SAS® FORUM
RUSSIA 2015

SAS Forum

Transactional Fraud

Filip Verbeke, Sales Manager Fraud Solutions ▪ South West Europe

THE POWER TO KNOW.

Digital channels are under attack….

SAS FORUM RUSSIA 2015

FFA Financial Fraud Action UK — Working together to prevent fraud
Cheque & Credit Clearing Company
THE UKCARDS ASSOCIATION

ADDRESS
2 Thomas More Square
London
E1W 1YN
WEBSITE
www.financialfraudaction.org.uk
DIRECT LINE
020 3217 8436
EMAIL
press@ukcards-ffauk.org.uk

NEWS RELEASE

CUSTOMERS URGED TO BE VIGILANT AS FRAUDSTERS INCREASE SCAM ATTACKS

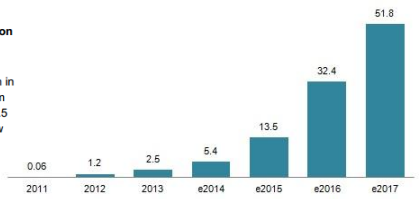
- **Card fraud rises, but as a proportion of spending remains flat at 7.4p for every £100 spent during first half of 2014**
- **Rise in remote banking fraud losses as criminals target businesses and consumers through telephone 'Vishing' and computer viruses**
- **Banks highlight warning signs of scams, 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 £29.3 million, up 71 per cent from £17.1 million in 2013. Telephone banking fraud rose to £6.6 million, up 20 per cent from £5.5 million. Intelligence suggests criminals are targeting business accounts which typically allow higher value fraudulent transactions.

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

Number of Unique New Mobile Malware Strains Released Per Year, 2011 to e2017 (In millions)
Source: Aite Group



The Telegraph

Home | Video | News | World | Sport | Finance | Comment | Culture | Travel | Life | Women
Companies | Comment | Personal Finance | ISAs | Economy | Markets | Property | Festival of
ISAs | Investing | Pensions | Savings | Interest Rates | Funds | Mortgages | Credit Cards | Ex
HOME » FINANCE » PERSONAL FINANCE » BANK ACCOUNTS

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

Fraud losses on UK cards have jumped 15pc year-on-year with a 70pc surge in online banking fraud

sas THE POWER TO KNOW.

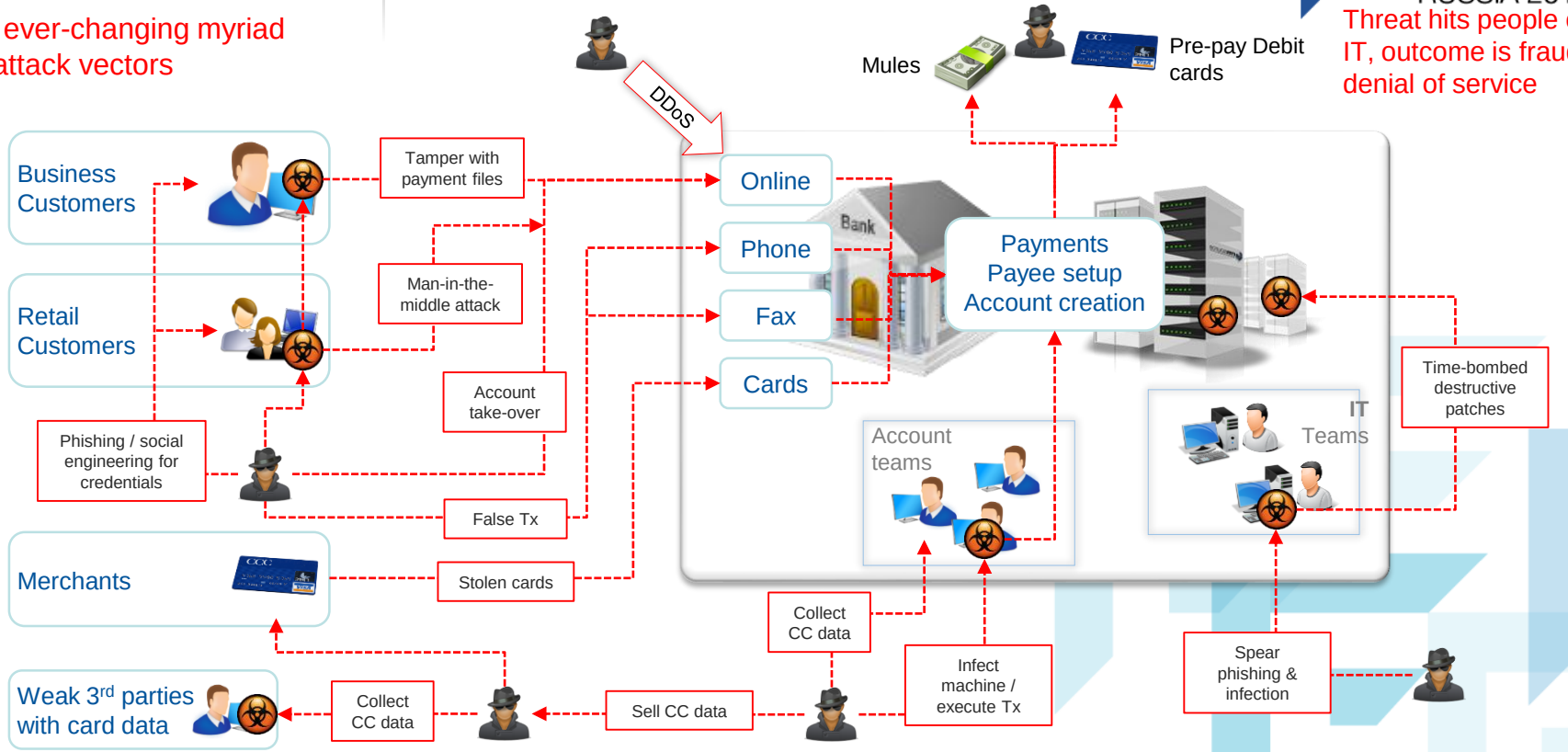
Cyber Security

CYBER THREAT LANDSCAPE FOR BANKS

SAS FORUM RUSSIA 2015

An ever-changing myriad of attack vectors

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



SAS THE POWER TO KNOW.

Cyber Security

CYBER FRAUD

SAS FORUM RUSSIA 2015

Data Sources

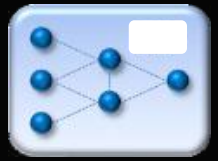
- Logs and alerts
- Bank Business Tx
- Firewalls / IDS / SIEM
- Anti-Virus
- Machine logs
- Web logs
- External "bad lists"

Data Integration / Enhance data / Networked data

Pre-filter → IT activity

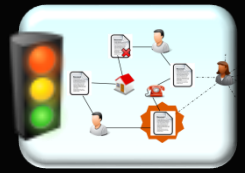
Pre-filter → Business Tx activity

Pre-filter → Internet activity

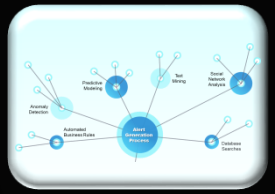


Analytics / Kill chain analysis Detection and Alerting

Prioritised alerts



Hybrid Analytics Model



End user services

Reporting / explore & search data

Case Management

Cyber Security

CYBER SECURITY

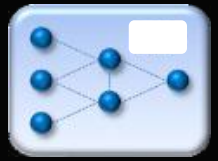
SAS FORUM RUSSIA 2015

Data Sources

- Logs and alerts
- Accounts
- Financial Tx
- Non-financial Tx
- Staff activity
- Cyber alerts
- External "bad lists"

Data Integration / Enhance data / Networked data

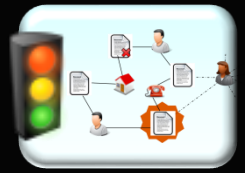
- Pre-filter
- DQ
- Aggregate



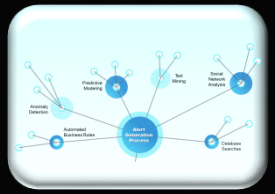
- Tx
- Entity
- Network

Analytics / Fraud models Detection and Alerting

Prioritised alerts



Hybrid Analytics Model



End user services

Reporting / explore & search data

Case Management

The technology response

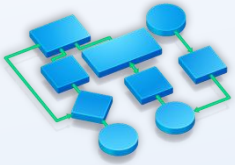
CYBER CRIME IS A BIG DATA STORY

USER EXPERIENCE & MANAGEMENT

Data Input

Build Scenarios

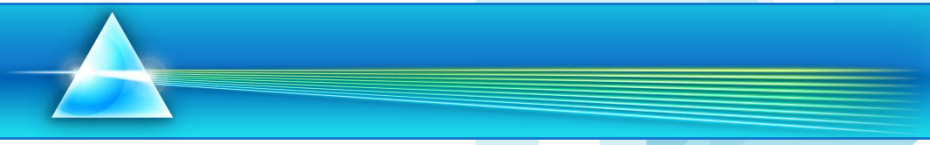
Simulation / Deployment
(Simulation available in GA Release)



Alert Generation / Case Management

Monitor & Report

SAS® LASR™ ANALYTIC SERVER



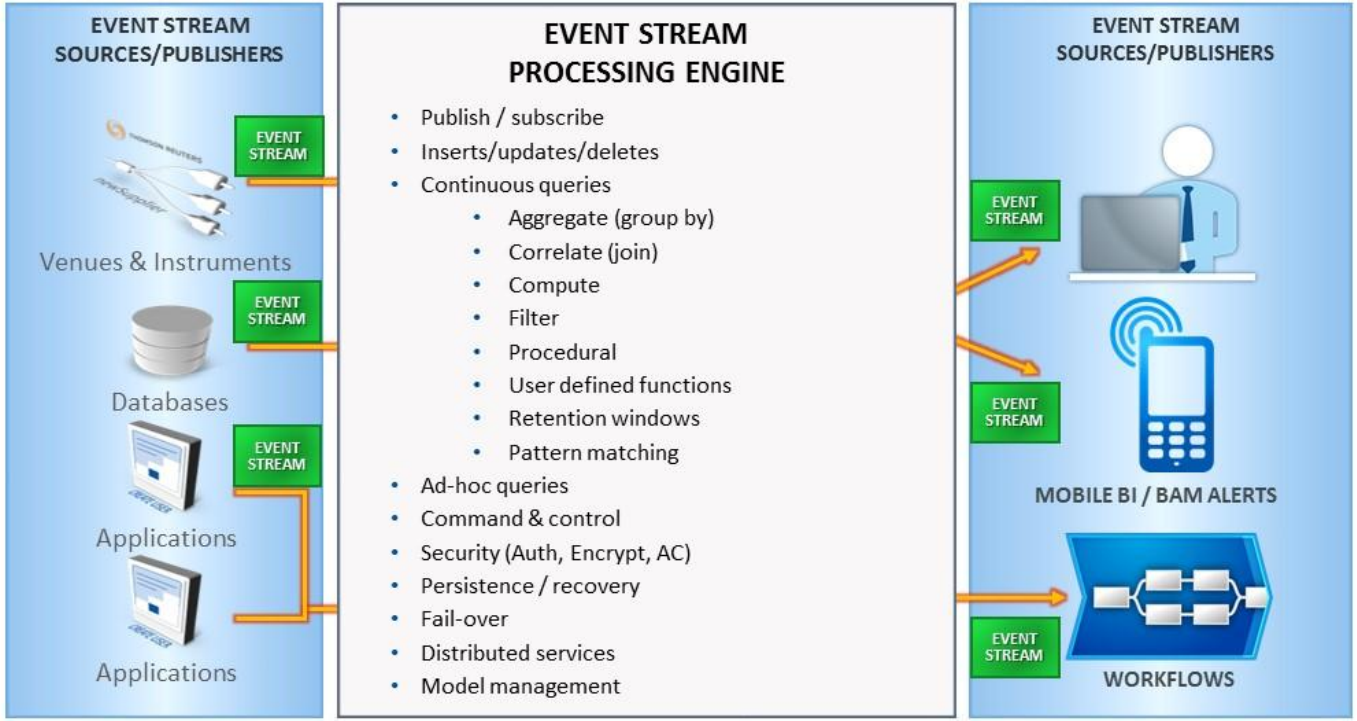
SAS® DEPLOYMENT ENVIRONMENTS

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

Event Stream Processor

SAS FORUM RUSSIA 2015

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



sas THE POWER TO KNOW.

SAS® SECURITY INTELLIGENCE

LAYERED APPROACH

"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

Layer 1	Layer 2	Layer 3	Layer 4	Layer 5
ENDPOINT CENTRIC: Authentication, Device ID, Geo Location	**NAVIGATION CENTRIC:** Analyzes session behavior	**CHANNEL CENTRIC:** Monitors account behavior for a channel	**CROSS CHANNEL CENTRIC:** Monitors entity behavior across channels	**ENTITY LINK ANALYSIS:** Enables Analysis of Relationships

ONLINE BANKING PAYMENTS FRAUD

POINTS OF VULNERABILITY FOR ONLINE FRAUD

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

Point of exit

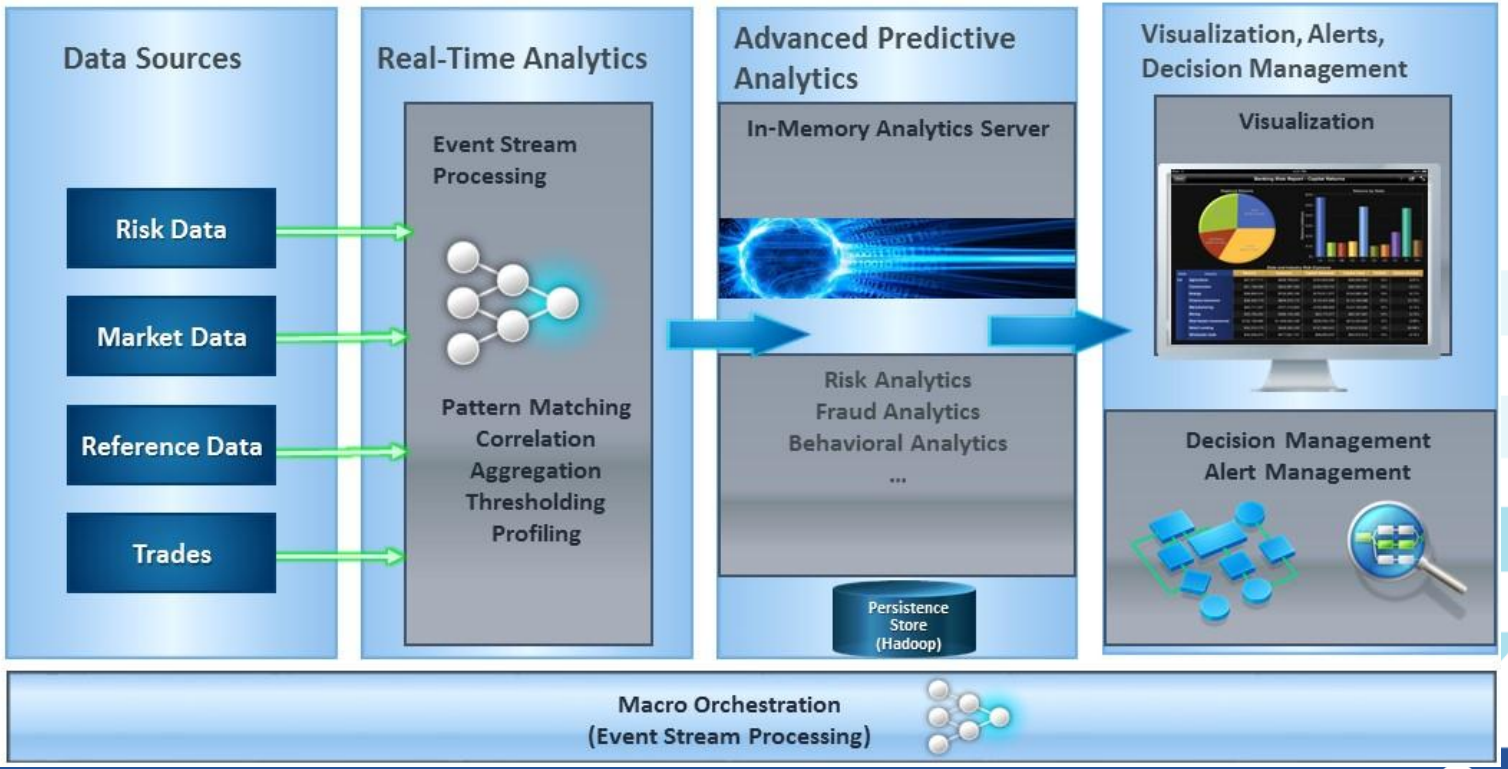
- New beneficiaries
- Velocity of transactions
- Suspicious session activity

✓ **Create alerts!**

Real time, in memory

SAS FORUM RUSSIA 2015

HYBRID (MULTI-STAGED) DATA ANALYTICS



THE POWER TO KNOW.

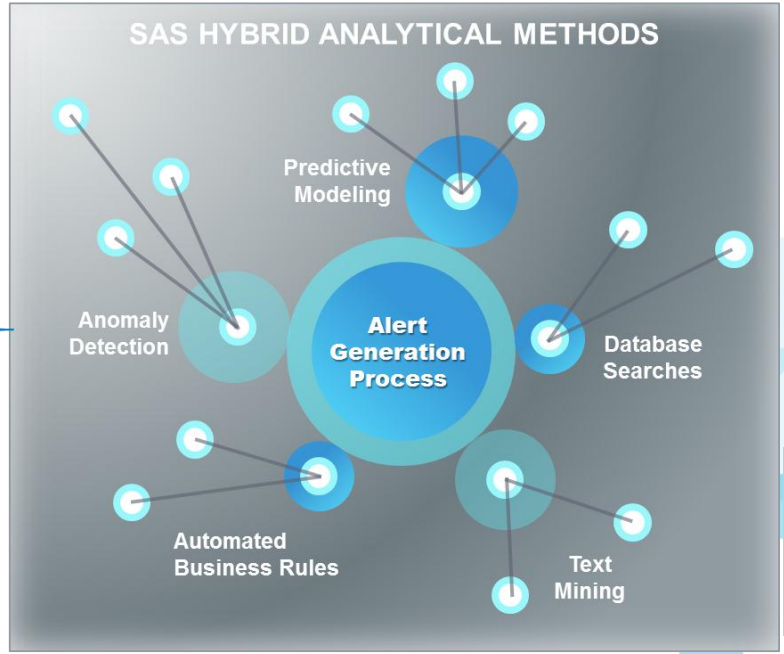
High performance analytics

UNIQUE HYBRID APPROACH TO ANALYTICS

SAS FORUM RUSSIA 2015

SNA (example): Links to mule account such as a shared mobile number

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



Anomaly detection (example): The client is accessing their account from a new channel

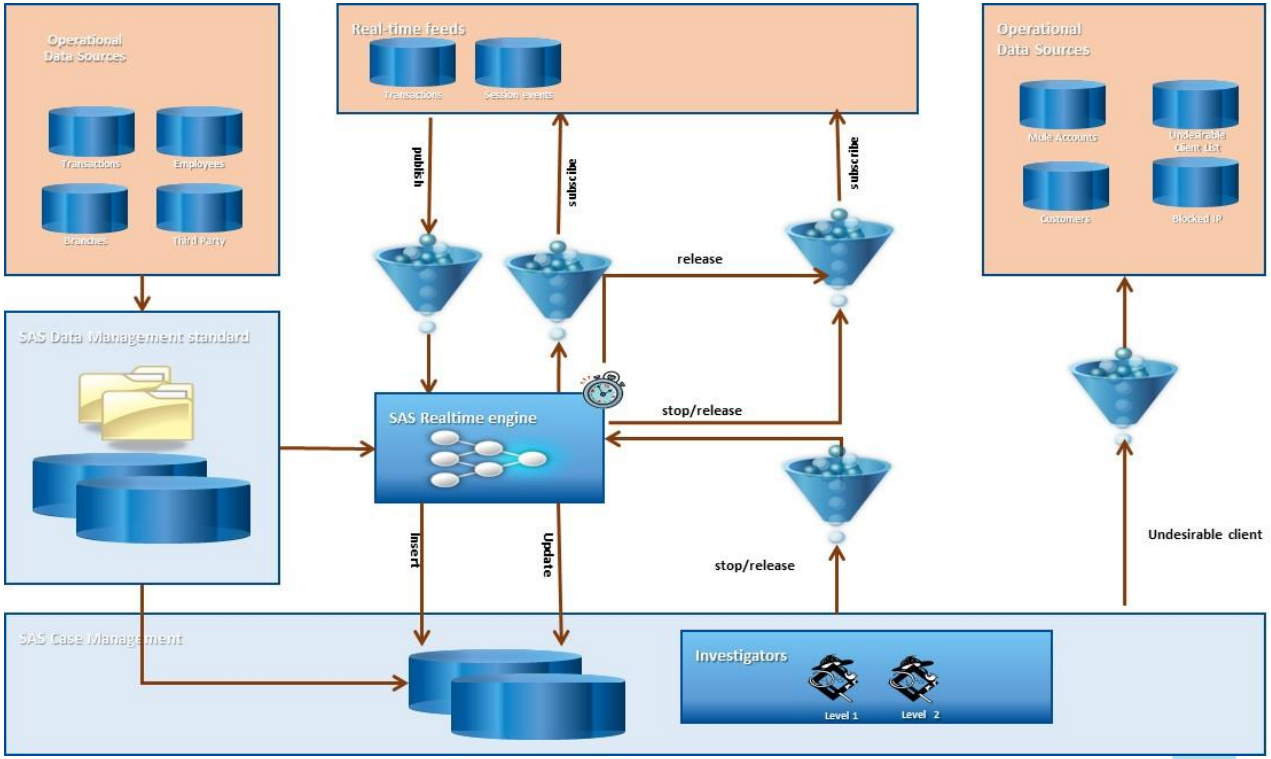
Business rule (example): Transaction above $xx to a new beneficiary

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

Text mining (example): Transaction narrative showing suspicious payments

sas THE POWER TO KNOW.

Real Time Decisioning



CASE STUDY

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

Mules

16:11	6.025 €	1
16:13	3.128 €	2
16:16	3.128 €	3
16:18	3.128 €	4
16:39	3.128 €	5
16:42	2.981 €	6
17:09	**74.561 €**	7
17:11	**68.211 €**	S 1
17:20	2.900€	S 2

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 €
3 ATM	3.940 €
3 POS	68.149 €
1 transfert	250 €

POTENTIAL PHASE I IMPACT

AS-IS	Average 14000 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

MULE SCORECARD ASSESSMENT

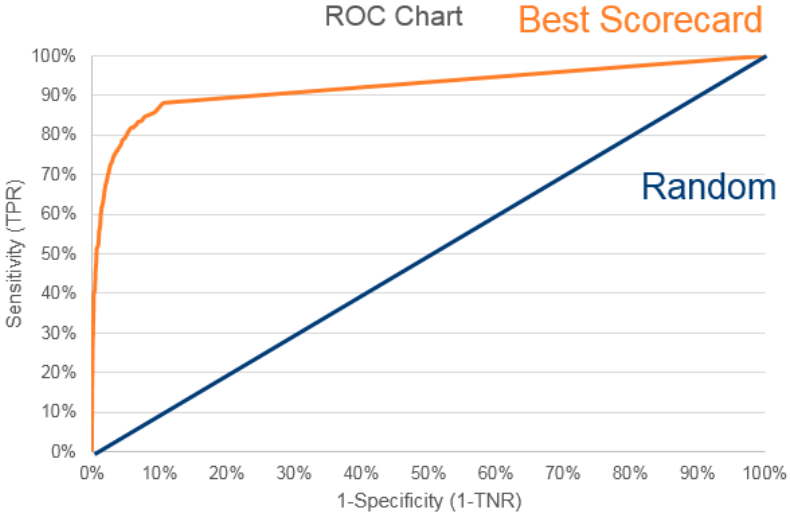
ROC CHART

SAS FORUM RUSSIA 2015

ROC on Validation = 0.9550

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)

SCORECARD PAYMENTS

EXAMPLE TRANSACTION SCORED

SAS FORUM RUSSIA 2015

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

RULES SELECTED FOR PHASE 1

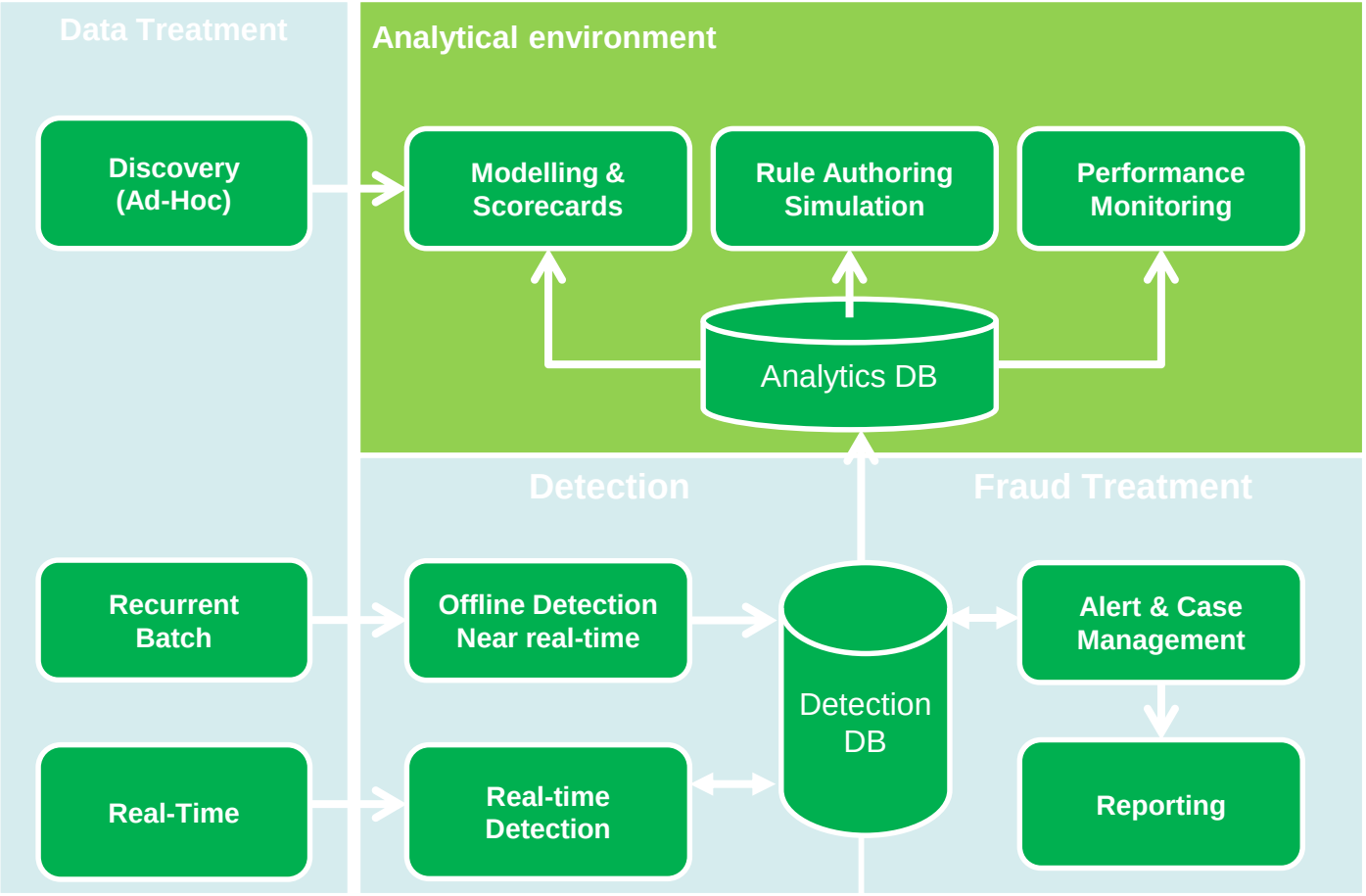
Rules	Value	Scorecard Points
Amount_250_799	0	26
Amount_250_799	1	-84
Amount_799_2105	1	-27
Amount_799_2105	0	17
Amount_3000_4560	1	39
Amount_3000_4560	0	5
Amount_plus4560	1	37
Amount_plus4560	0	0
Prec_MeToMe	1	19
Prec_MeToMe	0	9
BenefVHIGHriskMule	1	44
BenefVHIGHriskMule	0	9
BenefHIGHriskMule	1	106
BenefHIGHriskMule	0	1
BenefMEDriskMule	1	94
BenefMEDriskMule	0	-28
OrigDutch	0	-23
OrigDutch	1	25
CommunicationIsBlank	1	38
CommunicationIsBlank	0	-71

New Rules	Value	Scorecard Points
new_rule_benef_nat	1	55
new_rule_benef_nat	0	16
new_rule_benef_nat	_MISSING_	-49
new_rule_lag_less1min	1	-11
new_rule_lag_less1min	0	15
new_rule_lag_1to15min	1	18
new_rule_lag_1to15min	0	4
new_rule_lag_plus1247min	0	31
new_rule_lag_plus1247min	1	-46
new_rule_oldage_plus63	1	-44
new_rule_oldage_plus63	0	2
new_rule_2till8pm	1	32
new_rule_2till8pm	0	-29
new_rule_weekday	0	-55
new_rule_weekday	1	13

= 26+17+…-71 = 421 points > CUT-OFF ➔ Alert

THE POWER TO KNOW.

FRAUD ARCHITECTURE OVERVIEW



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

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

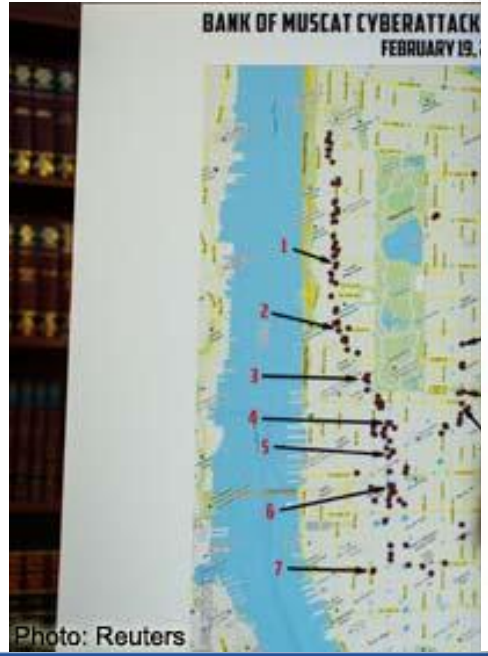


Photo: Reuters

ADVANCED ANALYTICS

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

Fraud Management Operation

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

SAS Fraud Management Solution

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.

Integration

Integration with other fraud/risk solutions (Link Analysis, AML, etc.)

Input

Signatures

Transaction

Geographic data

Neural Network Model

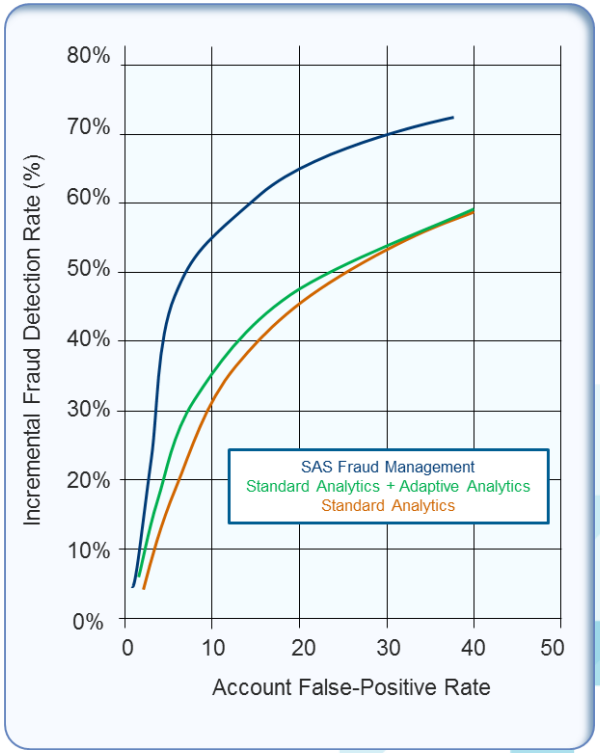
Score with Reason Codes

HSBC Case Study – Enterprise Fraud Detection

SAS FORUM RUSSIA 2015

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



sas THE POWER TO KNOW.

CLIENT EXAMPLE

ONE OF AMERICA'S LARGEST BANKS

SAS FORUM RUSSIA 2015

Challenges

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

Real time credit & fraud decisions

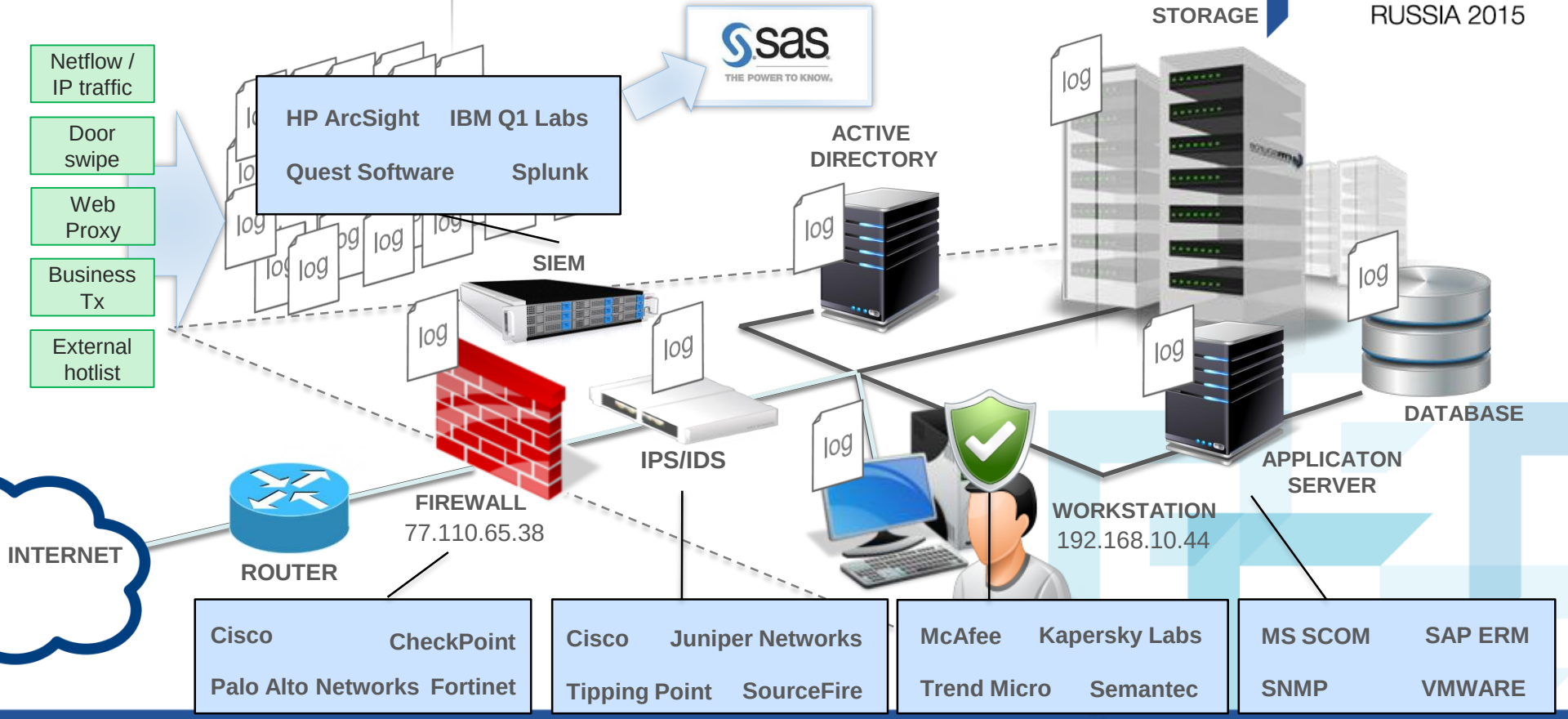
- Replacing home grown system
- ROI: 100 million $ in Y1, of which 60 million $ from new revenue and 40 million $ from fraud loss reduction.
- Operational cost reduction: from 3000 rules to 100 rules and a single model
- Credit and fraud : credit decisioning + fraud decisioning – single data source

CYBER SECURITY

Cyber Security

MANY POTENTIAL DATA SOURCES

SAS FORUM RUSSIA 2015



SAS THE POWER TO KNOW.

SAS solution

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

- 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.

SAS® FORUM
RUSSIA 2015

SAS Forum

sas THE POWER TO KNOW.