SAS Forum

Transactional Fraud

Filip Verbeke, Sales Manager Fraud Solutions • South West Europe
Digital channels are under attack....

Key Business drivers

- A need for multi-layer, analytics-driven & real time detection
- Increase organisational efficiency
- Reduce fraud losses and false positives and improves value detection rates
- Tackling money mules
- Improve customer experience and bank’s reputation

NEWS RELEASE

CUSTOMERS URGED TO BE VIGILANT AS FRAUDSTERS INCREASE SCAM ATTACKS

- Card fraud rises, but as a proportion of spending remains flat at 7.4p for every £100 spent during first half of 2014
- Rise in remote banking fraud losses as criminals target businesses and consumers through telephone ‘phishing’ and computer viruses
- Banks highlight warning signs of scams, and support calls made by City of London Police Commissioner for national awareness campaign

Losses on remote banking fraud rose to £35.9 million, up 59 per cent from £22.6 million in 2013. Within this total, online banking fraud losses rose to £25.3 million, up 71 per cent from £17.1 million in 2013. Telephone banking fraud rose to £8.6 million, up 20 per cent from £7.5 million. Intelligence suggests criminals are targeting business accounts which typically allow higher value fraudulent transactions.

The Telegraph

Online banking fraud up 71pc despite rise of log-in gadgets

Fraud losses on UK cards have jumped 42pc year-on-year with a 71pc surge in online banking fraud
An ever-changing myriad of attack vectors

- **Business Customers**
  - Phishing / social engineering for credentials

- **Retail Customers**
  - Man-in-the-middle attack
  - Account take-over
  - False Tx

- **Merchants**
  - Stolen cards

- **Weak 3rd parties with card data**
  - Collect CC data
  - Sell CC data

- **Payments**
  - Payee setup
  - Account creation

- **Online**
  - Tamper with payment files

- **Phone**
  - Mules
  - Pre-pay Debit cards

- **Fax**
  - IT Teams
  - Time-bombed destructive patches

- **Cards**
  - Collect CC data
  - Infected machine / execute Tx

- **DDoS**

- **Threat hits people or IT, outcome is fraud or denial of service**

**SAS FORUM RUSSIA 2015**

- **Stolen cards**
  - Collect CC data
Cyber Security

Data Sources
- Logs and alerts
- Bank Business Tx
- Firewalls / IDS / SIEM
- Anti-Virus
- Machine logs
- Web logs
- External “bad lists”

Data Integration / Enhance data / Networked data
- IT activity
- Business Tx activity
- Internet activity

Analytics / Kill chain analysis
- Prioritised alerts

Detection and Alerting
Hybrid Analytics Model

End user services
- Reporting / explore & search data
- Case Management

Cyber FRAUD

IT activity

Business Tx activity

Internet activity

Copyright © 2015, SAS Institute Inc. All right reserved.
CYBER CRIME IS A BIG DATA STORY

USER EXPERIENCE & MANAGEMENT

Data Input
Build Scenarios
Simulation / Deployment (Simulation available in GA Release)
Alert Generation / Case Management
Monitor & Report

SAS® LASR™ ANALYTIC SERVER

SAS® DEPLOYMENT ENVIRONMENTS

BATCH/IN-DATABASE
IN-MEMORY
REAL-TIME & STREAMING

The technology response
Event Stream Processor

EVENT STREAM PROCESSING ENGINE: EVENT-DRIVEN, FLOW-CENTRIC

- Publish / subscribe
- Inserts/updates/deletes
- Continuous queries
  - Aggregate (group by)
  - Correlate (join)
  - Compute
  - Filter
  - Procedural
  - User defined functions
  - Retention windows
  - Pattern matching
- Ad-hoc queries
- Command & control
- Security (Auth, Encrypt, AC)
- Persistence / recovery
- Fail-over
- Distributed services
- Model management
“Companies are reevaluating how they tackle security since a fragmented approach is consistently leaving organizations at greater risks of attack. A more holistic approach to security ensures all layers of protection function together.”

Avivah Litan, VP Distinguished Gartner Analyst
ONLINE BANKING PAYMENTS FRAUD
POINTS OF VULNERABILITY FOR ONLINE FRAUD

**Point of exit**
- New beneficiaries
- Velocity of transactions
- Suspicious session activity

**Create alerts!**

**Point of compromise**
Score incoming transactions for:
- Anomalous behaviour
- Change of details
- Drain of funds from savings account (me2me transfers)

**Customer behaviour**
Score customers over their lifetimes for:
- Possible mule accounts
- Victim propensity
- Appearance on a watch-list
- Unusual behaviour

**OPEN BOX SOLUTION COVERING ALL AREAS**
High performance analytics

- **Anomaly detection (example):** The client is accessing their account from a new channel
- **SNA (example):** Links to mule account such as a shared mobile number
- **Business rule (example):** Transaction above $xx to a new beneficiary

**SAS HYBRID ANALYTICAL METHODS**

- **Alert Generation Process**
  - Anomaly Detection
  - Predictive Modeling
  - Database Searches
  - Automated Business Rules
  - Text Mining

**LEVELS OF DETECTION**

- Network
- Entity
- Event

**Predictive modelling (example):** Model based on variables such as payment amount and balance

**Database Searches (example):** Looking for matches across the Black-Lists

**Text mining (example):** Transaction narrative showing suspicious payments
Real Time Decisioning
What was the problem?

Victim

Current Account

16:08 8.600€
16:14 30.000€
16:45 49.457€
17:08 7.000 €

Saving Account

16:11 6.025 €
16:13 3.128 €
16:16 3.128 €
16:18 3.128 €
16:39 3.128 €
16:42 2.981 €
17:09 74.561 €

Mules

16:11
16:13
16:16
16:18
16:39
16:42
17:09

Cash-out

4 ATM  ➔  3.600 €
2 POS  ➔  2.341 €
1 ATM  ➔  520 €
7 POS  ➔  2.592 €
2 ATM  ➔  831 €
8 POS  ➔  1.997 €
1 ATM  ➔  598 €
1 ATM  ➔  700 €
6 POS  ➔  2.377 €
1 ATM  ➔  480 €
5 POS  ➔  2.388 €

S 1
S 2

17:11 68.211 €
17.20 2.900 €
FMF Project

POTENTIAL PHASE I IMPACT

AS-IS
- Average 14,000 alerts per day
- 50% detection rate
- 0.01% of alerts are fraud

PHASE I*
- Average ±40 alerts per day
- 90% Detection rate
- 2.5% of alerts are fraud

* Indicated by an analysis on historical data – no guarantees towards future performance
The ROC chart shows how well the model is able to be specific (catch only “bads”) and sensitive (catch all “bads” simultaneously). Sensitivity and 1-Specificity are displayed for various cutoff values. The more the chart bends to the top left, the better.

The ROC measures the area under the curve. The bigger the area, the better the model. A perfect model will have a ROC close from 1.

ROC >0.9 very good model
ROC > 0.8 good model
ROC > 0.7 ok model

Sensitivity = True Positive Rate = TP / (TP + FN)
Specificity = True Negative Rate = TN / (FP + TN)
Transaction Amount: 3499 eur
Beneficiary has a very high mule probability
Benef is BNP Customer and Nationality is Belgian
Preceding transaction is MetoMe
Preceding transaction is in last 15 min
Originator has more than 63 year old
Originator is french speaking
Transaction time is 4pm on friday
Communication Field is not blank

\[
= 26+17+\ldots-71 = 421 \text{ points} > \text{CUT-OFF} \Rightarrow \text{Alert}
\]
SOLUTION BENEFITS

- More suspicious cases identified
  - Including both previously undetected fraudulent networks and extensions to already identified fraud
- Reduction in false positive rates
  - Significant improvement in ‘quality’ of suspicious cases past for investigation
- Improved investigation efficiency
  - Each referral taking 1/2 – 1/3 the time to investigate using SAS’ link analysis visualization
- One consistent, end to end, underlying platform
  - Platform can also be leveraged for credit risk, card risk, AML and FATCA
CARD FRAUD
“Unlimited Operation”

Targeted 2 Payments Processors

RAKBANK (United Arab Emirates)
Bank of Muscat (Oman)

10 hours
24 countries
36,000 transactions
$40 million USD
ADVANCED ANALYTICS

- Advanced patent analytics to detect risk exposure and fraud with less customer inconvenience.
- Multi-entity Statures
- Hybrid Model Technology (Custom)
- Enhanced API

Enterprise Platform

- Single Platform processing for all Products & Channels; Deposit, ACH, Wire, Cards, Payments, Acquirer, Mobile Banking, Online, etc.

100% Real-Time Decision

Ability to score and decision 100% of all transaction types in real-time, all LOBs.

Fraud Management Operation

Multi-Org structure to manage multi-client (Processor) or ‘Silo’ environment. Separation of data, cases and rules control per business requirements

Integration

Integration with other fraud/risk solutions (Link Analysis, AML, etc.)
NEURAL NETWORK MODEL COMPONENTS

**Input**
- Signatures
- Transaction
- Geographic data

**Neural Network Model**

**Score with Reason Codes**
**Highlights**

- Ability to decision 100% of *ALL* transactions in real-time
- Enhanced signature approach that incorporates cross-product / cross channel data
- Ability to leverage additional data in fraud decision process (expanded API to include non-monetary, e-banking, mobile channel, etc...)
- Incremental fraud detection over incumbent – SAS detects 47% more fraud at 20:1 AFPR.
- Enterprise Solution – Establish platform for transaction decisioning across all bank products and channels
Challenges

- Source data once and use across many different business purposes
- Modernize analytics approach for banks largest credit card portfolio
- Generate more revenue from enhanced risk based approach to credit & fraud decisioning
- Enterprise analytical approach: striking balance between customer experience and fraud losses

Real time credit & fraud decisions

- Replacing home grown system
- ROI: 100 million $ in Y1, of which 60 million $ from new revenue and 40 million $ from fraud loss reduction.
- Operational cost reduction: from 3000 rules to 100 rules and a single model
- Credit and fraud: credit decisioning + fraud decisioning – single data source
Cyber Security

Many potential data sources:

- Netflow / IP traffic
- Door swipe
- Web Proxy
- Business Tx
- External hotlist

Network components:

- Router: 77.110.65.38
- Firewall: 192.168.10.44

Security systems:

- SIEM
- IPS/IDS
- Cisco
- CheckPoint
- Palo Alto Networks
- Fortinet
- Tipping Point
- SourceFire
- McAfee
- Kaspersky Labs
- Trend Micro
- Semantec
- MS SCOM
- SAP ERM
- SNMP
- VMWARE

Data sources:

- HP ArcSight
- IBM Q1 Labs
- Quest Software
- Splunk
- Active Directory
- Enterprise Storage
- Database
- Application Server
- Workstation
- Internet
- Splunk
- IBM Q1 Labs
- Quest Software
- Splunk
**SAS solution**

- Hundreds/Thousands of alerts per day
- Ad-hoc and reactive
- Rules & Signature based

---

**Current Environment:**

**Future State:**

SAS Advanced Analytics

---

- High Performance Analytics + Real Time Decisioning
- Hybrid Analytics to derive contextual awareness & risk prioritization
- Identify patterns of behaviors, compromised accounts & high risk activity
- Ability to identify the threat *before* the data loss
NETFLOW ANALYTICS FEATURES

- Contextual data enrichment. Augments network flow with business information and external threat data to detect cyberrisks based on your specific business workflows.
- "Right-timed," multilayered analytics. Optimizes the speed and complexity of analytics across the real-time, near-time and "any-time" continuum for faster and deeper situational awareness.
- Visual data exploration. Enables risk exploration without requiring previous analytics knowledge or expertise.
- Continuously updated intelligence. Behavioral analytics automatically evolve cyberanalytic models based on new events, new data and new context.
- Cost-efficient, optimized data storage. Reduces your storage footprint by saving only the relevant data for analysis on commodity hardware.