Using an IBM i2 Solution to Investigate Fraud and Financial Crimes

The combination of machine-led analytics and human-led analysis capabilities helps users quickly find hidden connections and non-obvious patterns to pinpoint the illicit activities of the sophisticated fraudsters.

Highlights:

- Visualize fraudulent activities by ingesting and analysing large, disparate silos of data sets with unprecedented speed
- Open your fraud defenses aperture with comprehensive analysis, in near real-time
- Quickly identify threats, fraudsters, illicit activities and hidden criminal connections with multi-dimensional visual analysis and advanced analytics
- Securely share insights and intelligence within, across and among organizations, using i2 charts and dashboards

Introduction

Moving faster than the speed of threat and thwarting illicit activities of the fraudsters and criminals with an effective and efficient solution is a goal of many financial services sector and other organizations. This goal is achievable when using existing rules-based systems together with threat and intelligence analysis to outsmart sophisticated fraudsters.

The exponential rise in the sophistication of Fraud and Financial Crimes means that the addition of human-led investigation and intelligence analysis is another crucial step organizations must take, regardless of the impact to standard operating procedures. Keeping an asymmetrical advantage over criminal activities is a never ending battle and winning the battle does not come with any rewards. The only outcome is that normal business operations are not impacted.

In this solution approach guide, we will discuss how using an IBM i2 solution to investigate fraud and financial crimes can help an organization achieve an asymmetrical advantage by removing the fraudsters greatest weapon, their ability to remain concealed. IBM i2's industry-leading, multi-dimensional intelligence analysis offers a powerful solution that helps users simplify complex networks and detect non-obvious relationships and hidden patterns.

An IBM i2 solution can be used for many types of fraud and financial crime, such as:

- Money Laundering
- Crime / Terrorist Financing

- Insurance Fraud
- Bribery and Corruption
- Sanction List
- Tax Evasion
- Credit Card Fraud
- Counterfeiting
- Insider Fraud
- Securities and Trading Fraud
- Retail and Online Trading
- Embezzlement
- Gaming & Betting Fraud
- Money Transfer and Payment Frauds
- Supply Chain Compromise

Regardless of the fraud and financial crime types, four attributes hold true:

1) There is always an individual or group of individuals behind all frauds.
2) Sophisticated fraud generates digital footprints that can be followed, if discovered.
3) Remaining non-obvious and undetected is key to a successful fraud attack.
4) Fraudsters will continue to evolve their attack vectors until successful.

The Need for Threat and Intelligence Analysis

National security and law enforcement has relied on IBM i2 solutions for nearly 30 years, helping analysts turn overwhelming and disparate data into actionable insight and intelligence, in near real time. The solution can help ensure an understanding of your threat landscape and identify vulnerabilities so as to disrupt and uncover threats. It can help you quickly find hidden connections and critical patterns buried in internal, external and open-source data.

IBM i2 solutions for the investigation of fraud & financial crimes can yield the following benefits:

- Identify attempts at fraud, money laundering and cybercrime-related activities
- Reduce the volume of false positive and false negative alerts while increasing the quality of alerts
- Uncover complex, suspicious cross-channel fraud sooner
- Distinguish fraudsters from your valued customers quickly
- Improve analyst and investigator effectiveness and efficiency
- Reduce losses and minimize the impact to the customer experience
- Help meet regulatory compliance obligations
- Employ enterprise intelligence to continuously adjust operations and stay ahead of trends.

Overall, a threat and intelligence analysis solution needs to increase understanding of complex criminal, terrorist, and fraudulent networks. An IBM i2 solution for the investigation of fraud and financial crimes allows analysts to gain better insight and understanding of the structure, hierarchy and ‘modus-operandi’ of complex networks, aids the decision-making process and ensures best resource utilization for operational activities in network disruption, surveillance, or suspension.

Where to Start?

Fraudsters are smart agile people therefore we need similar types of people to mount a defense. To move faster than the speed of threat and outthink the fraudsters requires a dedicated team. In some cases, these teams may exist today within an institution. Going forward, it is anticipated that these type of teams will be more common.

Special Investigations Unit (SIU) / Fraud Investigation Unit (FIU)
The SIU / FIU can be the operational heart of intelligence analysis for an organization. It is typically staffed by a Head of Intelligence Unit with analysts of various seniorities, supervisors, investigators, case managers and researchers. The primary value add of such a unit is to produce actionable intelligence for key decision makers that clearly identifies fraud and financial crimes patterns or areas of potential vulnerability. These teams need to be operated across many business functions as it is critical that they can follow a lead to discovery and thwart sophisticated attacks.

By doing so, it models itself around the success of law enforcement and military intelligence analysis units.

It is important to recognize that the primary goal is not typically prosecution against an individual or an organization, but to reduce the organization's financial losses, exposure, and reputational risk of financial crimes. In addition, the organization will be expected to adhere to legal directives that require proactive stance on financial crimes. For those organizations wanting to take legal action against perpetrators, they would pass information on to law enforcement.

Get the basics right and build from there
Every organization has some defenses. There are many vendors that supply excellent real time rules engines to detect and alert on transactional issues. Examples of common alerts from rules engines could include:

- Alerting on person-of-interest on a sanction watchlist who is interacting with your organization
- Cancel credit cards being used at a POS (point of sale)
- Large sums of money deposited to unknown accounts by unknown depositors
- False insurance claims.

Transactional detection rules will easily alert and stop these activities if the rules have been configured previously for these known detection triggers. For more advanced detection, rules engines need to correlate connected events from many parts of the organization to raise an alert and stop all the associated transactions.

These real time, inline rules engines will stop a significant quantity of illicit activities. Once detected or discovered response teams can also get involved, i.e. they may update a customer to a possible fraudulent account takeover on their account. More often than not they need to validate a false positive and reset rules logic.
Yet there are shortcomings to this rule-based approach:

- Rules engines can only detect and discover issues against known activities or patterns
- Organizations can over rely on rules
- Sophisticated frauds are designed to circumvent rules
- There are always rule gaps
- Rules are focused on detecting the attack and not detecting the seamless harmless preparation.

These rules engines should be optimized to catch as many illicit activities as possible to reduce the workload on those groups using a threat and intelligence analysis solution.

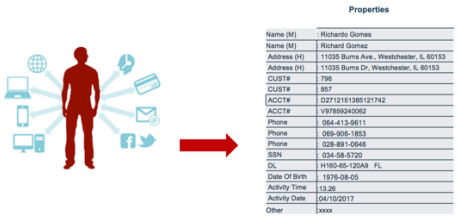
How to Investigate Fraud and Financial Crimes

Start with the "why" investigative analysis:
Given rules-based defences do not stop all fraudulent activities, it is important to consider that:

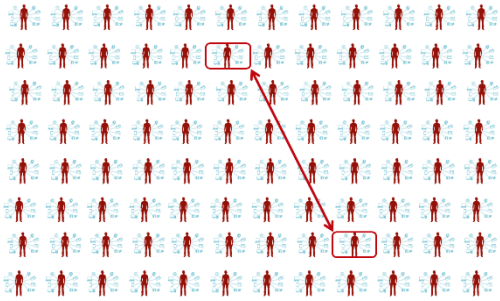
- Staying concealed and the use of non-obvious illicit activities give the fraudsters and financial criminals the best possible chance of success
- Not all frauds start inside an organization - planning and preparation can be started externally yet still have a traceable digital footprint that can be seen if using the proper tools
- Everything is connected; finding relevant connections and linkages is the main goal of the investigator, this in turn allows them to produce actionable intelligence used by intervention teams.

Understanding link analytics
If everything is connected, there must be a way to represent linkages that connect individuals, entities and events. This is called *link analysis* which is a data analysis technique used to evaluate relationships (connections) between nodes (objects). Relationships may be identified among various types of nodes, including organizations, people and transactions. These links are connected via Entity-Link-Property (ELP).

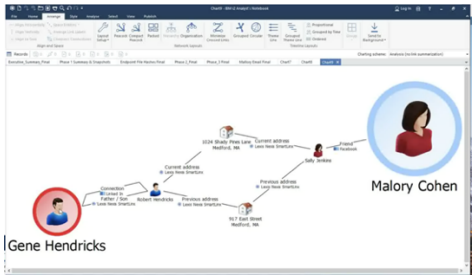
We all have attributes that define us.



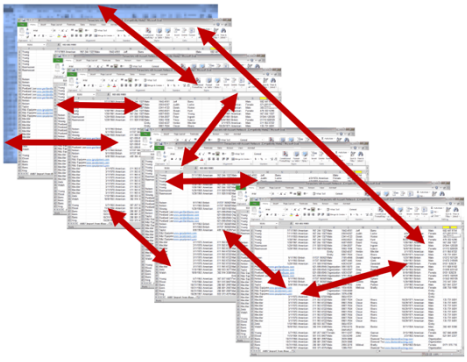
Identities and entities have attributes (properties).



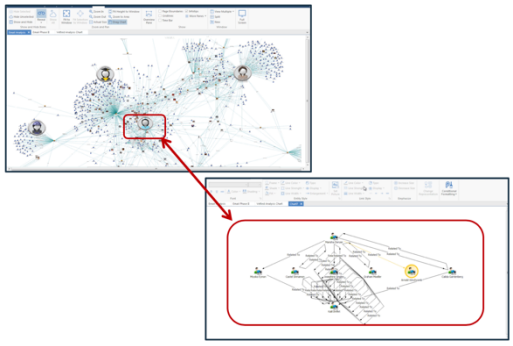
ELPs can link individuals together over multi-degrees of separation and across data sets.



A simple example of this cross linkage: Person 1 is friends with Person 2 on a social media site. Person 2 lives with Person 3 as found on a commercially available public domain data provider. Person 3 is the father of Person 4 and a director in his company. Therefore, Person 4 has a connection to Person 1 that was found in data existing outside an organization yet easily accessed.



By using link analytics one can find patterns across many data sources, both internal and external, and then with their attribution can find linkages between individuals to individuals, organizations to organizations, or some combination of both.



Once these linkages are identified, they can be isolated to surface the illicit network of transactions (e.g. AML) or connected people (e.g. insurance fraud). These are just simple examples of how link analytics is used in fraud and financial crimes investigations.

The quantity of combinations / permutations of links in a network can be extremely large. For example, 100 individuals with 12 attributes per individual (name, phone number, address, IP, etc.) can have 117,612 possible connections:

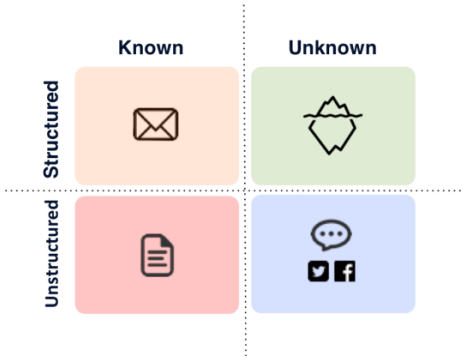
$$(100\text{-}1)^2 \times 12 = 117{,}612$$

Possible connections can range in the billions when the quantity of entities in a network is 30,000+, which as an example, could be a mid-size bank. Pivot tables and rules engines will most certainly struggle or fail in processing such large numbers. Therefore, the combination of machine-led analytics and human-led analysis capabilities will allow you

quickly find hidden connections and non-obvious patterns that pinpoints the illicit activities of the sophisticated fraudsters. To find these linkages requires access to data.

Where does the data come from?
When investigating fraud and financial crimes it is key to open the aperture to allow data to be seen across many data sources. Fraudsters will look to conceal their illicit activities by hiding from the detection rules. Unusual patterns may not be seen in just one data source or even in one type of data. Looking across many data sources and many data types can allow concealment to be more easily seen. Organizations must consider the ingestion of data and intelligence from beyond their structured data stores.

There exists 4 *Quadrants of Data,* that when merged, can uncover the real fraudsters patterns and intent. An IBM i2 solution can merge data from these 4 areas:



- Known / Structured Data:
  Highly structured data stored in the organization's data bases that can contain financial transactions, customer information, historical activities, etc.

- Unknown / Structured Data:
  Located in the deep dark web. A very large percentage of the Internet is not indexed by popular search engines. There exists a wealth of structured information in unknown locations. Early stage fraudulent activities can exist in the deep web. Identifying these activities by key words or phrases enables the link analysis solution to anticipate possible incoming frauds.

- Known / Unstructured Data:
  Enterprise information can be stored across the organization in many unstructured documents such as: csv, pdf and doc files, threat reports, etc. Analysis of this overwhelming data can reveal hidden insights that would otherwise be missed. The ability to use previously stored intelligence and data from sources across the entire organization is key.

- Unknown / Unstructured Data:
  Social media sites may offer linkages between people and events that are not known by the organization. Additional network analytics can be supplemented by social media data, i.e. who's connected to who.

Using readily available data ingestion tools, these different types of data can be easily ingested into an IBM i2 solutions to offer a highly enriched view of the person(s) of interest or entities of interest. When investigating bribery, corruption, insurance fraud and sanction list violations, much of this information will come from OSINT (Open Source Intelligence) data.

What starts an Fraud and Financial Crime investigation?

An investigation can be started from 3 main trigger points:

- Trigger Point 1: Rules engine detection has issued an alert on something of concern but is unable to pinpoint actual issue.
- Trigger Point 2: Indicators of Concern (IOCs) have been spotted during OSINT monitoring.
- Trigger Point 3: Testing hypotheses using exploratory investigations is started by an investigator who is concerned that frauds in other organizations may exist in their organization, yet undetected.

When an investigation is initiated via trigger point 1, the analyst should enter all known alert data and information into a case

management system to be assigned to an investigator.

In the case of trigger point 2, the OSINT monitoring team should enter all known alert data and information into a case management system to be assigned to an investigator.

With trigger point 3, if an investigator finds unusual activity during a hypotheses testing, they should open up, self-assign a case.

Examples of common trigger points:

- Money laundering: significant funds are being deposited (a.k.a. placement)
- Insurance fraud: Claimant has connections to other claims or claimants
- Bribery and corruption business process models are being abused or OSINT discussions are taking place
- Sanction list: Connections between customers and sanction list appear
- Tax evaders: Inconsistences in financial transactions are detected
- Credit card fraud: Abnormal behavior in transactions or OSINT card selling is taking place
- Insider fraud: Suspicious activities have been noticed around an employee or partner
- Retail and online trading accounts: Transactional behavior not normal to standard activities begins
- Embezzlement: Unusual transactions are being detected
- Gaming & betting fraud: Unusual transactions have been detected by new accounts with basic setup information
- Money transfer and payment frauds: some accounts have suspicious connections or transactions to many other accounts.

Regardless of the trigger points, once an investigation is assigned, speed to actionable intelligence is of critical importance.

Where to start in setting up a Fraud and Financial crimes investigation solution?

Begin with the end in mind, ask oneself, what is the end result we want to achieve? This is usually the need to find the network of illicit activities and find the who and how of the incident. The following model helps to define:

WHO: Who needs this information?
Once an investigation has been concluded the details are sent to an intervention team who then could work with others such as: HR if an insider, Money Laundering Reporting Officer, law enforcement and/or SIU/FIU teams to help implement policy.

WHAT: What is needed by an intervention team or other supporting teams?
A chart to understand who and what is connected to the illicit activities with evidence genealogy.

*W*HY: Why is a deeper investigation needed?
Fraudulent activities are rarely the work of a single individual and finding the complete network is key to its full removal.

Mapping out gaps between current processes and procedures to combat fraud and financial crimes (e.g. rules engine effectiveness, threat reports value, current investigation methods, workflow / case management, usefulness of actionable intelligence generated) and the "to-be" environment (e.g. handoff between rules and investigations, extraction of relevant threat report data, use of OSINT, cross-organization reporting, etc.) can help an organization prepare to implement a fraud investigation solution.

Defining the boundaries for an IBM i2 investigation solution

Selecting the IBM i2 solution that is right for your organization is based on 3 main drivers:

- Number of users and how they interact
- Scale and scope of data
- Advanced feature/function requirements

Users:
Defining type and quantity of users will set the size of the project. Users can be classified as:

Committed users: The analysts / investigators, their primary role being to investigate assigned cases. They will have a strong

working knowledge of the features and functions of the IBM i2 solution. Having a background in investigations from previous roles in law enforcement or intelligence communities is a distinct advantage.

Casual Users: Are users who receive link charts from the Committed Users for the inclusion in their cases, and may use basic IBM i2 search and discovery capabilities.

Consumers: Are the final users of the output of the investigations such as HR, MRCO, intervention teams, etc. Output of the investigations may be supplied via link charts or screen captures.

Controllers: Are tasked with ensuring cases are assigned to the correct users via the case management tools. They also ensure workloads are balanced and are completed in recommended times.

Collectors: These individuals are responsible for setting up all the data sources that are needed by the investigators in their investigations. They need to build and configure the ETLs (Extract, Transform, Load) and data models. They will have a very good understanding of the IBM i2 solution from an underlying systems and data perspective.

Direct users of the IBM i2 solution include committed users, casual users and collectors.

Data:
The size and type of data will define the size and design of the investigation solution. Data can be captured in multiple ways depending on type of solution:

1) Enterprise solution: ETL data into an enterprise repository, flexible ad-hoc import of data and simple connector query of data (data remains in place)
2) Workgroup solution: import data from variety of sources (e.g. spreadsheet, text file, XML file, other database) into a shared workgroup repository
3) Individual: input data onto the chart and optional individual repository, load small flat files and simple connector query of data.

Features and Functions of i2

An IBM i2 solution for the investigation of fraud and financial crimes offers:

Flexible data ingestion
Ingest structured and unstructured data including dark web and open-source intelligence (OSINT) data, including a simple connector approach to query data

Advanced analytics and entity resolution
Quickly identify threats, threat actors and hidden connections using multi-dimensional visual analysis and advanced analytics, and contextual entity resolution with alerting

Speed and scale
Analyze large, disparate silos of data with unprecedented speed to gain actionable intelligence

Use by analysts and more casual users
Leverage thin client search and discovery capability to enable non-analyst users, such as investigators, to quickly and simply access critical data to carry out target investigations.

Depending on the specific requirements, the IBM i2 solution portfolio can support many different use case requirements. These can be set up as a standalone system or be embedded into a broader enterprise solution.

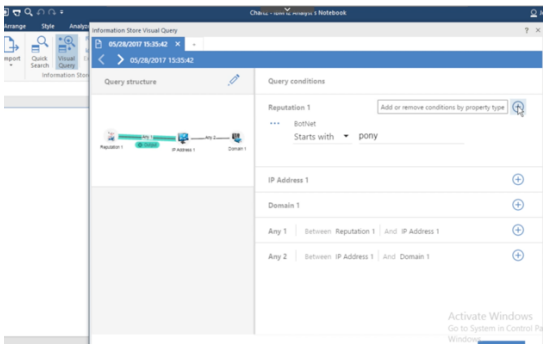
Such a broader enterprise solution is commonly connected to other existing supporting products and processes, including:

1) Case management
2) Detection rules engines for alerting
3) Storage drives for reports
4) Data and OSINT connectors
5) Executive dashboards

IBM i2 software comes with a rich set of easy to use features and functions. The following are the commonly used capabilities in the fraud and financial crimes investigation space:

Visual Query
Visual query allows a user to create a visual shape of the question. Single entities through to complex networks containing indirect

relationships can be defined without the need to learn a complex query language. Properties can be assigned to entity and link types to hone results. Query definitions can be saved for re-use and shared across the operation.

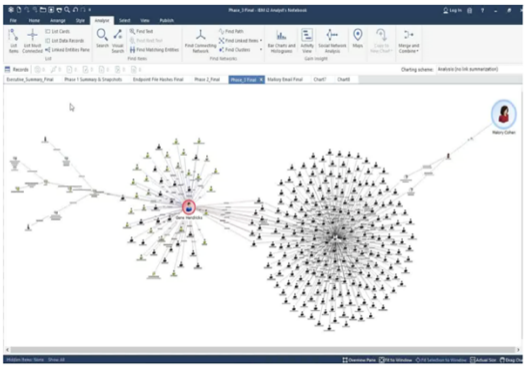


Visual Query view

A simple question can be asked. For example, what is known about the claimant, their connection to others, their connection to other claims and any listing on a watchlist? This visual query, will return a link chart. It is easy re-query with additional conditions such as time or location constraints.

Expand, Filtered Expand

When a repository item is charted, a user may wish to uncover further information that is known about the item from their repository. By expanding the item, any associated items in the repository will be charted, providing more context on the item and enabling further analysis. Filtered expand provides a way to chart further information, and allows the user to determine the extent of the expansion by limiting the types of information and setting the charting scheme they wish to use. This will minimize any noise and clutter on chart.



Filtered Expand view

Filter expand allows the fraud investigator to look for any illicit patterns in the data from a visual point of view. This could allow user to start with a group of individuals and then pivot onto their bank account transactions.

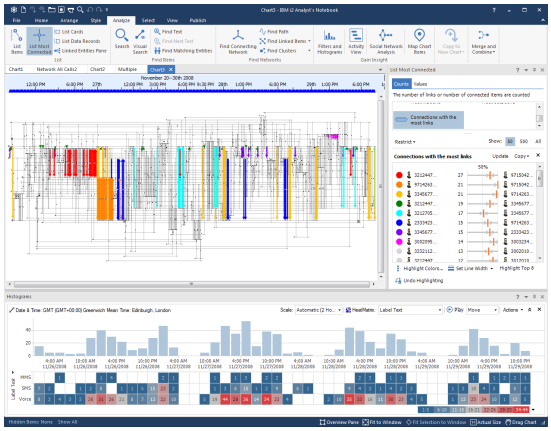
Timeline Analysis Charting

Temporal views can be used to illustrate how sequences of events unfold over time. It can reveal the interactions between entities and portray when these interactions occur. Timeline charts are commonly used to analyze information such as telephone call records (and other forms of communications) or financial transactions. They also enable users to build a picture of a sequence of events for time periods of interest. These charts provide a powerful visualization that help to simplify the analysis and briefing of key temporal information. They make it easy to follow a money trail across many accounts.

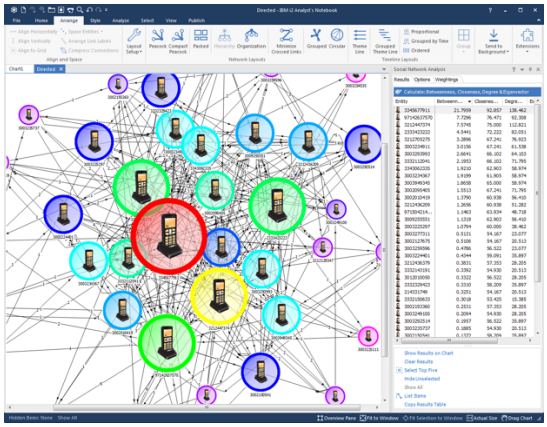
Timeline Analysis view

Heat Matrix View

The Heat Matrix takes the temporal analysis a step further. It offers a more detailed breakdown of the temporal content of data, allowing users to map / visualize activities against two temporal ranges. This capability helps to provide a much quicker answer to temporal questions. Users can quickly identify patterns in activity or aspects of a target's likely pattern. It also helps identify how and when a target individual works and whether there are any regular patterns in terms of their common activities.



Heat Matrix view

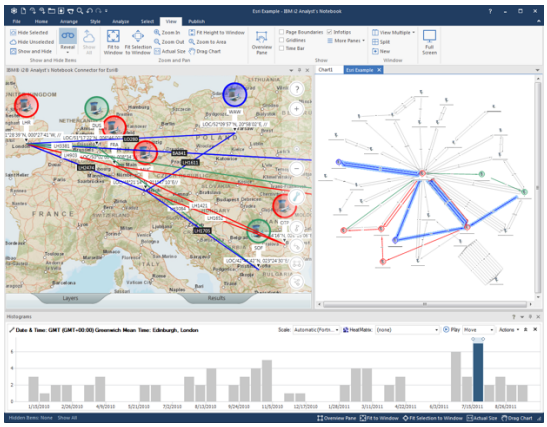


Social Network Analysis view

Name Disambiguation
A 24x7 automated identity resolution and recommendation engine alerts analysts when new information is available and when data points have been altered, strengthened or resolved. It will match on all available attributes, including historial attributes. It enables users to quickly determine when multiple identities are the same. Proactive alerts call out when matches arise among otherwise seemingly hidden connections, helping to highlight non-obvious relations.

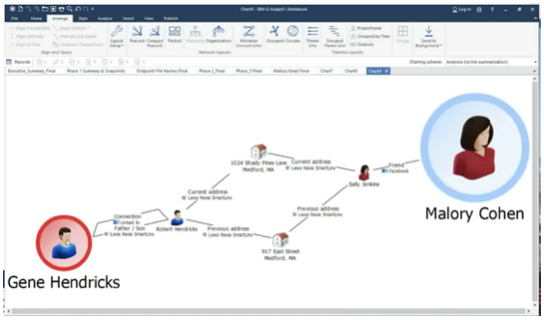
Social Network Analysis
With this capability, it is possible to examine group structures and communication flows within a network chart by focusing on the relationships that exist between entities. Organizational theories are combined with mathematical models to help you understand the dynamics of groups and organizations in which the user has an interest. The IBM i2 solution enables users to better understand relationships between customer data sets, unstructured data sets and OSINT data sets.

Geospatial Analysis
IBM i2 solutions offer an integrated environment for link, temporal and geospatial analysis in a single work environment to build a detailed and robust analysis picture more quickly, improving the timely delivery of rich, actionable intelligence. If a chart entity's attribute has associated GIS data or a tag that can be converted to GIS data (i.e. an address) using commercially available maps, an entity can then be easily be displayed on that map. Geo special boundaries can also be used as part of a query or filter function.



Geospatial Analysis view

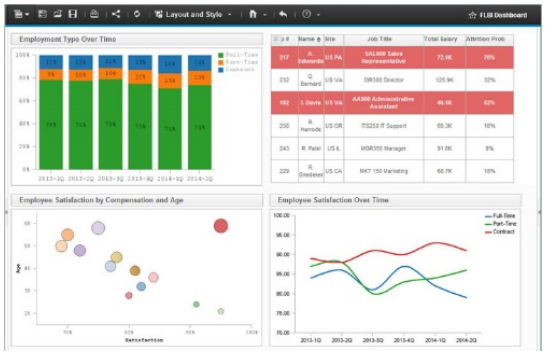
Find Path
Identifying hidden connection paths between items that appear to be directly connected is key in determining potential relationships between parties. The Find Path function helps to identify paths from one item to another, based on user specified criteria. It helps answer the questions of "Is Item A connected to Item B and how are they connected?". Users are able to set rules about which items are allowed on the path (both entities and links). These rules allow users to exclude particular relationships or communication types as being valid connection paths.



Find Path view

Conditional Formatting
For conditional formatting, users can define a set of rules to automate the process of formatting chart data to emphasize significant information for analysis or presentation purposes. Saved rules can automate repetitive tasks that are required across many charts. Multiple rules can be set up to perform complex formatting tasks. These rules can be configured to work against the properties contained within chart entities, links, and attributes. Since conditional formatting specifications can be saved, organizations are provided with an effective method of standardizing analysis and briefing tasks across wider teams.

Executive Dashboard
An organization can use business intelligence functionality to write custom analytics over their data. You can use these views to understand the immediate and downstream effects of decisions that span potentially complex interrelated factors. Consistent snapshots of business performance are provided in enterprise-class reports and independently assembled dashboards based on trusted information. Thus, non-technical and technical business intelligence users and IT alike can respond quickly to rapidly changing business needs.



Executive Dashboard view

Building out a full solution

Protecting an organization from fraud and financial crimes should be fully integrated into the end-to-end master business process of an organization. As fraudsters will look for any vulnerabilities / gaps to exploit. With integrated and layered defenses (a.k.a. "Defense in Depth") an organization can significantly reduce these gaps.

Layer Defenses
Tiers 1 and 2 (transactional and correlational detection) are rules-based layers that run in real time against transactional systems. They will identify any events that do not conform to the known rules. They can also be used to set off a trigger point to start an investigation in tier 3.

Tier 3 is used for deep investigations based on triggers that have detected an anomaly but not the full event. Examples of this could be the opening of many new bank accounts, which by itself is not an event that needs investigation, but may be a coordinated "placement" step for a possible money laundering operation in the future. A request to investigate and look for collusion could be the next course of action.

There are many use cases that benefit from using an IBM i2 solution to fight fraud and financial crimes. The following section highlight some examples:

Anti-Money Laundering Investigations using an IBM i2 solution

Compelling reason to act
Organizations may unwillingly allow money to be laundered via their platforms, yet can be liable for significant fines imposed from financial regulators who deem unsatisfactorily the organization's ability to stop these illicit activities.

The shortcomings of the current approach for anti-money laundering detection
Many organizations currently rely heavily and sometimes exclusively on rules engines. These automatic inline, real time detection rules engines, while critical for the defense against fraud and financial crimes, are not the ultimate solution.

Concepts of intelligence operations: the new approach incorporating i2
As money enters a financial system (placement), it is mixed with other clean funds (layering) and then re-surfaces as normal

business funds (integration), yet a digital footprint always remains. The IBM i2 solution with the combination of machine-led analytics and human-led analysis can easily link activities, individuals and entities across multi-degrees of data separation, no matter how sophisticated the deception or concealment.

Sanction Violation Investigations using an IBM i2 solution

Compelling reason to act
Sanction regulations are put in place to protect international trade and commerce from organizations or nations who are willing to use illegal practices in their operations. Such practices include human trafficking, counterfeiting, embargoed goods, human rights violations, terrorism. Organizations who unknowingly break sanction rules can still receive significant fines from international regulators. To ensure this does not happen, it is key to know your customers, know you partners and know who might be connected to who to ensure sanction violations do not happen.

The shortcomings of the current approach for sanction violation detection
Global organized crime rings (OCRs) and terrorist organizations will attempt to place as many layers or intermediators, so as to circumvent sanction detection systems. Trying to understand connections across multi-channel transactions with different individuals, can take a long time to determine, sometimes longer then the life cycle of the illegal transactions. This delay can allow the relevant parties to slip away and never be identified.

Concepts of intelligence operations: the new approach incorporating i2
As many layers or intermediators enter the transaction process, all-source data is required to understand the connections. This data can be a combination of sanction lists, social media, news reports, international watch lists, company's registration information, etc. An IBM i2 solution can quickly and seamlessly combine this data to discover inappropriate individuals or entities in the mix. It can occur even before a transaction has taken place, ensuring a financial institution can withdraw services and remain in compliance with international sanction regulations.

Anti-Bribery and Corruption Investigations using an IBM i2 solution

Compelling reason to act
Unfortunately, everybody has a price and even the most legitimate and trustworthy individuals can sometimes fall victim to bribery and corruption. This could be because of financial pressure or being discovered in a compromised position. Also, certain individuals can be targeted, such as politically exposed persons who have been entrusted with a prominent public function. Regardless of their motivation, if these individuals are not discovered, significant revenue loss, reputation loss or regulatory fines can be the ultimate effect on an organization.

The shortcomings of the current approach for anti-bribery and corruption detection
Individuals who usually fall victim to bribery and corruption have a good working knowledge of the system and can be experts in covering their tracks. As the root of the bribery and corruption may come from outside the system, it can be very difficult to find a direct or indirect link that associates the bribed and the briber. These non-obvious connections can also have a weak signal, thus are difficult to detect .

Concepts of intelligence operations: the new approach incorporating i2
The trigger point for anti-bribery and corruption is not always obvious and may need human observations and alerting. This could be seen as an individual's change in direction on policy, increase in their disposable income or work pattern modifications. Once seen (typically by user behavioral analytics/UBA), an investigation into the individual's digital footprint and connected network can be started. The combination of electronic communications (email, call data records/CDR, social media posts) with transactional data (funds movement, approval processes, data access

permission) and social network analytics (who, when, where, how, why) allows an investigator to build up a pattern of life using the IBM i2 solution.

Auto Insurance Fraud Investigations using an IBM i2 solution

Compelling reason to act
The domestic insurance industry's move of its customer interactions such as policy applications and claim processing online has drastically increased the efficiency of their business, yet allowed fraudsters additional opportunities to commit insurance fraud. Individuals can open many policies using different identities or falsify claim reports from the comfort of their keyboards. With large illicit financial opportunities, fraudsters can continue to evolve the sophistication of their insurance frauds.

The shortcomings of the current approach for insurance fraud detection
Insurance fraud detection systems are based on rules engines that try to connect illicit activities with known trigger conditions, such as: individual is on an insurance watchlist, insurance claim is not covered by the policy, individual has a known connection with the other person involved in the accident or organized crime gangs are working as a team in staging accidents such as "crash for cash". The most sophisticated frauds will conceal their real intent as they attempt to make all circumstances connected to the claim as legitimate as possible. Rules engines will struggle to detect the non-obvious patterns.

Concepts of intelligence operations: the new approach incorporating i2
To surface illicit auto insurance claims, the investigator must open up the viewing aperture of the case. This is achieved by starting with the claim or claimant in question and identifying what link attributes connect them to any other claim or claim pattern. This can include attributes such as: policy type (size, age, conditions), vehicle type (size, age, conditions, passengers), victims and accused connection, who knows who (age, location, history with other claims, social media). Using an IBM i2 solution, an investigator can visualize the "find path" across these networks to surface these illicit linkages.

Conclusions

IBM i2 provides a sophisticated, yet easy-to-use environment that enables fraud and financial crime investigators to search large, complex and dynamic data sets. Analysts and investigators can quickly uncover information buried in large volumes of data with the help of automated and assisted analytics. Freed from the requirement to use complicated query languages and the need to constantly monitor incoming data, these users can concentrate on collaboratively creating and sharing valuable intelligence outcomes.

An IBM i2 solution enables fraud and financial crime investigators to provide rapid, in-depth analyses of large data volumes, while enabling their organizations to make smarter and timelier decisions. The intuitive search and discovery capabilities open up the tool to a wider range of users.

Overall, the scalability, modularity and interoperability of IBM i2 solutions enables organizations to deploy features and functionality to meet the needs of multiple operating environments, missions and users.

For more information

To learn more about IBM i2 solutions for fighting sophisticated fraud and financial crime threats, visit www.ibm.com/security/intelligence-analysis/i2