IBM Performance 2012

Smarter Analytics. Smarter Outcomes.

Banking Fraud

Learn how IBM Smarter Analytics helps banks to detect and prevent payment fraud across the customer interaction channels using sophisticated real-time Analytics technology.

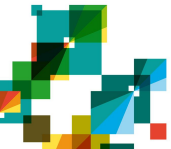
Marco Gomes

Industry Solution Architect, IBM Business Analytics

13 November 2012

Agenda

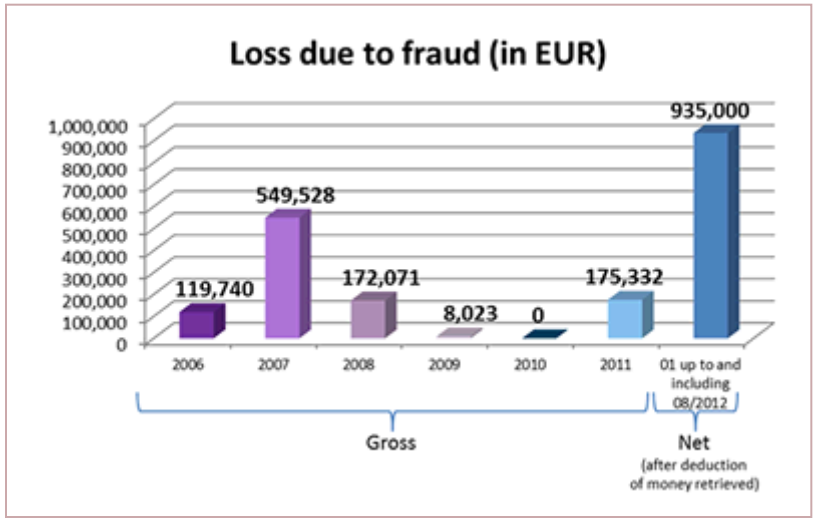
1. Significance of fighting banking fraud
2. Analytics drives value
3. Conclusions



Trends illustrate that banking fraud is rapidly increasing, and even worse getting more complex

Belgium

- Febelfin: "… no spectacular rise in the number of Internet banking fraud cases. Internet banking is one of the safest ways of banking."
- Belgium[1]: Internet banking gross fraud 2,4M€ in 1st half 2012



Market

- Netherlands[2] : 14% rise internet banking fraud in H1 2012 to 27m€
- UK[3]: 28% rise internet banking fraud in H1 2012 to 22m£
- Worldwide, cybercrime becomes more sophisticated and diverse[4]


White Paper

McAfee An Intel Company | Guardian Analytics

Dissecting Operation High Roller

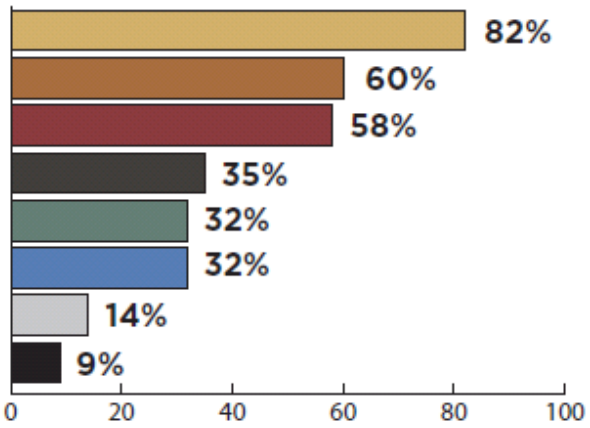
Dave Marcus, Director of Advanced Research and Threat Intelligence, McAfee
Ryan Sherstobitoff, Threat Researcher, Guardian Analytics

How the high-tech mantra of "automation and innovation" helps a multi-tiered global fraud ring target high net worth businesses and individuals. Building on established Zeus and SpyEye tactics, this ring adds many breakthroughs: bypasses for physical "chip and pin" authentication, automated mule account databases, server-based fraudulent transactions, and attempted transfers to mule business accounts as high as €100,000 ($130,000 USD). Where Europe has been the primary target for this and other financial fraud rings in the past, our research found the thefts spreading outside Europe, including the United States and Colombia.

Source:
1) *Febelfin*
2) *Nederlandse Vereniging van Banken*
3) *Financial Fraud Action UK*
4) *McAfee*

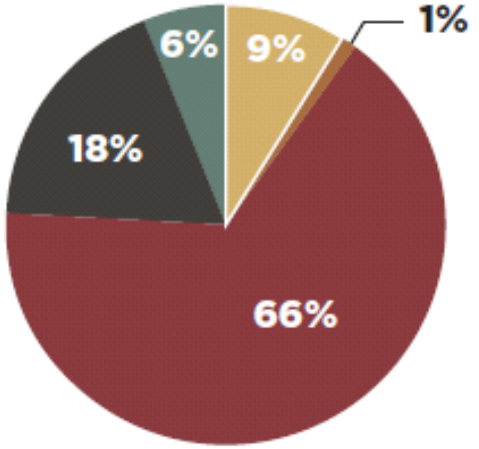
While banks digitized, fraud detection became recursively difficult[1]

How is a fraud incident involving your organization typically detected?



- 82% - When a customer notifies us
- 60% - Through automated data analysis or transaction monitoring software
- 58% - At the point of transaction
- 35% - Third-party notification
- 32% - At the point of origination
- 32% - During account audit/reconciliation
- 14% - Internal whistleblower
- 9% - Third-party investigation

In your opinion, how effective are current anti-fraud security controls?

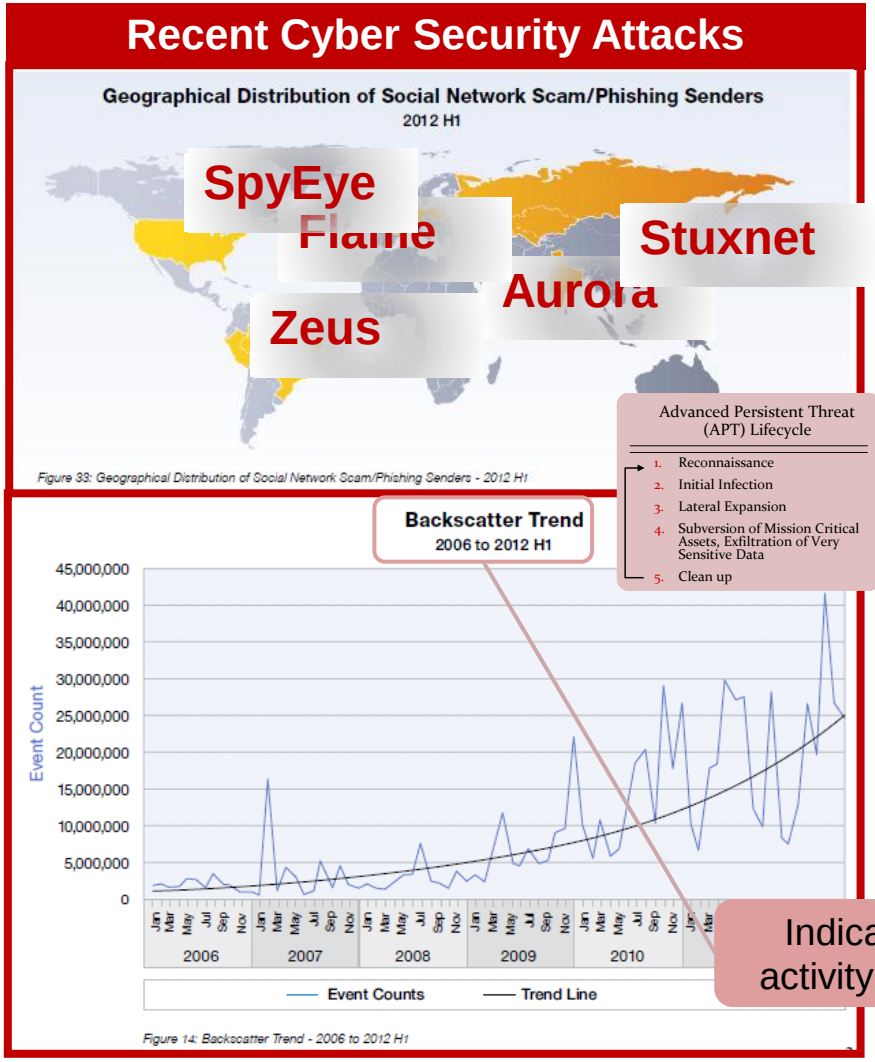


- 9% - Very effective: Consistently detect cross-channel patterns; keep pace with fraud trends
- 1% - Effective
- 66% - Somewhat effective: Struggle to work cross-channel; difficult to integrate with other applications and tools
- 18% - Ineffective: Fail to keep up with evolving threat landscape
- 6% - Not applicable: Current levels of fraudulent activities don't warrant the investment in controls

Source:

1) 2012 Faces of Fraud survey, Information Security Media Group, 200 US respondents

We need to see online banking fraud in the context of cyber security threats[1]



Indicates malicious activity on the Internet

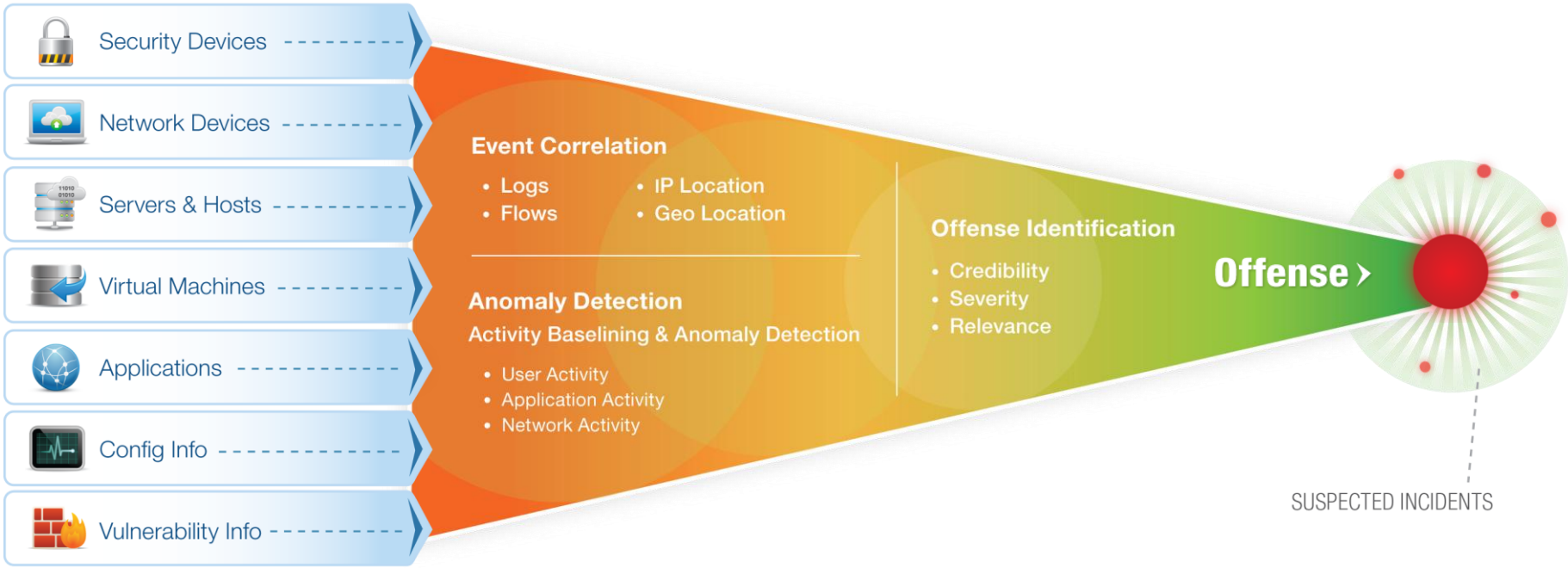
New Attack Activity

- Rise in phishing based malware distribution and click fraud
- Rise in Shell Command Injection attacks

The Challenge of Mobile and the Cloud

- Mobile exploit disclosures up
- Cloud requires new thinking
- Social Networking no longer fringe pass-time

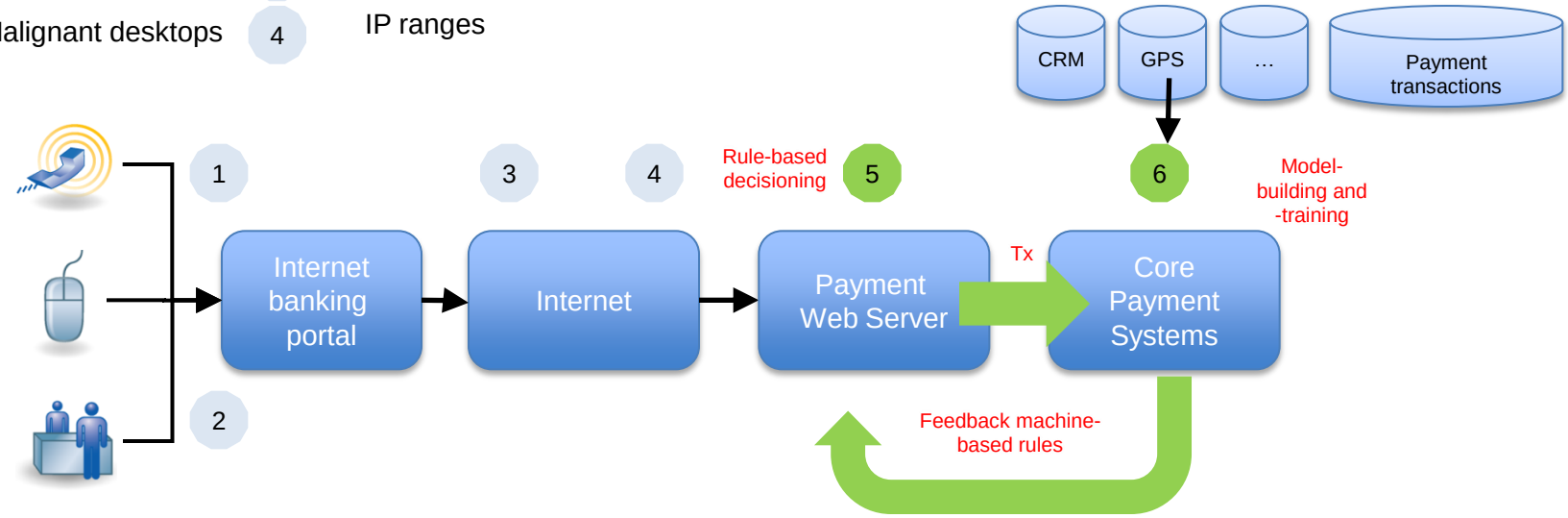
IBM is unique by taking a data-driven, machine learning approach to detection



Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

IBM's solution adds cross-channel, real-time behavior-based detection upon execution

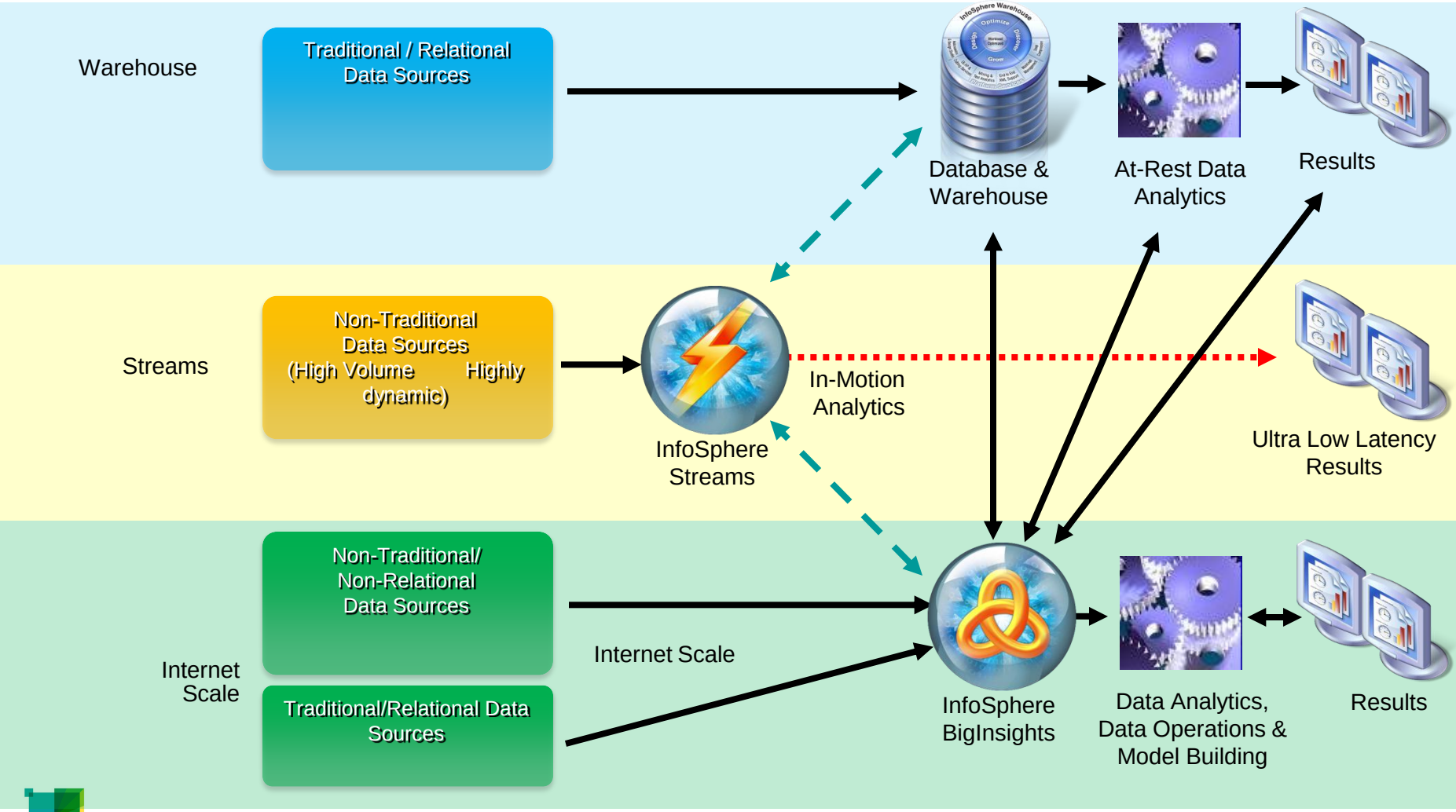
1 Mules
2 Malignant desktops
3 Botnets
4 IP ranges



- The internet-based payment cycle originates from consumers who use their desktop to work with a bank's internet payment portal.
- Banks have usually implemented different mechanisms to identify and monitor fraudulent activity in the browser, on the internet and in between the network points.
- Most banks have put in place different solutions to serve monitoring needs in these control points.
- Data from these points could hold valuable addititional information that could be included to enhance analytical insight.

- IBM proposes to automate preventive fraud detection by deploying a real-time rule-based decisioning engine. The engine will provide two key capabilities:
  - Real-time rule-based decisioning on inbound transactions with easily configurable, reusable business rules
  - Data mining and pattern analysis on historical data sources, including payment transactions, CRM and other data sources. Data mining is focused on obtaining deep insight into the characteristics of fraudulent transactions.
- By combining these capabilities, a bank will install a learning machine from the back-end analysis to real-time prevention of fraud. Each cycle will strengthen barriers and further reduce investigative back-log.

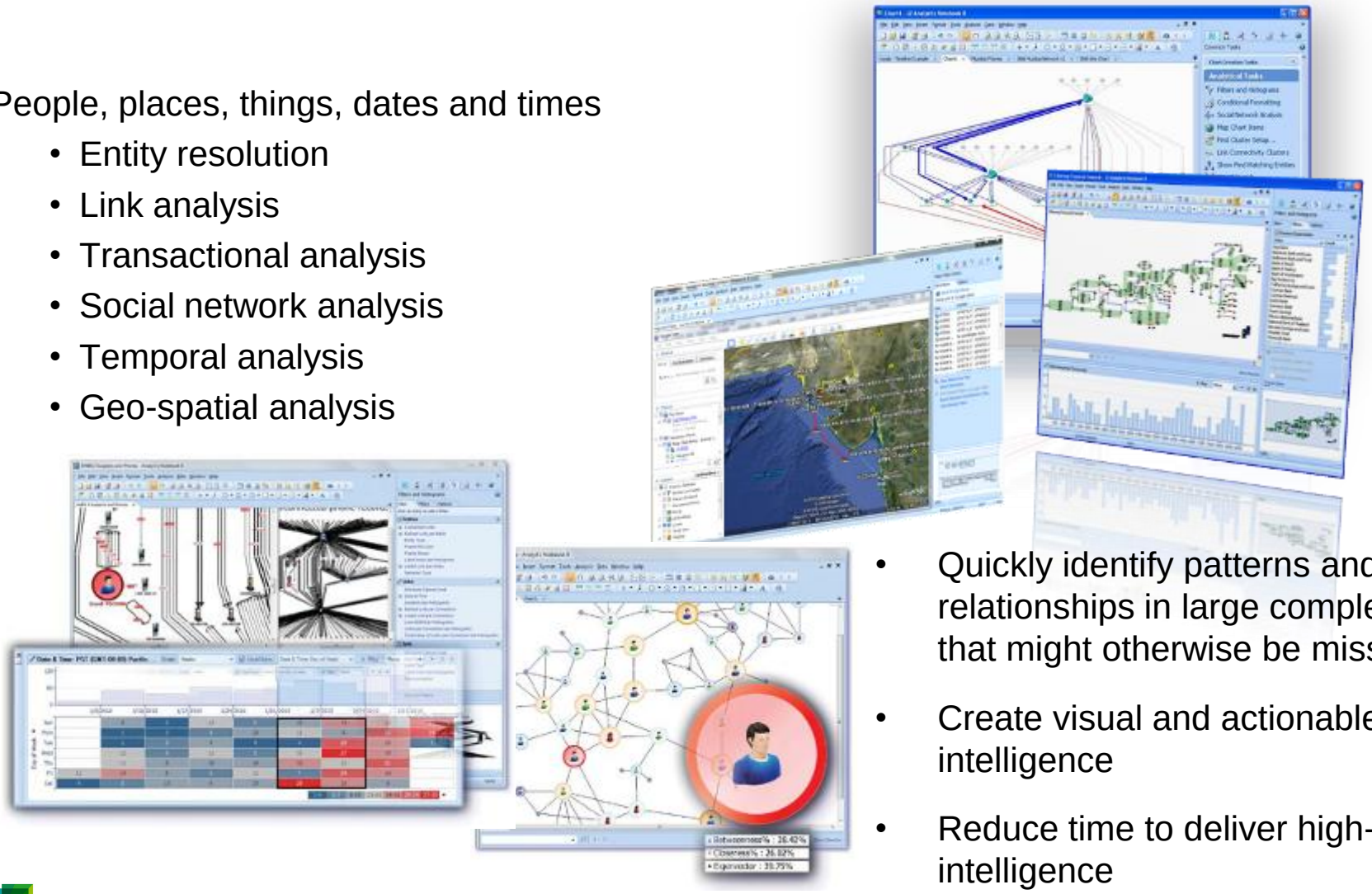
Cross new boundaries with new technologies: A Big Data approach to fraud



Don’t look for the fraud, look for the fraudster

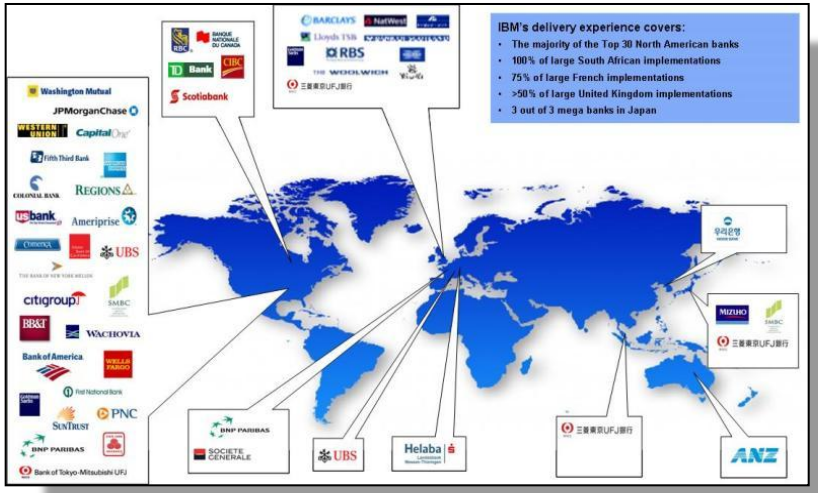
People, places, things, dates and times

- 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

IBM is growing a significant global financial crime competency



Client Problem	Benefit
Monetary Fraud	Large on-line retail bank in Singapore with over 1.75 million users improves security with TAS implementation.
Sanctions Screening	Reduced watch list checks from 8-12 hours to less than 15 minutes, increased names checked from 2,500 to more than 40,000, reduced false positives by 75%, realized ROI in 3 months
Credit Risk Scoring	Reduced bad debt by 15+% and credit score every customer daily
AML Transaction Monitoring	Improved efficiency by 60% reducing administrative costs, reduced alerts by 90%, increased accuracy by 60%
Online Fraud Detection	Lowered fraudulent transfers by 50% 70% false positive reduction by eliminating unnecessary customer validation calls
Link Analysis	The system helped prevent more than 1,000 customers from losing funds to fraud in the first 50 days of its use. reduced fraud by 30 percent during that same period while improving AML compliance requirements.


IBM Software
WebSphere

Thought Leadership White Paper

Preventing fraud in credit and debit card transactions

Look beyond packaged solutions for a holistic approach

Let's build a smarter planet

Visa Europe

Processing payments with unprecedented agility and reliability

Smart is...

An open clearing and settlement platform that allows Visa Europe to create and implement vast numbers of complex business rules faster than ever before.

Visa Europe addressed the unique nature of the European market by building a **new payment platform** which houses tens of thousands of business rules governing payment clearing and settlement. An open business rules management system **speeds time-to-market** and gains **cost efficiencies**. The result is greater business agility and competitiveness for both Visa Europe and its 4,000-plus member institutions. Simulation capabilities are soon expected to allow business users to **become more proactive, predicting and assessing the impact of changes** to key business rule parameters.

The European marketplace is highly complex. Efforts to unify it from an economic and commercial standpoint have been under way for decades, yet to this day it is still comprised of many discrete markets, currencies and sets of regulations. One of the latest efforts to strengthen the market through unification, led by the European Union was the creation of the Single Euro Payment Area (SEPA) and ratified by European Union member states adopting the Payment Services Directive (PSD, 2007/64/EC).

The SEPA initiative created a common set of rules for payments in countries using the Euro, under which all electronic payments are considered domestic, even those that take place across national borders. The goal was to create greater efficiency and promote commerce.

A strategic response to these specific and unique European member institutions business drivers was required and, as a result, Visa Europe became a dedicated European payments provider and wholly independent organization from the global payments provider Visa Inc.

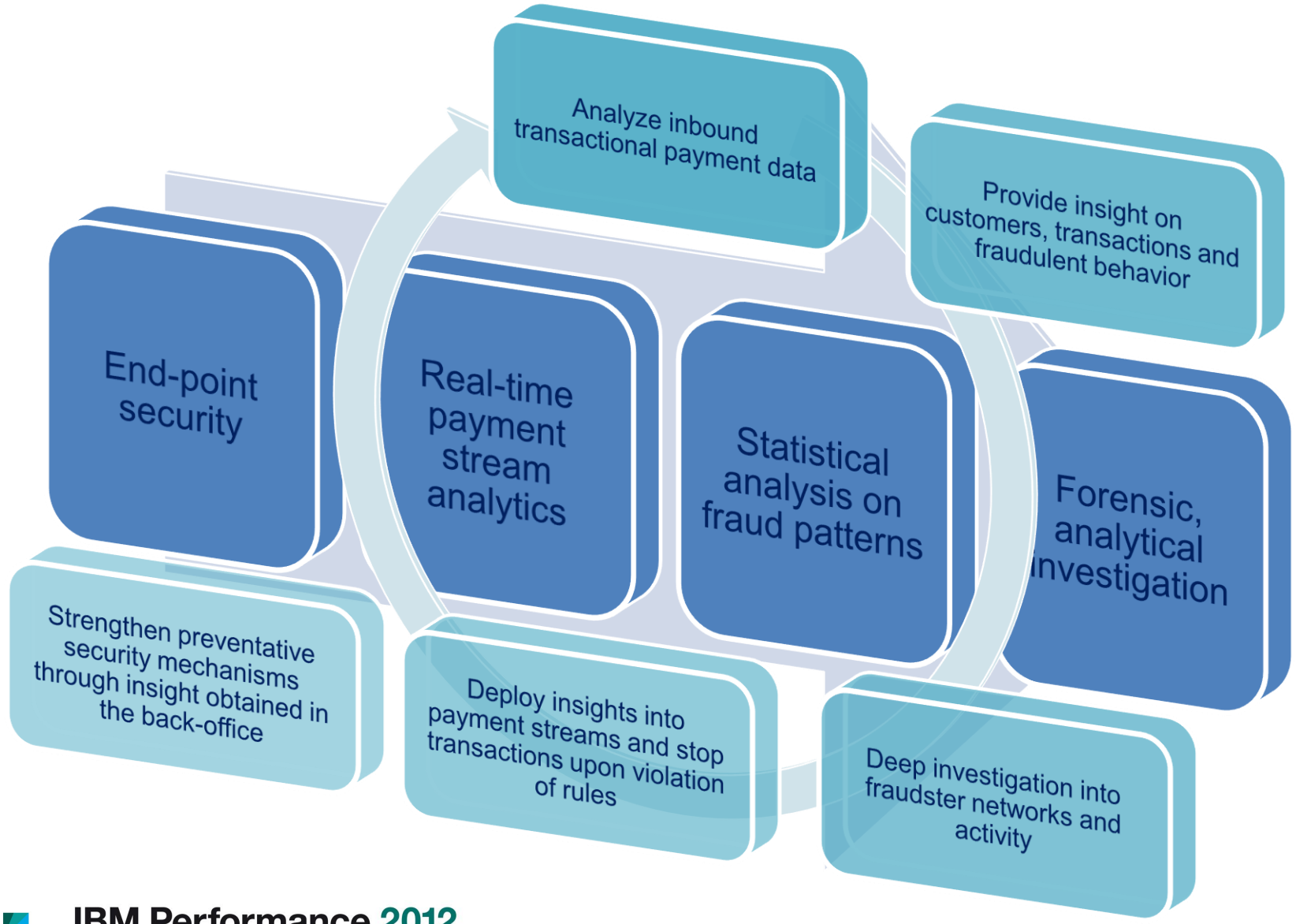
A complex landscape calls for a new approach

Growing Visa Europe in response to the nature of the European environment became a challenge while remaining part of the global Visa Inc organization and global set of demands for change. This made it difficult to make responsive changes to shifting regulations and market conditions. This is why the creation of a dedicated European organization was deemed a wise move.

The issue is one of complexity. Each time a Visa card is used anywhere in the world, an authorization takes place and a transaction is created between the issuer's financial institution and that of the merchant. At the end of each day, all of those millions of transactions must be settled.

IBM

Conclusions



Questions

Marco Gomes
Industry Solution Architect
Business Analytics
IBM Software Group

+31 (0) 205133544
+31 (0) 615005091

marco.gomes@nl.ibm.com