2015 TRENDS MOBILE IS HERE TO STAY
Some 30 billion objects may be connected to the Internet of Things¹ by 2020.

- 7 billion–10 billion objects in 2013
- 26 billion–30 billion objects in 2020
- ~15–20% growth annually

¹A networking of physical objects via embedded devices that collect and/or transmit information.

Source: Forecasts derived from ABI Research; expert interviews; Gartner; IDC; McKinsey analysis
Cloud services will account for more than 50% of IT spend in the next few years.
Figure 1. What keeps you up at night?
Three responses permitted

- Not knowing where confidential data is: 57%
- Migration to new mobile platforms: 51%
- Temporary worker or contractor mistakes: 50%
- Third party or outsourcer management of data: 42%
- Migration to cloud ecosystem: 24%
- Hackers: 23%
- Non-compliance with laws or regulations: 21%
- Broken business processes: 16%
- Employee mistakes: 10%
- Malicious employees: 6%
Figure 3. Do you know where your sensitive or confidential data is located?

- Yes, all data: 16% structured, 7% unstructured
- Yes, most data: 22% structured, 10% unstructured
- Yes, some data: 38% structured, 42% unstructured
- No: 24% structured, 41% unstructured

Data is categorized as structured or unstructured.
FRAUD COMPLEXITY

SPAM – MitB – Application fraud

Money Mules

1. Users receive spammed messages with an embedded malicious link. When users click on the link, they are led to the installation of malicious extensions.

2. The malicious extension displays forged boleto on affected systems.

3. The malicious extension steals and sends boleto information (date and value) from affected systems.

4. Malicious extensions (Chrome/FireFox) are downloaded from cloud storage services.

5. Users unknowingly send money to the money mules using the compromised boleto.

6. The cybercriminals collect the stolen money from the money mules.

7. The cybercriminals use open source “boleto” generator software.

8. The generated forged boleto number and bar code are sent back to the extension.

C&C Server

Hosted in bulletproof hosting service.
(R)EVOLUTION EMV ATTACK

Testing & manipulation of banking system vulnerabilities
TOWER GROUP FRAUD LOSS INCREASING ALONG WITH COMPLEXITY

Financial Losses from Fraud Over in 2014
Percentage of Respondents

- 51% Increase
- 27% No Change
- 13% Unsure
- 9% Decrease

Source: iSMG Faces of Fraud Study, 2014.
Abnormal Churn Rates Due to Fraud, By Industry

Percent of Abnormal Customer Churn, 2014

- Pharmaceutical: 6.2%
- Financial: 6.1%
- Healthcare: 5.9%
- Services: 4.2%
- Technology: 4.1%
- Communications: 3.6%
- Industrial: 3.6%
- Transportation: 3.0%
- Consumer: 3.0%
- Hospitality: 2.9%
- Energy: 2.8%
- Education: 2.4%
- Research: 2.3%
- Media: 2.1%
- Retail: 1.3%
- Public: 0.3%

Source: iSMG Faces of Fraud SI
HOW DO I BALANCE BUSINESS EXPANSION AND THE INHERENT VULNERABILITIES?

q. With increasing data & vulnerabilities, how do I know that YOU are my customer?
   A. Behavioral Analytics

   q. I need to stop fraudulent payments sooner. How do I get faster decisions?
      A. Real-time Decisioning (Pre-payment)

q. How do I keep up with the changing trends? How do I get analytic results faster?
   A. In-memory Analytics

   q. How do I more effectively manage and store the data in a cost effective manner?
      A. Streaming & Hadoop

q. How do I prepare for the unknowns that are in the horizon? How do I respond quickly to intra-day events?
   A. Data Visualization & Forensic Discovery
In Hours, Thieves Took $45 Million in A.T.M. Scheme

It was a brazen bank heist, but a 21st-century version in which the criminals never wore ski masks, threatened a teller or set foot in a vault.

In two precision operations that involved people in more than two dozen countries acting in close coordination and with surgical precision, thieves stole $45 million from thousands of A.T.M.‘s in a matter of hours.

In New York City alone, the thieves responsible for A.T.M. withdrawals struck 2,904 machines over 10 hours starting on Feb. 19, withdrawing $2.4 million.

Bank fines for AML violations scale with the severity of the violation

Fines levied for a range of reasons from internal "payment stripping" to knowingly making payments to sanctioned countries.

Source: www.bankersacqcity.com/AML/fines
THE NEW ENTERPRISE

COVERING THE FULL SPECTRUM

defined analytics  behavioral monitoring  dynamic in-memory  ad-hoc / unstructured data  Unknown Patterns

Detection Operations  Ideation / Validation  Proactive Forensics
Case Management & Reporting

Analytics
- Detection Operations
  - Continuous Monitoring
- Peer-Based & Predictive Analytics
- Networks & Linking
- Validation / Optimization
  - Model Tuning & Optimization
  - Visualization
  - Simulation
- Proactive Forensics
  - Analytics & Data Discovery
  - Global Search & Visual Investigation
  - Ad Hoc Network Analysis

Data Mgt.
- ETL / Data Quality
- Data Federation
- Entity Resolution

Keywords:
- defined analytics
- behavioral monitoring
- dynamic in-memory
- ad-hoc / unstructured data
- Unknown Patterns
DETECTION OPERATIONS  CARD FRAUD TIER I BANK

CHALLENGES

• Modernize analytic approach for one of largest US credit card portfolios
• Steady increase in Customer Dissatisfaction from Credit Card usage being declined inappropriately
• Increased fraud losses
• Increasingly difficult to maintain the prior fraud platform with 3,000+ rules

SOLUTION

• SAS® Enterprise Fraud Management™ solution
• Real-time SONNA decisioning (100% of transactions)
• Behavioral profiling (multi-entity “Signatures” & Dynamic Summarization)
• Consortium-aware custom models

BUSINESS IMPACT

$60M / year increase in bottom line from increased revenue

$40M / year bottom line savings from fraud loss prevention

Reduction from 3,000 rules to 1 model + 75 rules
DETECTION OPERATIONS

AUTO CLAIMS FRAUD DETECTION

CHALLENGES
- No-fault fraud exposure difficult to detect
- Bakeoff POC for suspicious claim detection in KY & MI auto claims
- Major data quality & entity resolution issues
- Incorporate 3rd party data from NICB, ISO

SOLUTION
SaaS: SAS® Fraud Framework for Insurance
- Time to value less than 3 months
- 16% of accepted alerts also flagged for medical management issues, demonstrating value beyond just “fraud”

BUSINESS IMPACT
- 74% alert acceptance rate
- 162% increase in suspicious providers
- $2.2m previously unidentified questionable medical provider exposure

SAS Fraud Framework “exceeded our expectations and showed SAS understanding of no fault fraud issues and SIU needs.”

- Grange SIU Manager

Copyright © 2015, SAS Institute Inc. All rights reserved.
VALIDATION / OPTIMIZATION

FINANCIAL CRIMES ANALYTICS

CHALLENGES

• Consolidate reputation exposure: AML, Fraud
• Heightened regulatory pressures
• Need to scale their transaction monitoring processes
• Desire to improve model risk tuning & optimization
• Current vendor used “black box” analytics
• Apply network analytics against historical investigations to quantify organized ring exposure

SOLUTION

• High Performance AML
• Hadoop & Teradata data management strategy
• Visualization (Visual Analytics & Visual Scenario Designer™)

PROFILE

GLOBAL TIER 1 BANK

PEER BANKS UNDER Cease & Desist Orders

COMBINED FIU
FORENSIC DISCOVERY

VISUAL INVESTIGATOR

SAS® Visual Investigator

SAS Enterprise Case Management • Search

Your search matched 126 results

Case ID: 2014-14239
Wed, Sep 24, 2014 04:27:59 PM | Case status: Investigate | Primary owner: Marian
comments: mb mb notes mb

2014-12401 - Theodora Haley
Mon, Sep 1, 2014 02:47:01 PM | Type: Generic | National ID: 540-37-0173
comments: phone calls testing notes

Case ID: 2014-12401
comments: phone calls testing notes

Case ID: 2014-14171
Tue, Sep 30, 2014 02:04:28 PM | Case status: New | Primary owner: Marian
comments: blah blah I love this nifty notes area

2014-14171 - Lindsey Kozey
Mon, Sep 1, 2014 02:47:01 PM | Type: Generic | National ID: 110-29-3898
comments: blah blah I love this nifty notes area

notes_for_search_using_ssl.txt
Mon, Jul 7, 2014 03:39:34 AM | Extension: txt | Size: 6793
To properly secure the server you should also comment out the unsecure connector running on port 8983

notes_for_search_using_ssl.txt
Thu, Jul 3, 2014 07:35:34 AM | Extension: txt | Size: 6793
To properly secure the server you should also comment out the unsecure connector running on port 8983

Enterprise Case Management 6.2 Admin Guide.pdf
For information about support fixes, see the SAS Notes that are available on the SAS Technical Support - Support website. Search for available SAS Notes for SAS Enterprise Case Management at http://support.sas.com/Delete Any Case Comment Enables users to delete any case comment. Delete My Case Comment Enables users ... Incident Comment Enables users to delete any incident comment. Delete My Incident Comment Enables users...
Employ innovative use of technology, domain expertise and analytics to create business solutions that reduce losses from fraud & improper payments, modernize compliance, and identify threats to public safety & national security.

Fraud & Security Intelligence

Enterprise Extendibility

Analytic Driven Detection

Real-time Authoring & Simulation

Visualization & Forensic Discovery
QUESTIONS?