IBM i2 Fraud Intelligence Analysis

Identifying, investigating and disrupting fraud

Highlights:

- Analyze and visualize complex cross-channel attacks
- Involve relevant staff and agencies in investigations
- Integrate fraud investigation into standard procedures
- Provide briefings according to role and responsibility

Fraud is a significant and evolving challenge for the financial industry, costing an estimated five to eight percent of revenues1 per annum. Criminals are becoming increasingly adept at exploiting weaknesses across multiple systems, possibly in collusion with employees, and attempting to hide in the siloed nature of Enterprise data. As well as damage to the balance sheet, fraud poses a real threat to brand and reputation with potential impact on customers, shareholders and regulators. However, each interaction with your systems leaves a small breadcrumb and with it, the opportunity to intelligently link them to identify, detect and disrupt threats.

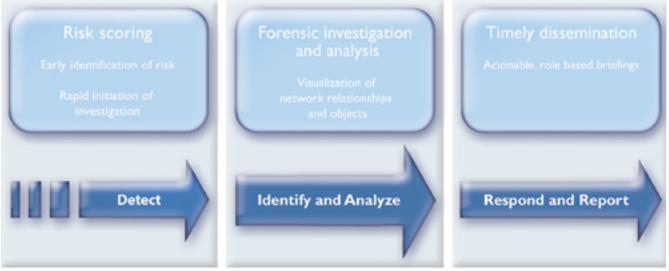
Traditionally, companies have countered fraud with point solutions that target a specific, known threat. This approach can be difficult to manage, often missing cross-channel and asymmetric attacks perpetrated by organized criminals and, almost always, resulting in a more expensive, fragmented solution. This “rear view mirror” approach can also fail to spot new and emerging attacks.

IBM® i2® Fraud Intelligence Analysis is designed to provide critical insights to aid in investigating complex incidents, producing actionable visualization of critical people and events and documenting results for potential litigation.

If you cannot see the full picture you cannot respond

Fraud Intelligence Analysis takes an holistic approach to this problem by providing:

- Inclusion of virtually any data source to provide comprehensive visibility of activity.
- Event and rule driven procedures to aid faster remediation and to support Know Your Customer and Customer Due Diligence.
- Distributed investigative and collaborative tools designed to leverage relevant skills and knowledge to improve results.
- Identification and forensic investigation of suspicious or unexpected activities and threats using market-leading analysis and visualization tools.
- Automated briefing updates based on role and responsibility which allow analysts and investigators to share evidence and analytical results in near-real time.



Governance, risk and compliance

The nature of fraud demands that detection, management and treatment fall within the GRC functions of an organization. The differing, but interlinked, requirements of risk management, compliance, and internal and external investigation groups demand different views of fraudulent activity and, most importantly, proof to support decisions and actions.

Fraud Intelligence Analysis is designed to provide each of these corporate functions with the ability to view appropriate elements of fraud patterns and to collaborate more effectively so that appropriate actions can be taken to meet the needs of each department for the management and treatment of fraud.

Analytics and visualization

Fraud Intelligence Analysis includes market leading analytical tools designed to provide rapid forensic investigation of abnormal and unexpected behavior.

With this solution, vast quantities of data from unrelated sources can be analyzed and visualized in a number of rich formats to support your investigation.

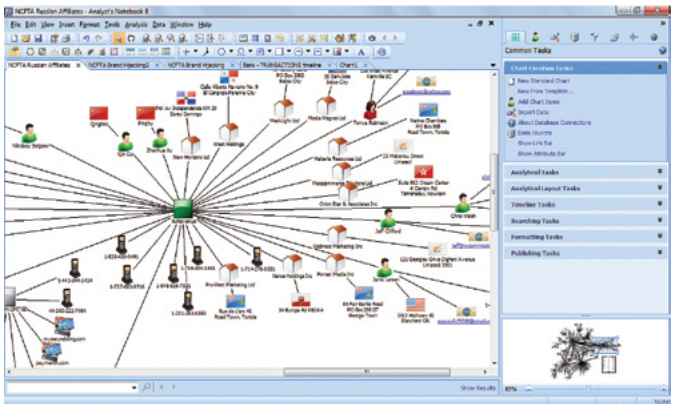


Figure 2: Association - who knows who and how are they linked?

Risk alerting

Early identification of possible fraud can eliminate the cost, time and pain associated with complex investigations and reclamation. Knowing "who is who" and "who knows who" is critical to this process. Key fraud indicators combine information from watch lists, known fraudsters and other relevant sources in a risk scorecard that provides visibility of risk to help enable proactive remedial action.

Collaboration and investigation

Fraud prevention requires intelligence and involvement from across your organization. Fraud Intelligence Analysis provides an intuitive, security-rich interface for stakeholders to contribute to, share and analyze investigative data leading to faster, more informed decision making.

Investigation management

IBM i2 Fraud Intelligence Analysis can be adapted to support your internal processes. Business rules and events may may b combined to form standard operating procedures (SOP's) and support your Compliance requirements.

Investigation monitoring

Providing visibility of the fraud investigation can greatly assist both investigation efficiency, and also improve fraud awareness across your enterprise; a great asset in the fight against fraud. Key performance indicators (KPI's) can be used to monitor progress and KPI and related content may be displayed through user and role specific dashboards.

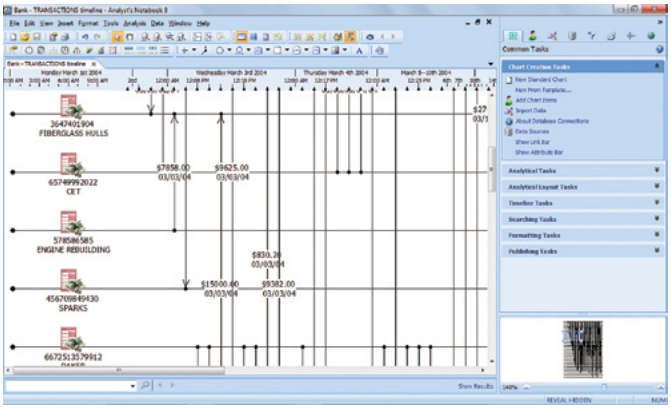


Figure 3: Temporal - incidents and involved parties on a timeline

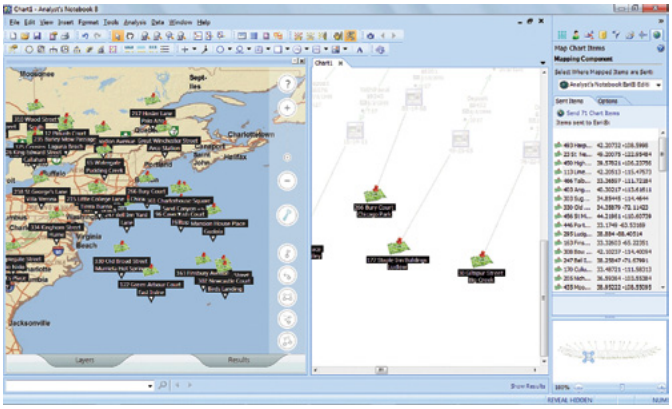
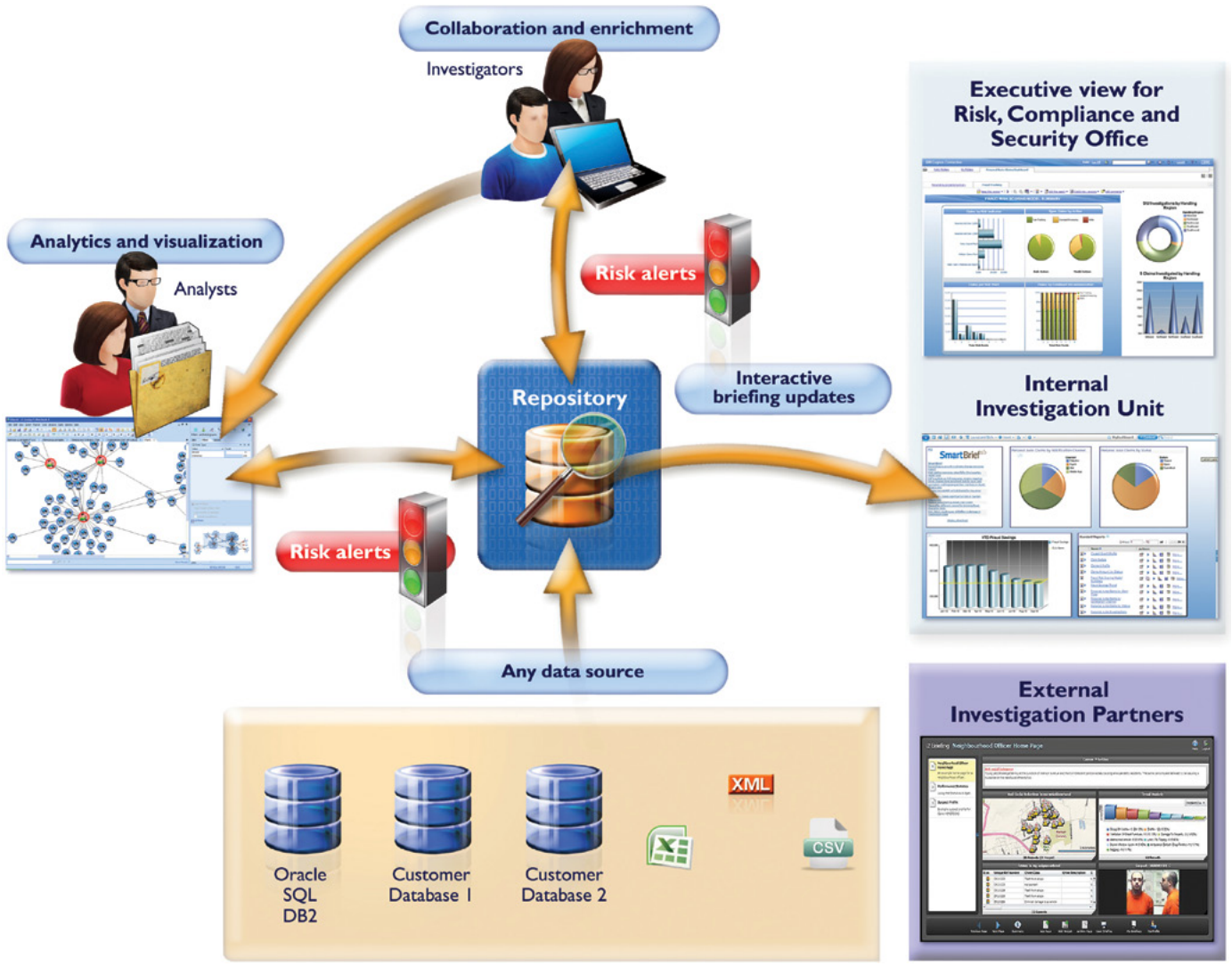


Figure 4: Geo-spatial - incidents on Maps



Combating cross-channel attacks

Data may be locked in disparate, unconnected databases and can be in a structured or unstructured form.

Fraud Intelligence Analysis is designed to combat this by working across your data silos to provide a “joined up”, rich view of related events, people and objects.

Potential benefits

- Faster implementation and returns, typically within weeks.
- Flexibility. Data can be left on existing servers and investigative and briefing interfaces are delivered over thin client.
- Alignment with your internal information policy. Only appropriate information is available to users based on role.
- Extensibility. Can be integrated with existing systems as well as other IBM solutions.

Financial fraud user cases

Major US Insurer: $250,000 fraudulent claim successfully identified and investigated within three hours

A major US insurance company received a suspicious claim for a stolen automobile and had only thirty days to determine whether it was legitimate before being obliged to settle. Using Fraud Intelligence Analysis, the investigator was able to rapidly investigate the social network connected to the owner of the vehicle and discovered a link to an unusually structured export company. By enriching his investigation further through collaboration with the US Customs and Border patrol, he determined that the vehicle had been exported several weeks before the claim. The investigator tracked the car to Italy and found additional proof that it had been serviced there and the identity of the new owner was the wife of the claimant with an assumed identity. The claim was denied and handed to law enforcement.

"Using Analyst's Notebook, I was able to clearly identify a claim as fraudulent in less than three hours, an accomplishment that would have taken months without the i2 product."

— Raphael Lawson, Head of Fraud, Fraud Investigation.

For more information

To learn more about IBM i2 Fraud Intelligence Analysis, please contact your IBM representative, or visit: **ibm.com**/i2software

To learn more about all of the IBM Smarter Cities solutions, visit: **ibm.com**/smartercities

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America

November 2012

1 Forrester Market Overview: Fraud Management Solutions 2010.

Please Recycle

ZZS03075-USEN-02