

SmarterBanking



Financial Crimes



Financial Crimes Challenges

Volume & velocity of money flows are increasing and existing systems are struggling to keep up.

Cost of combating financial crime is rising driving bankers to seek synergies between fraud prevention, anti-money laundering, sanctions and IT security.



IT Security

- Criminals have sophisticated tools, malware & cyber warfare outpacing institutions security measures.
- The attack surface is growing (byod, mobile, outsourcing)



Enterprise Fraud

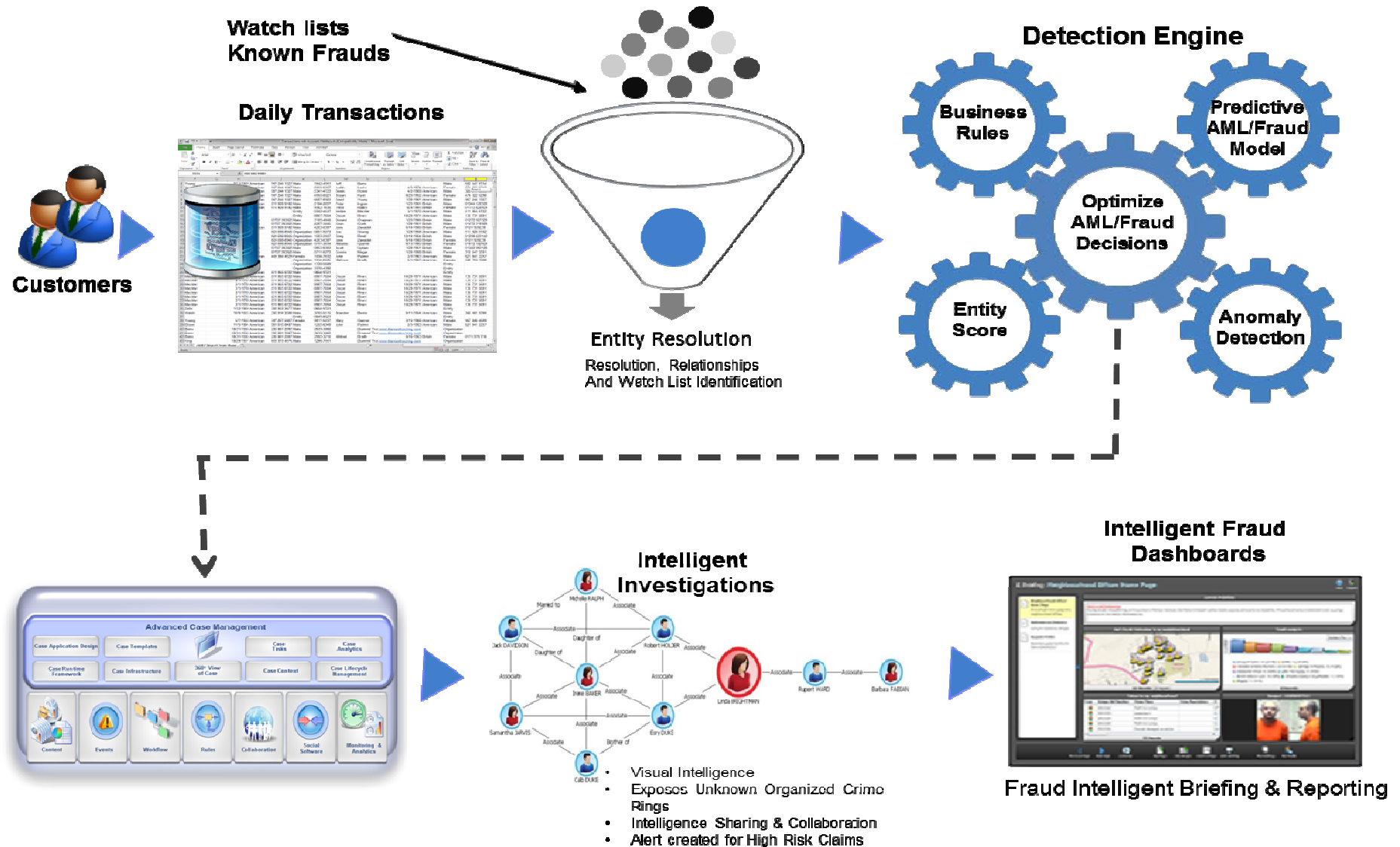
- Fraudsters are well funded. Networks are extensive including insiders and mules.
- Fraud schemes spreading across organizations and the ability to make intelligent, quick decisions have been elusive.



Anti Money Laundering & Sanctions Work

- Operational Costs are increasing.
- False positives are too high.

Financial Crimes High Level Process



What is Our Solution?

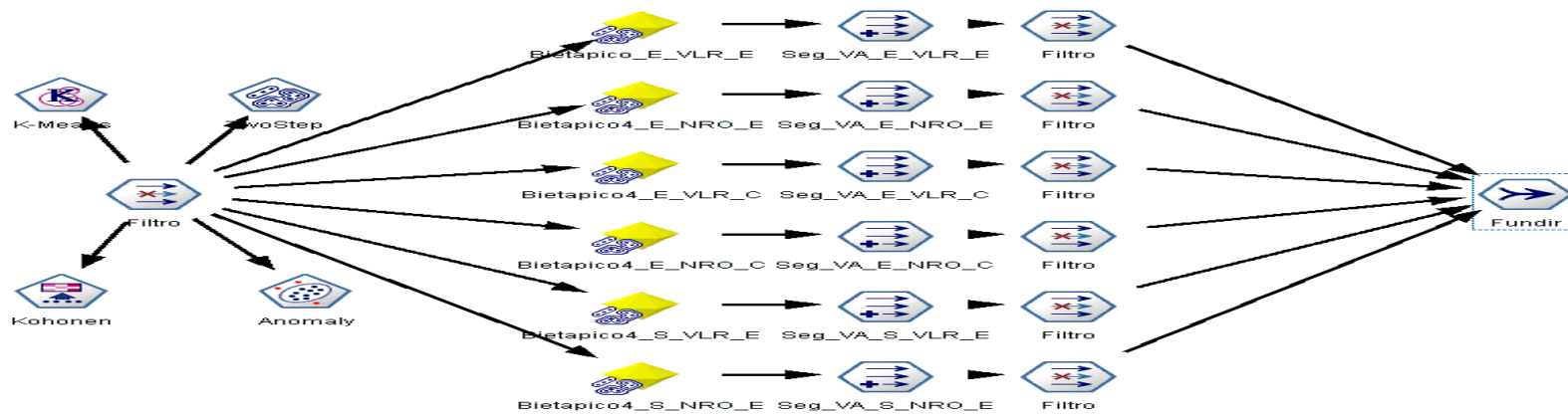
A Fraud Prevention & Anti-Money Laundering Solution

Comprehensive solution which has intelligence based fraud detection with minimal false-positive rates offering much lower operational costs while improving customer satisfaction. It incorporates business capabilities for **Online Fraud, Employee Fraud, Transaction Monitoring and Suspicious Behavior Detection , List Screening and Know Your Customer Scoring** including the following technical capabilities:

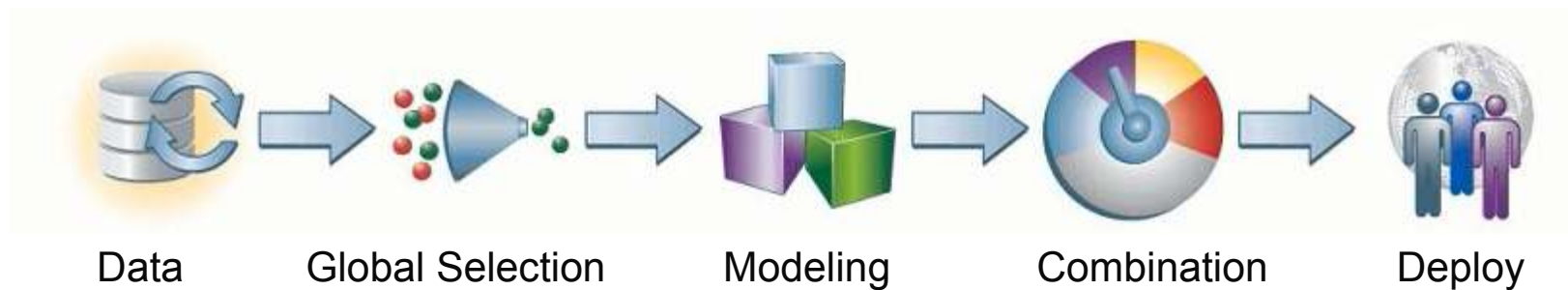
- Analytic Development, Training, Learning and Modeling Environment
- Real-Time Scoring, Detection and Prevention of Fraudulent and Suspicious Activity System
- Big Data & Content Analytics
- One Billion+ Name Database and Analytics
- Intelligent Investigation - Deep Visualization, Investigation & Forensics Readiness

IBM SPSS

Selecting the appropriate model and training



And deployment of models into production



South American Bank - Transaction Monitoring

Challenge

Although current AML solutions did adapt over time to changes they were not responsive enough as the “launderers” are always looking for new alternatives causing existing approaches to quickly atrophy.

Objectives

To replace traditional warning systems based on parameters and rules with data mining modeling techniques through transactional behavior analysis as a key risk factor to detect unusual or suspicious transactions so they could act accordingly.

Results

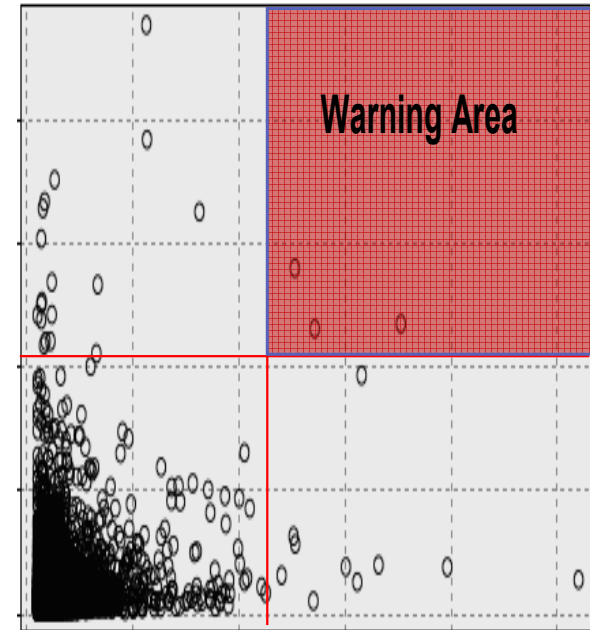
They were able to improve efficiency by 60% generating dramatic ROI savings and slashing the administrative costs for AML. Focus was on reducing the number of suspicious operations that required auditing by more than 90%. Increased the accuracy in identifying positive cases of money laundering for generating SARs (suspicious activity reports): reported cases from 25% to 60%.

Key Take Aways

They performed the reverse analytics of modeling customers known historical usage patterns to score against current usage generating key indicators and triggering customer anomalies.

They redefining customer segmentation based on usage patterns around dollar amounts, volume of transactions and type of transactions using advance algorithms, scatter plots, clusters, exploratory, seasonal analysis and demographics

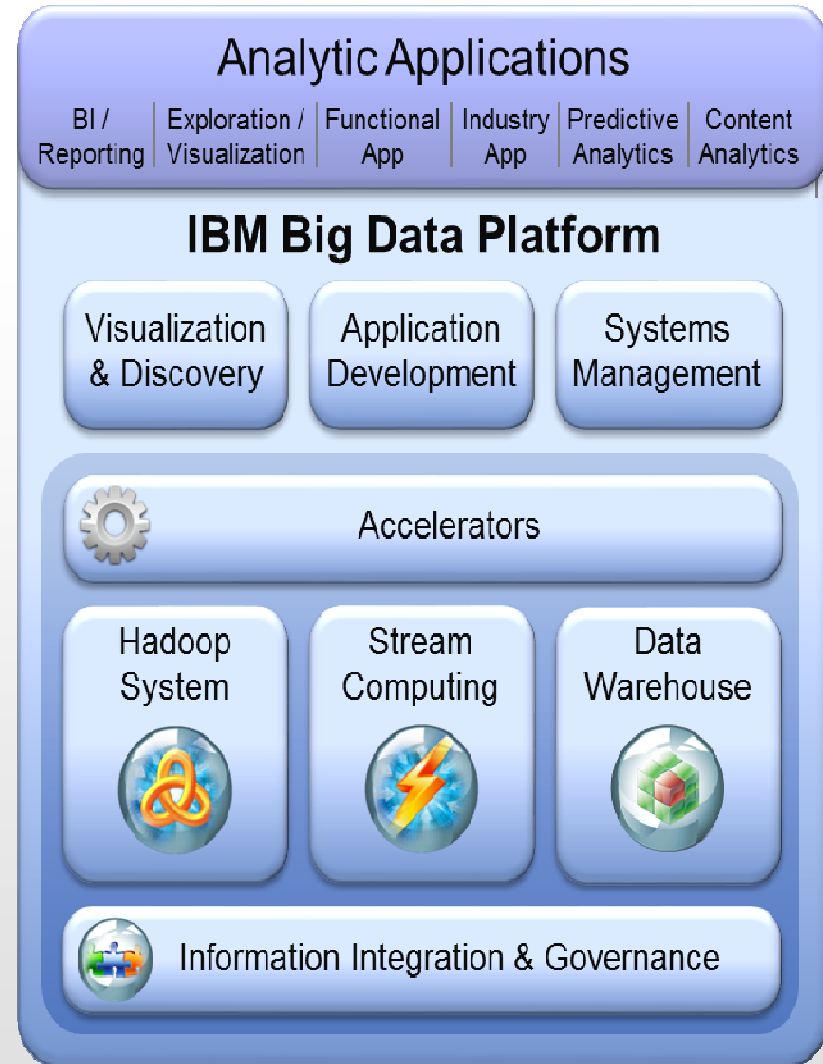
Allows Organizations to have a business discussion regarding what action to take (NOT JUST FOR RISK & FINANCIAL CRIMES, BUT ALSO FOR REVENUE AND PROFIT ACTIVITIES)



Big Data = Variety, Velocity and Volume with Veracity



- Big Data doesn't operate in a silo.
- Builds on traditional BI, providing the ability to aggregate and analyze much more data.
- Cost effectively – based on open source.
- IBM builds on open source with enterprise-grade capabilities, integration and security.
- Accelerators: extensive text analytics and machine learning IP on both data-in-motion and data-at-rest. Annotated Query Language.
- IBM is investing in this space:
 - Largest commercial research organization (19 years of patent leadership)
 - \$14+ B investment in acquisitions in 5 yrs.



Content Analytics as a critical enabler

(c) 2001, Chicago Tribune.
 Visit the Chicago Tribune on the Internet
 at <http://www.chicago.tribune.com/>
 Distributed by Knight Ridder/Tribune
 Information Services.
 By Stephen J. Hedges and Cam Simpson

.....
 The Finsbury Park Mosque is the center of
 radical Muslim activism in England. Through
 its doors have passed at least three of the men
 now held on suspicion of terrorist activity in
 France, England and Belgium, as well as one
 Algerian man in prison in the United States.
 "The mosque's chief cleric, Abu Hamza al-
 Masri lost two hands fighting the Soviet Union
 in Afghanistan and he advocates the
 elimination of Western influence from Muslim
 countries. He was arrested in London in 1999
 for his alleged involvement in a Yemen bomb
 plot, but was set free after Yemen failed to
 produce enough evidence to have him
 extradited. ."

Fact

Event

<Organization>Finsbury Park Mosque</Organization>
<Country>England</Country>
<Country>France</Country>
<Country>England</Country>
<Country>Belgium</Country>
<Country>United States</Country>
<Person>Abu Hamza al-Masri</Person>
<PersonPositionOrganization> <OFFLEN OFFSET="3576" LENGTH="45" /> <Person>Abu Hamza al-Masri</Person> <Position>chief cleric</Position> <Organization>Finsbury Park Mosque</Organization> </PersonPositionOrganization>
<City>London</City>
<PersonArrest> <OFFLEN OFFSET="3771" LENGTH="61" /> <Person>Abu Hamza al-Masri</Person> <Location>London</Location> <Date>1999</Date> <Reason>his alleged involvement in a Yemen bomb plot</Reason> </PersonArrest>

IBM InfoSphere Global Name Recognition

Leading worldwide multi-cultural name analytic technology

- ❑ 1B Name Facts in the Repository
- ❑ 200 Cultures Linguistically Studied
- ❑ Detailed Engine Parameter tuning
- ❑ Culturally Aware rules engine with a statistical name knowledge base
- ❑ Only name analytic product on DHS SafetyAct list

- Names remain the single most important means for identifying people
- People everywhere in the world are learning how easy it is to circumvent our name search systems



Customer -- Responding to New Challenges

A Major Canadian Financial Institution

BUSINESS DRIVERS

- *Compliance - Dramatically lower costs from false positives and false negatives*
- *Adhere to Canadian Government mandated PEP list screening requirements*
- *Avoid hiring and training dozens of new fraud analysts required to keep pace*

Solution Value Proposition:

- IBM Global Name Recognition software and GBS Services to:
 - Increase accuracy in real-time watch lists checking
 - Decrease false positives and false negatives in real-time PEP list checking
 - Avoid need to hire and train additional fraud analysts as watch list volumes grow

Solution Results:

- Reduced false positives and false negatives from 75% - 95% before Global Name Recognition to almost 0%
- Avoided need to recruit, hire and train up to 24 new fraud analysts
- Dramatically improved speed and accuracy of watch list checking
- Improve regulatory compliance in AML and Anti-Terrorist Funding

Who is who? no matter how hard they try to hide!

ID 1987839



Kate Mills
4737 Cimarron Dr.
Bolton, MA 01512
Phone: (978)365-6631
DOB: 12/13/71



ID 1786616

Katie Green
P.O. Box 12743
Clinton, MA 01510
Phone: (978)365-6631
Kinear

ID 8987009



Kate Mills-Green
1 Bourne St.
Bolton, MA 01512
Phone: (501)661-8044
Silverback
DOB: 12/12/71



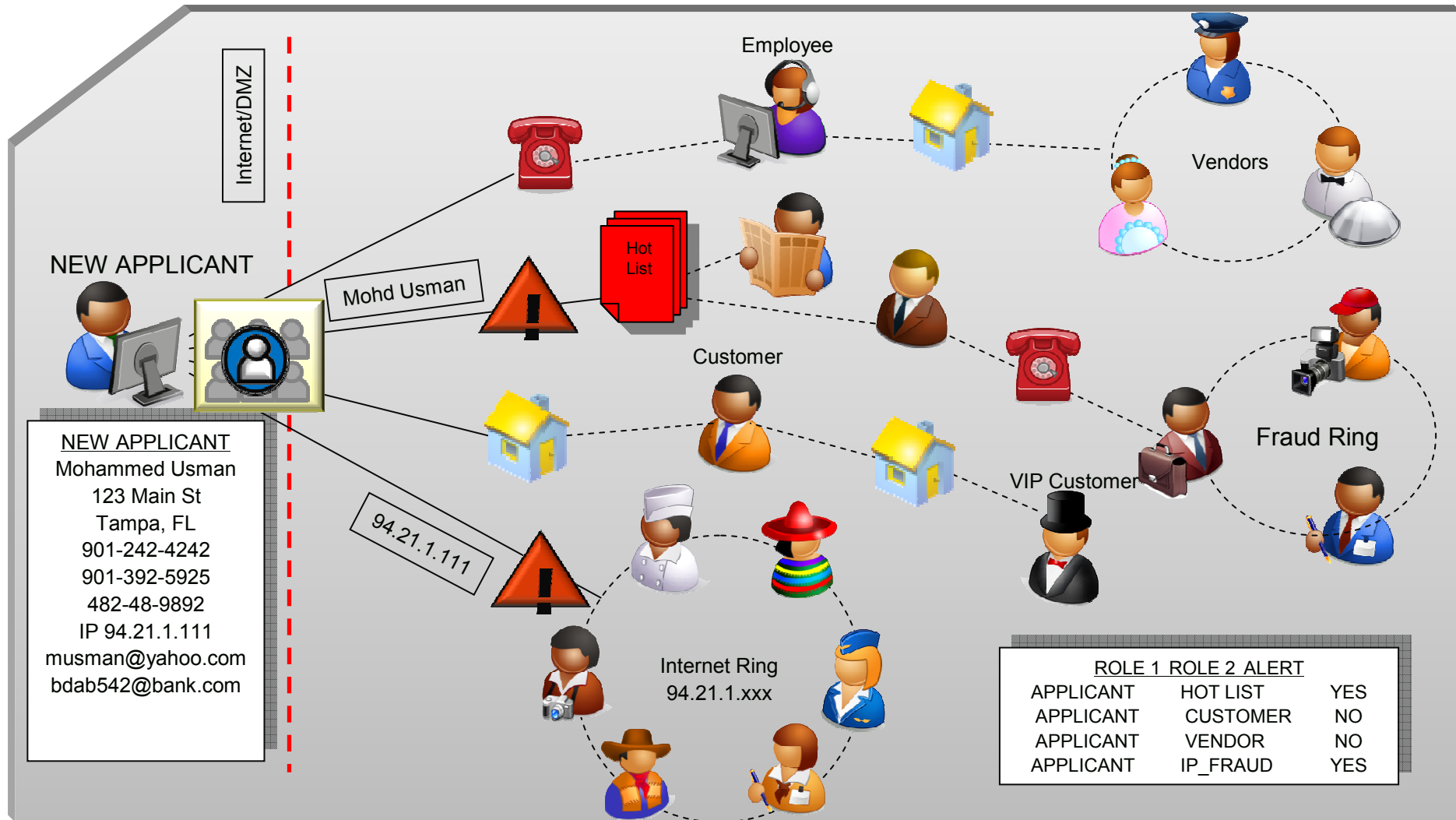
ID 3335673

Katherine D. Green
4737 Cimarron Dr.
Easton, MA 02334
Phone:(508)278-6019
Zycast Int.
DOB: 11/13/71

Entity #14465

ADDRESSES	NAMES	ADDITIONAL
4737 Cimarron Dr. Easton, MA 02334	Katherine D. Green	DOB: 12/13/71
1 Bourne St. Bolton, MA 01512	Kate Mills-Green	Phone:(508)278-6019
P.O. Box 12743 Clinton, MA 01510	Katie Green	(978)365-6631
	Kate Mills	(501)661-8044
	Kate Green	Work: Zycast Int.
	Kate M. Green	Silverback

And Link Analysis | “Who Knows Who?”



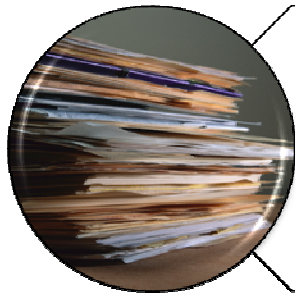
Alerts Tell You When Something is Wrong



Role Alert: When entities are resolved or related

Examples

- Employee is a vendor
- Employee shares address with vendor
- POI shares last name and phone number with police officer
- Employee shares bank account with employee
- Person has more than one name



Attribute Alert: When an entity with specific set of attributes is found

Examples

- If a name is ever encountered
- When an address of a suspect is ever encountered
- When any collection of one or more attributes is found



Event Alert: When an transactions and identities match alert rules

Examples

- Five money transfers in 24 hours over \$10,000 by one person
- More than one account opened in 2 days by same person
- 10 or more code violations reported in 5 days by same inspector

Identity Insight Case Study

Enhancing Compliance and Fighting Consumer Fraud



Challenge

With 230,000 locations in 196 countries MoneyGram International faced pressure to keep up with fraud and compliance regulations affecting the international business landscape.

Solution

- IBM® InfoSphere® Identity Insight solutions
- IBM InfoSphere Information Server
- IBM InfoSphere DataStage®
- IBM Business Partner: Alpine Consulting, Inc.

Result

- Stopped more than US\$125 million in fraud to date
- Increased ability to identify and interrupt potentially fraudulent transactions by 40%
- Prevented thousands of customers from losing funds to fraud
- Realized a 72% reduction in consumer fraud complaints in one year

Business Benefits

Understanding who its clients are is helping MoneyGram International identify and stop fraudulent, unauthorized money transfers, thereby addressing a common problem for financial institutions worldwide. Using a powerful, algorithms-based software platform, MoneyGram International has new insight into “who’s who?” “who knows whom?” and “who does what?” as it analyzes transactions to identify known and unknown people attempting to move money. With the solution, MoneyGram International can quickly identify questionable patterns, proactively enact processing rules, and quickly become compliant with new regulations, preventing thousands of customers from losing funds to fraud.

“We are able to detect and respond to fraud far faster than before to protect our consumers as well as our global network of agents. We must remain ever vigilant in the face of more sophisticated financial fraudsters.”

*—Ted Bridenstine, Systems Development Manager,
MoneyGram International*

“Deep Forensics” | Enterprise Forensic Readiness

Financial Services organizations have many different Financial Crime systems which contain a wealth of data yet many operate in individual silos or geographies.

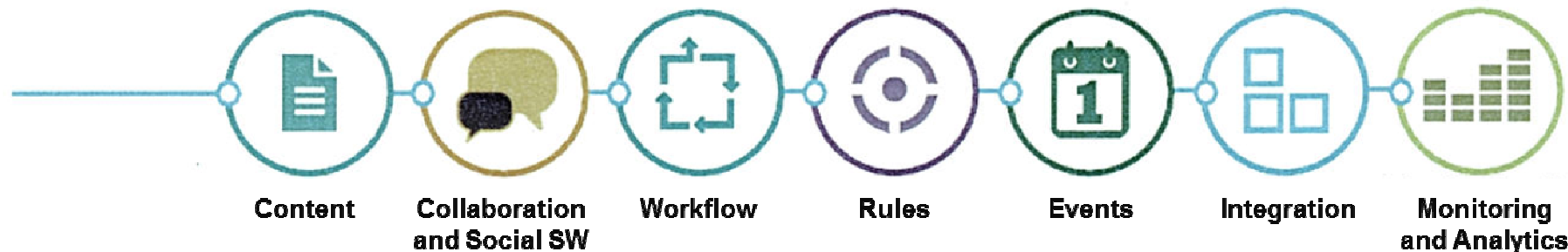
Bankers are struggling to answer the fundamental financial crimes questions:

- Are any of my customers involved in cross border payments with sanctioned parties?
- How is my staff doing in investigating AML alerts, are there any I should worry about? Can I help them by prioritising or reducing the number of alerts?
- Is there data within my organization or available to my organization which would allow the fraud team resolve cases quicker?
- What enterprise or group level capabilities exist for financial crimes?

Track investigations with IBM's Advance Case Management



- Central view of alert cases from across systems and business units.
- Handles many different types of cases, and alerts, by using flexible and extensible data model.
- Proactive pushing of cases to relevant business units when risk is detected.
- Provides coordination and management of overall case evaluation processes.
- Supports expert case users with flexible process structures and user interfaces.
- Supports data privacy and retention policies.
- Provides more efficiency and transparency, better management information.
- Support compliance with audit and case history.
- Build up a body of case history which can be used for further analytics and improve detection models.

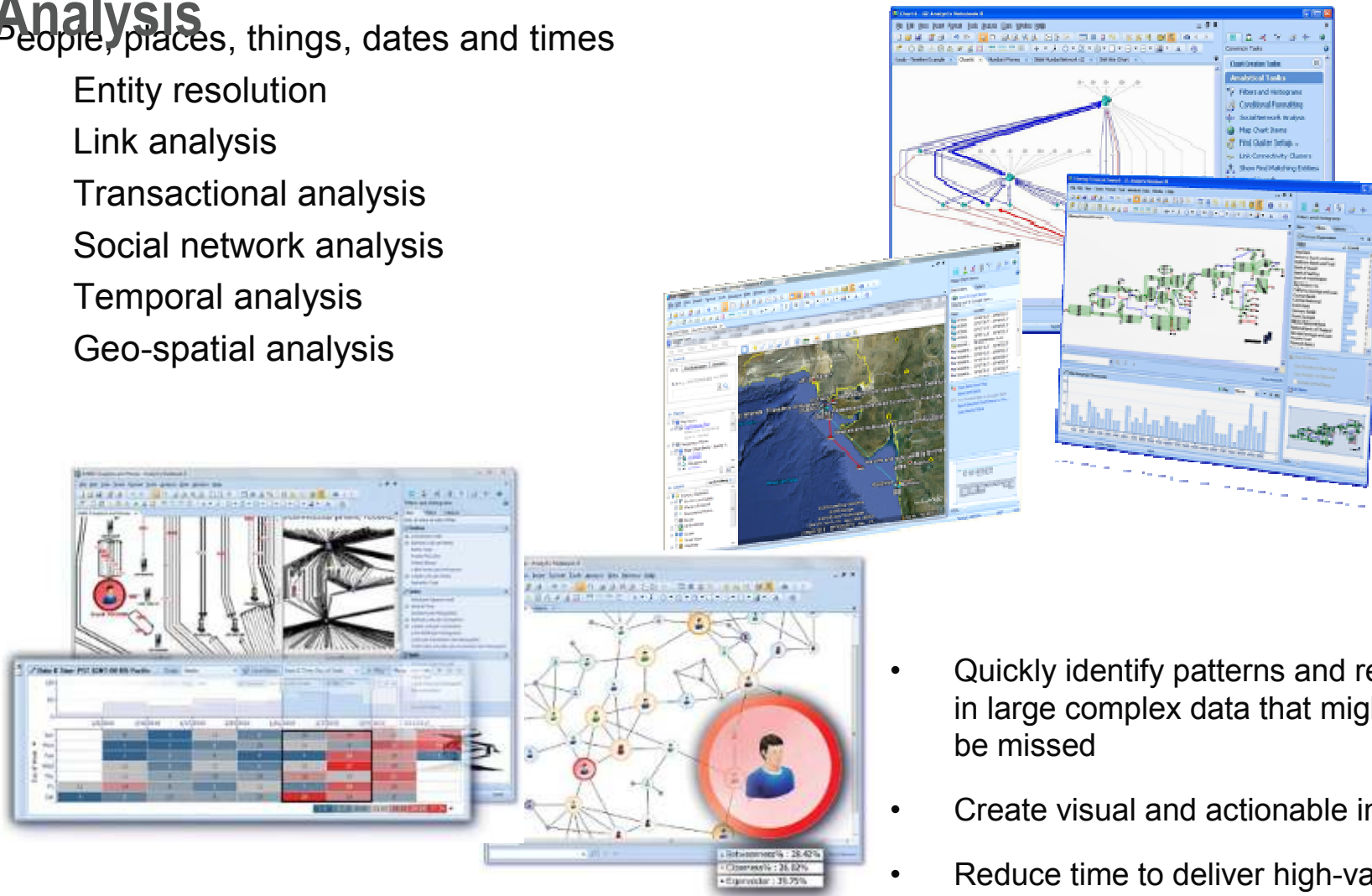


Forensic Investigation with IBM i2 Fraud Intelligence

Analysis

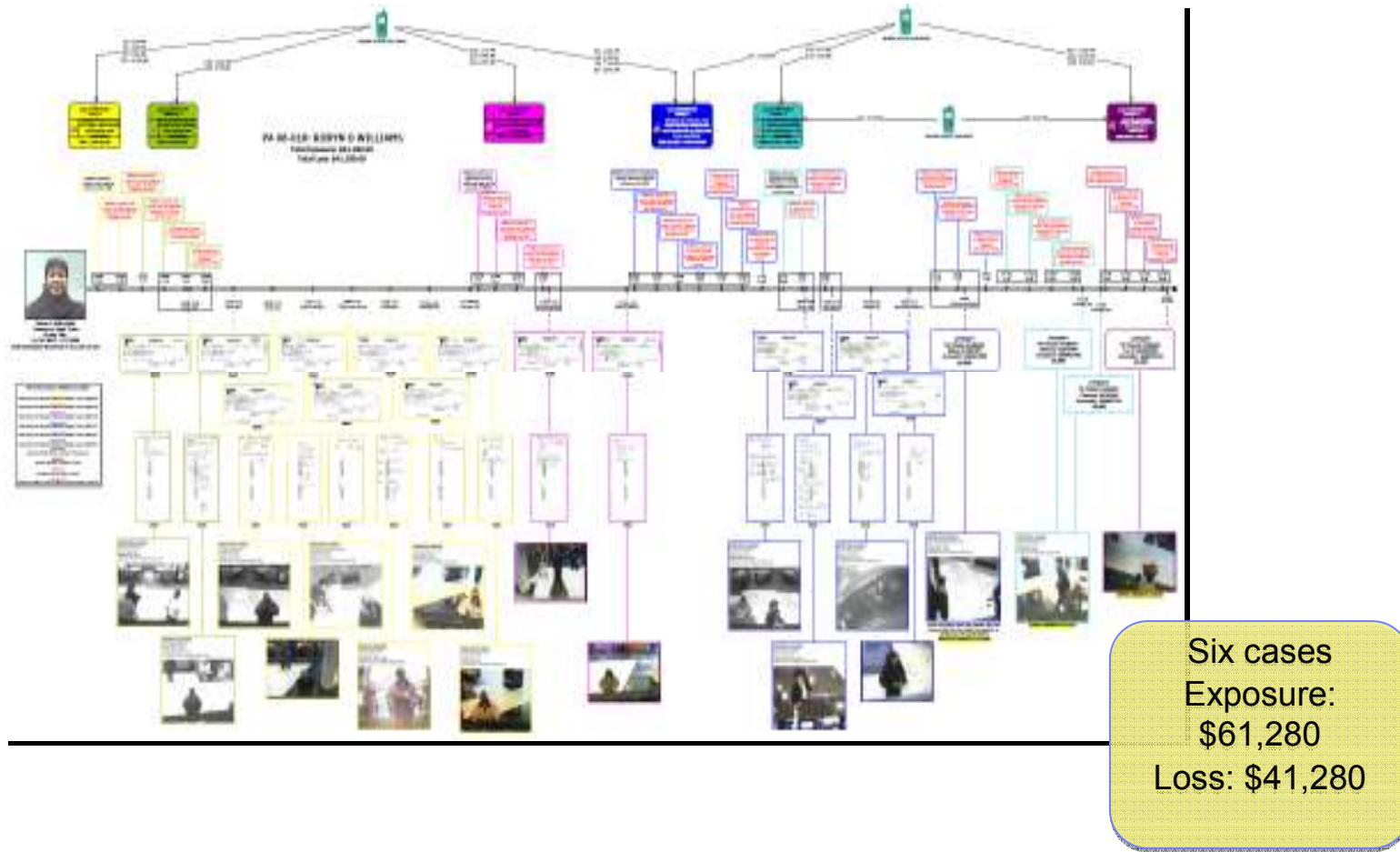
People, places, things, dates and times

- Entity resolution
- Link analysis
- Transactional analysis
- Social network analysis
- Temporal analysis
- Geo-spatial analysis



- Quickly identify patterns and relationships in large complex data that might otherwise be missed
- Create visual and actionable intelligence
- Reduce time to deliver high-value intelligence

Case Study: Insider Threat *Canadian Financial Institution*



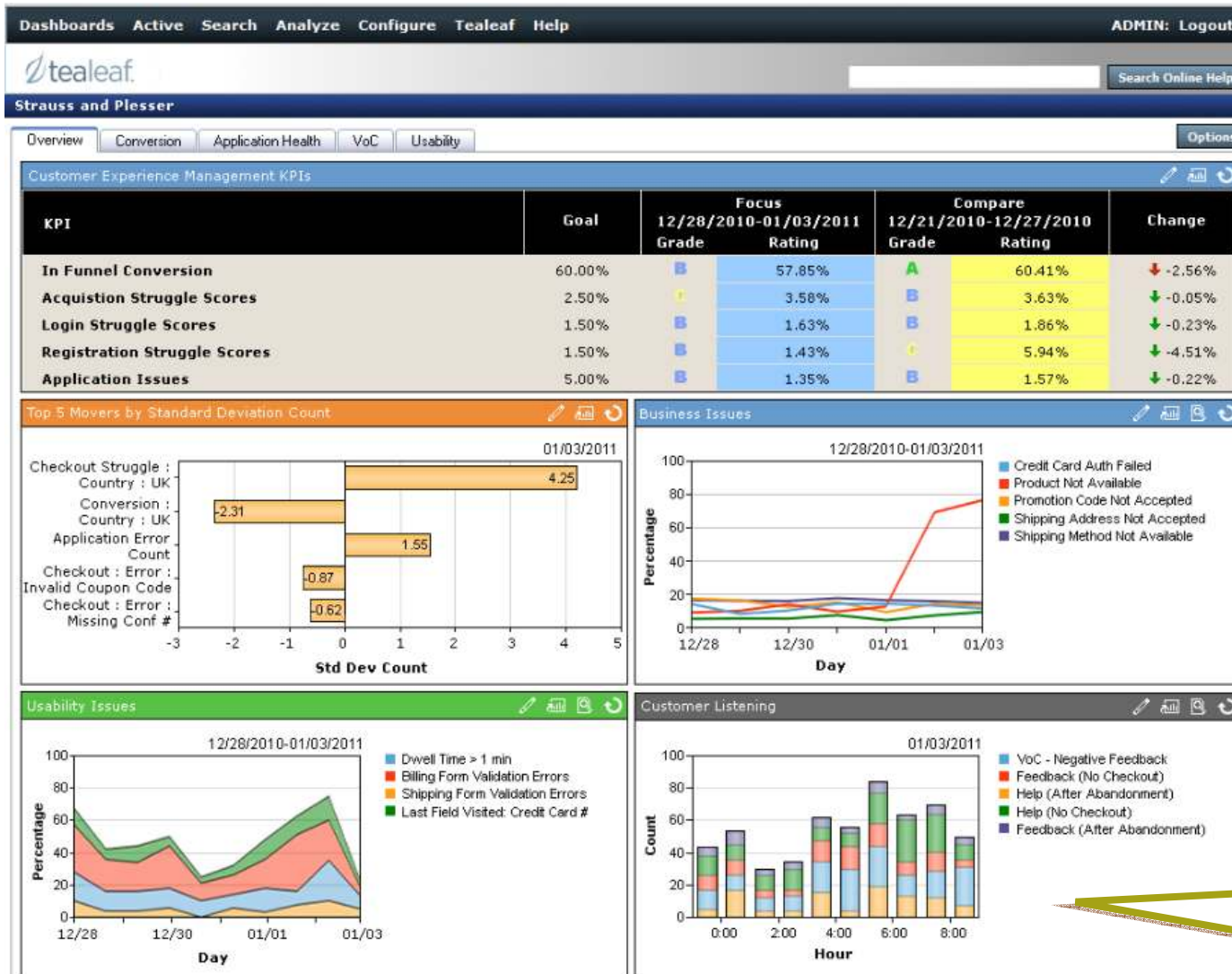
Tealeaf for Fraud Forensics



Tealeaf captures the complete data set (browser views along with HTTP/S request and HTTP/S response data), Banks have seen that Tealeaf also becomes a powerful ally in efforts to fight fraud , specifically:

- Tealeaf's products are designed [to acquire data passively](#) (i.e., out of band through a network tap or span port). This allows for detection -- becoming aware of fraudulent activity -- either in real time or post mortem
- Tealeaf can be used to block access to the website, or prevent the money from leaving the Bank via transfer (time-delayed)
- Research/Investigation -- With the complete stream of traffic capture and built in analytics, we can facilitate forensic discovery pivoting off any session or variable commonality
- Report Impact -- Understanding of the breach by depth, loss data viewed
- Action -- notification of parties affected as well as remediation process

Tealeaf Screen Shots



Mobile replay showing in screen gestures such as swipe, scroll and zoom

The Tealeaf Dashboard identifies sources of struggle

Case Study: Tealeaf for Fraud Forensics

USA Bank

- **Collecting information with Tealeaf to rigorously screen applications for identify theft-related fraud.**
- **Hundreds of development hours were saved by using Tealeaf to collect data rather than pulling it from our back-end systems.**
- **Tealeaf helps us identify sessions containing suspicious behavior that, without Tealeaf, we would be unable to detect through any other means.**

IBM Financial Crimes Platform Solution **Capabilities**

- **Analytics Training & Learning System**
- **Deployment/Runtime & Rules Engine**
- **Big Data & Content Analytics**
- **One Billion+ Name Database, Entity Resolution & Link Analysis**
- **Intelligent Investigation - Deep Visualization, Investigation & Forensics Readiness**

Thank You