Bell Integration

TRANSACT

TRANSFORM

RUN

RECYCLE

Fraud Analytics

Detect, Discover, Investigate, Prevent

IBM Platinum Business Partner™

Introduction

Around the world, fraud is an ever-increasing risk for businesses of all kinds and in every sector.

According to the Economist Intelligence Unit's 2015/2016 Global Fraud Report, 75% of the companies surveyed had been victims of fraud in the past year. Unsurprisingly, fraud is a particularly serious issue for financial institutions.

Indeed, Crowe Clark Whitehill's The Financial Cost of Fraud 2017 report identifies fraud as "the last great unreduced business cost". Based on reported losses, the study estimates that £125 billion is lost to fraud each year in the UK alone – that's more than the UK government spent on defence or education in 2016.

As prevalent as the fraud problem is, it can be a particularly tricky issue to address – especially for the financial services sector. Factors that contribute to the challenge analysts and investigators face include:

- The sheer volume of transactions that are handled
- The speed with which technology allows fraudsters to operate
- Siloed data sets; the difficulty of including external data sets and databases; the challenges of cross industry data collaboration
- Trying to make sense of the huge number of spreadsheets generated when undertaking an investigation.

In recent years, however, powerful visual intelligence analysis environments like IBM i2 Analyst Notebook have helped transform the fraud-detection efforts of public sector and commercial organisations alike, making it possible to:

- Gain full visibility of cross-channel and asymmetric attacks
- Create actionable visualisations of critical people and events
- Identify who knows who – and how they are linked
- Connect to and query multiple data sources
- Clearly communicate analysis findings in near real-time
- Use built-in investigation management and coordination tools to track and record key findings and decisions
- Document and share results and proof points for potential prosecution.

That's good news for financial institutions and government agencies seeking to identify actionable intelligence hidden within disparate data sets - and to build a single cohesive intelligence picture of complex fraud activities and networks.

The Industrialisation of Fraud and Financial Crime

Opportunistic acts – those in which individuals operate in an unplanned way and exaggerate or leverage a genuine claim or transaction - can often be dealt with early in the client interaction.

Complex schemes, however, require information from many disparate data sources to be combined before the full picture can be viewed and understood. Something that may seem nigh on impossible when faced with overwhelming volumes of data.

Gangs may be organised locally or regionally and may use a variety of online and offline approaches to communicate and organise or perpetrate an attack. All of which adds to the challenge for organisations seeking to achieve a global view of what's going on so they can identify and prevent cross-channel threats.

Canadian Bank Uncovers Mortgage Fraud Conspiracy

When a Canadian bank discovered what it believed to be the largest case of mortgage fraud in Canadian history, it needed a solution that would help it uncover the key players, investigate the complex data relationships between these parties and provide prosecutors with the evidence needed to dismantle the elaborate scheme. The bank also wanted to detect and prevent future mortgage fraud.

Using IBM i2 Analyst's Notebook software, the bank was able to organise and analyse multiple forms of data ingested from a variety of sources. This helped it quickly uncover key data and complex relationships, producing actionable intelligence that helped identify key members of the criminal network.

This included being able to pinpoint hundreds of people – including an MP, lawyers, mortgage brokers and four employees - who were part of a sophisticated criminal network made up of 14 interconnected groups.

The investigation stopped a mortgage fraud network that had stolen $140 million (USD) in its tracks and saved potentially millions of dollars on future loses by providing better fraud protection.

The growing 'industrialisation' of fraud schemes and activities demands a dynamic, intelligence driven approach. Clearly, today's organisations need the widest possible range of analytical capabilities if they are to undertake investigations in the most efficient way possible and respond fast.

In our experience, that means having:

- Data analytics that can connect, extract and fuse data from different sources into a unified 'analysis ready' whole.
- Flexible data ingestion models that enable investigation teams to access the internal and external data sources they need.
- Entity analytics to determine who-is-who and who-knows-who across fragmented data sets.
- Detection analytics to automatically uncover and flag potential fraud.
- Link analytics to understand and uncover relationships between people, organisations and events.
- Social network analysis to determine key players in large networks and chart relationships to support understanding of complex fraud and fraud rings.
- Reporting analytics to get the right information to the right people, in the right format.
- The ability to undertake detection in real-time or in batch – depending on the industry and transaction type.
- Timeline analysis – to quickly view temporal transactions.
- Geospatial mapping – the ability to map entities like people/vehicles/locations.
- Histograms and heat maps to identify spikes and regular event patterns.
- Content analytics capable of extracting key information from high volumes of unstructured data such as documents and web pages.

Tackling Fraud Head on

As we've seen, fraud is a growing issue for organisations in both the public and private sectors. That's especially the case for insurers. Indeed, according to a recent Accenture survey, insurers say they've seen a jump in fraudulent claims in recent years who also acknowledged that better fraud detection capabilities could help shave 5% of the claim costs.

Asked to identify the most important initiatives for strengthening their anti-fraud capabilities, they prioritised the following abilities and initiatives as being key to improving detection and prevention capabilities without adversely affecting the processing of legitimate claims:

- ➔ Improve the collection and analysis of internal and external data
- ➔ Employ predictive modelling, reviewing historical fraudulent claims to identify factors and elements that can help prevent future fraud
- ➔ Analysing the relationships that exist between the players involved in fraud to better detect organised insurance fraud

The velocity, variety and veracity of data generated in the claims handling process makes the use of statistical models based on sampling methods obsolete.

However, since analytics integrates data from diversified channels and makes it possible to combine internal data with third-party data, many insurers have started to use analytic techniques to detect and prevent fraudulent claims – and in some cases recover monies.

Turning Data into Intelligence

If you can't see the full picture, you can't respond. So, alongside adopting a holistic approach to fraud investigation that leverages market-leading analysis and visualisation tools, organisations need to be confident that analysts and investigators can share evidence and investigative findings in near-real time.

Complex fraud can touch many operational processes and systems, and the ability to work collaboratively and inclusively is vital when fighting complex organised attacks.

Indeed, breaking down the investigation silos will result in a rich and constantly refreshed source of intelligence that can be used to:

- ➔ Shorten future investigations
- ➔ Identify collusion and fraud rings
- ➔ Support detect and prevent strategies by surfacing intelligence in business systems and processes.

That's especially the case if you need to combine information from watch lists, known fraudsters and other relevant sources to create a risk scorecard that provides the 'risk visibility' that's required to take proactive remedial action fast.

Similarly, ensuring all investigation stakeholders across the organisation have full visibility of the fraud investigation is a key asset that can greatly assist investigation efficiency and demonstrate outcomes in a wider business context.

Solutions like IBM i2 provide reports that can be used by a variety of stakeholders:

- ➔ Investigators and analysts – lists of current investigations, performance
- ➔ Head of Investigation – oversight of team/individual performance, trends by investigation type, analyst utilisation
- ➔ C-suite/management reporting – oversight, performance, trends and financial analysis; demonstrating a stance against fraud and financial crime

Who Benefits from Fraud Intelligence Analysis?

Role	Activity
Chief Risk Officer	Risk reduction and improve stance against fraud.
Chief Finance Office	Improved financial rations, operational and efficiency improvements.
Chief Security Officer/Chief Information Security Officer	Greater understanding of cyber threat and attack vectors.
Head of Fraud	Improved investigation metrics – increased likelihood that fraudsters move to softer targets.
Head of Claims	Reduced payments to fraudulent claims and improved bottom line
Money Laundering Reporting Officer (MLRA), Chief AML Office	Ensuring entity resolution across business groups to achieve compliance.

Detect, Disrupt and Prevent

A globally recognised industry standard tool for intelligence analysis, IBM i2 Analyst's Notebook has become the 'go to' tool used by analysts to quickly collate, analyse and visualise data from disparate sources and reduce the time required to discover key information in complex data.

Indeed, we work with government agencies and businesses across a wide range of sectors, helping them use IBM i2 Analyst's Notebook to generate timely and actionable intelligence that can be used to identify, predict, prevent and disrupt criminal terrorist and fraudulent activities.

In our experience, i2Analyst's Notebook helps organisations to:

- **Rapidly piece together disparate data** into a single cohesive intelligence picture.
- **Identify key people, events, connections and patterns,** using innovative features like social network analysis, 'list most connected' and 'find connected networks'.
- **Increase understanding of the structure, hierarchy and method of operation** of criminal, terrorist and fraudulent networks.
- **Simplify the communication of complex data** to enable timely and accurate operational decision making.
- **Use visual analysis to boost investigation timeframes** and productivity.

Skipton Building Society – Smarter Financial Crime Investigations with Visual Intelligence Analysis

IBM i2 Analyst's Notebook helps Skipton's financial crime analysts identify connections between potentially suspicious transactions and reduce investigation timeframes by 80%.

As fraudsters get smarter, financial services companies are having to innovate. Which is why forward-thinking organisations like Skipton Building Society are turning to visual analytics technology platforms to help detect fraud attempts, minimise losses and prevent further exposure.

Introducing IBM i2Analyst's Notebook to the analyst team helped eliminate the time-consuming manual aspects of investigations. Now, as soon as Skipton's analysts find evidence of wrongdoing or identify a potential suspect, they can easily create simplified summary diagrams that can be shared with investigators and other shareholders or output as part of a report.

Faster analysis has helped Skipton react to fraud and crime incidents faster, stopping fraudsters in their tracks and blocking further criminal activity – without impacting business-as-usual.

Next Steps

Fraud is an ever-present threat for any organisation and the methods used by fraudsters are becoming increasing sophisticated.

Notoriously complex to unravel, it's imperative that businesses have the necessary defences in place to detect and prevent fraudulent activity.

Clearly, implementing top-quality fraud analytics into your organisation delivers the advantage of early detection and ensures you have the right tools in place to meet your compliance obligations.

And that's where solutions like IBM i2 Analyst's Notebook can help.

If you'd like to discover how to arm your analysts and investigators with multi-dimensional visual analysis capabilities that allow them to quickly uncover hidden connections and patterns in data, we should be talking.

Why not join us for a personalised demonstration of this powerful visual analysis tool?

Contact us to arrange a 1-2-1 demonstration, during which, we'll show you how to use innovative features like connected network visualisations and social network analysis. We'll also demonstrate how geospatial and temporal views can help uncover hidden connections and patterns in data.

We can even tailor the demonstration around a specific investigative challenge your organisation is currently facing.

To see for yourself how quickly you can generate the insights needed to identify and disrupt criminal, cyber or fraudulent threats, then contact us on:

marketing@bell-integration.com
or visit www.bell-integration.com