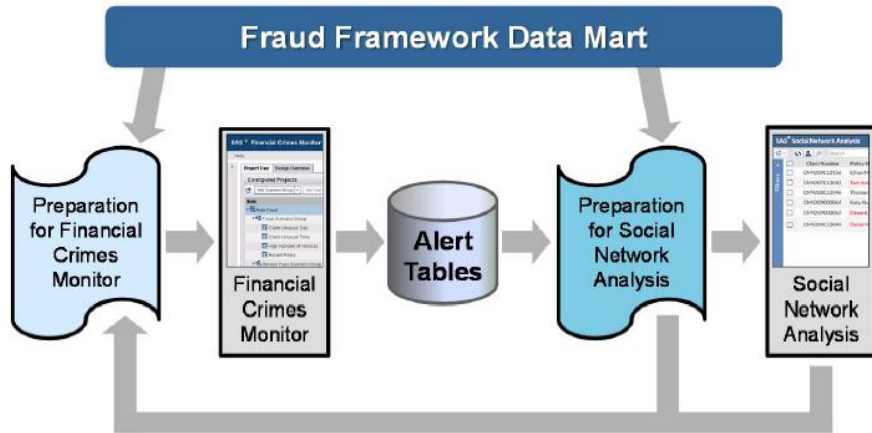
Cluster Summary

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





SAS® FORUM
UNITED KINGDOM 2015



THE
POWER
TO KNOW.

www.SAS.com