

## Smarter Cities Series: Understanding Fraud Investigation



**Redguides**  
for Business Leaders

James Luke  
Tim Cooper  
Rob Tucker

- Increase fraud investigation effectiveness for better results and reduced costs
- Improve client relationships by demonstrating a proactive stance against fraud
- Strengthen resistance to fraud by understanding system and process weakness





## Executive overview

Fraud and financial crime is a significant, persistent, and evolving challenge to the public and private sector. It costs an estimated five to eight percent of revenues per annum<sup>1</sup> and, overall, is measured in trillions of dollars.

In addition to the direct financial impact, there is also a real risk of long-term damage to reputation, client confidence, and violation of regulations, leading to fines and an impact on shareholder value in the private sector, and loss of confidence in public bodies.

Public awareness and nonacceptance of the costs of fraud and financial crime are also increasing. Clients expect to interact over many online and offline channels. The inevitable increase in the volume, variety, and velocity of data multiplies the risk of a successful attack. Criminals are becoming increasingly adept and knowledgeable at probing for and exploiting any system or process weakness. The complexity and fragmented nature of these interactions effectively hides the evidence. To see the complete picture, these disparate data sources must be combined.

Organizations who adopt a proactive response to fraud have a real competitive advantage with a tangible deterrent effect. Demonstrating and evidencing suspicious activity also provides a powerful challenge capability to prevent fraud. In certain circumstances, this evidence is passed to law enforcement for criminal prosecution. Fully uncovering how the fraud was perpetrated also enables system and process controls to be tightened to avoid repeated loss.

Traditionally, companies counter attacks with point or line of business solutions. This approach is difficult to manage, often missing complex cross-channel attacks by organized criminals. This approach also results in a more expensive, fragmented, and difficult to manage solution.

IBM® i2® Fraud Intelligence Analysis provides an integrated solution for fraud investigation and discovery. The solution enables the rapid documentation of fraud and financial crime and provides actionable intelligence for repudiation, remediation, and prosecution.

---

<sup>1</sup> Association of Certified Fraud Examiners, 2012 Report to the Nations:  
<http://www.acfe.com/rtn-highlights.aspx>

Key capabilities of the Fraud Intelligence Analysis solution include the following items:

- ▶ Powerful visual analytics for appraising and understanding of information to uncover fraudulent activities, networks, and targets.
- ▶ Built-in investigation management and coordination tools, keeping investigation work on track and recording key findings and decisions.
- ▶ Data acquisition capabilities to connect the investigation team to the right information quickly and effectively.
- ▶ Reporting and dashboards to show progress and effectiveness of investigations.
- ▶ Collaborative tools, supporting information sharing and communication, joining the dots between previously siloed investigation activities.

This IBM Redguide™ publication describes the Fraud Intelligence Analysis capabilities and offerings. This guide also explores how Fraud Intelligence Analysis can be used as part of a broader fraud and financial crime solution.

## Fraud and financial crime in different industries

The variety and evolution of fraud demands that an effective solution must be flexible enough to deal with continually evolving and ever changing attacks.

Table 1 lists some common examples of fraud and financial crime by industry.

*Table 1 Fraud examples by industry*

| Industry   | Type of fraud  |
|------------|--|
| Banking    | <ul style="list-style-type: none"> <li>▶ Card</li> <li>▶ ATM skimming</li> <li>▶ Check</li> <li>▶ ACH/Wire</li> <li>▶ Mortgage/loan</li> <li>▶ Accounting</li> <li>▶ Rogue/insider trading</li> </ul>                  |
| Insurance  | <ul style="list-style-type: none"> <li>▶ Staged accidents</li> <li>▶ Cash for crash</li> <li>▶ Slip and fall</li> <li>▶ Arson</li> <li>▶ Medical fraud</li> <li>▶ Property fraud</li> </ul>                            |
| Healthcare | <ul style="list-style-type: none"> <li>▶ Duplicate claims/services not rendered</li> <li>▶ Unnecessary services</li> <li>▶ Kickbacks</li> <li>▶ Unbundling of services</li> <li>▶ Upcoding (services/items)</li> </ul> |
| Retail     | <ul style="list-style-type: none"> <li>▶ Refund/returns</li> <li>▶ Discount</li> <li>▶ Vendor or supply chain theft</li> <li>▶ Sweethearting</li> <li>▶ Cash register tampering</li> </ul>                             |

| Industry                             | Type of fraud  |
|--------------------------------------|--|
| Telecommunications                   | <ul style="list-style-type: none"> <li>▶ Subscription</li> <li>▶ PBX hacking</li> <li>▶ International revenue share</li> <li>▶ Box breaking</li> <li>▶ Premium rate</li> </ul> |
| Central government                   | <ul style="list-style-type: none"> <li>▶ Procurement</li> <li>▶ Grant</li> <li>▶ Payroll</li> <li>▶ Tax</li> </ul>   |
| Local government and social services | <ul style="list-style-type: none"> <li>▶ Housing</li> <li>▶ Benefits</li> <li>▶ Procurement</li> <li>▶ Payroll</li> <li>▶ Tax</li> </ul>                                       |

## The evolution and industrialization of fraud and financial crime

At a summary level, fraud and financial crime can be split into two types of crimes:

- ▶ **Opportunistic**  
Usually individuals that operate in an unplanned way and exaggerating or leveraging a genuine claim or transaction.
- ▶ **Organized or complex**  
Groups working collusively, possibly with insider insight, targeting significant financial returns. Likely to be also involved in other criminal activity.

Generally, opportunistic acts are dealt with early in the client interaction. Complex schemes, however, require information from many disparate data sources to be combined, usually against tight time constraints, to support the investigation and remediation processes.

Although fraud intelligence analysis is frequently used to investigate high value opportunistic events, the more prevalent use cases for the solution are complex and organized in their nature.

Organized crime covers a wide spectrum. Gangs might be organized locally or regionally, relying on physical meetings, phone calls, or email to organize and perpetrate the attack. Alternatively, virtual gangs might be formed, trained, and equipped online, looking to perpetrate large-scale attacks that target direct financial gain through extortion. It is vital that an investigation solution has the flexibility to completely investigate and uncover all variations. A robust defense against this complexity of attack requires an holistic solution, of which Fraud Intelligence Analysis is a key component.

### Typical models are fragmented

Many organizations, particularly in the financial services sector, have multiple analytics systems in their respective lines of business, each reviewing transactions and identifying risk independently. Although these systems support the specific objectives of their particular business unit, it is advantageous to look across these systems, which helps to identify and prevent cross-channel threats.

Figure 1 shows an example of siloed operations within a banking environment.

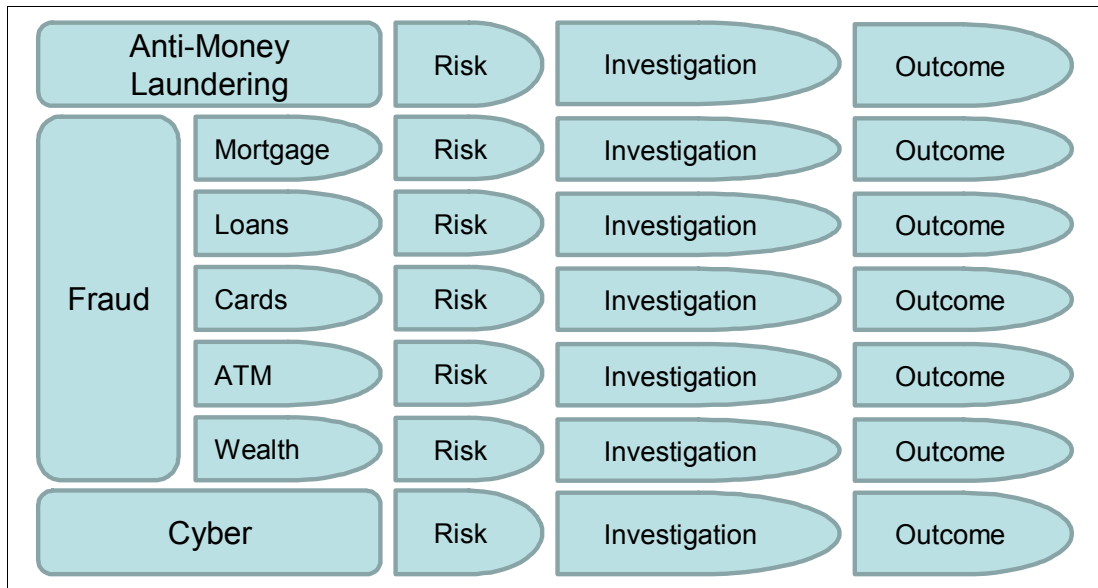


Figure 1 Siloed and potentially inefficient operations in a banking environment

## Fusing the data and process silos

To address the weakness that is inherent in a fragmented solution, a new type of fraud solution is required. This solution must take an holistic view of the enterprise so that data can be fused across the silos. The requirement to join the individual analytical and investigative silos is great. This might be a direct result of the increasing pressure from regulators, or driven internally through more visionary projects. In either case, the ability to investigate anomalous behavior across operating units and geographies provides real operational and competitive advantage.

Figure 2 shows an example of using a combined view to investigate a cross channel attack.

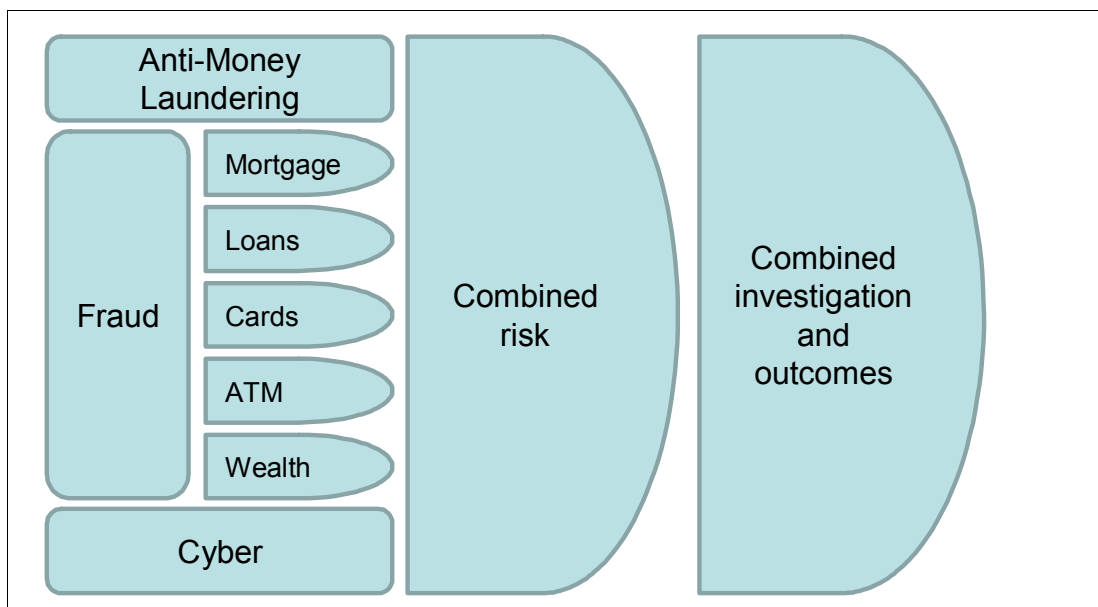


Figure 2 Using a combined view to investigate a cross channel attack

## Enterprise fraud management

Figure 3 shows that supporting the full lifecycle of fraud requires a holistic approach, provided as a set of the following modular but inter-dependent components:

► **Detect**

The detect component is used to continuously compare client, account, or transaction data to the data of cases that are known to be fraudulent. Suspicious transactions can be identified before a payment is made. Conversely, and importantly, valid transactions are identified and processed quickly, and with greater certainty.

► **Prevent**

The prevent component stops unwanted activities from taking place by making it clear to potential perpetrators that there is demonstrable suspicion of fraud, and that the risks that are associated with the transaction are high. The prevent component uses intelligence that is gathered by the discover and investigate components.

► **Discover**

The discover component is the process of identifying fraud patterns through the usage of a rich set of analytic capabilities. This information can then be encoded as business rules, predictive models, anomaly detection models, and entity analysis models that are ready for deployment into operational systems for real-time, near real-time, or batch processing fraud detection. The investigation team uses this intelligence to prioritize their activities.

► **Investigate**

The investigate component is the process of building cases for prosecution, recovery, or denial of payment. The output of the investigation is a link analysis chart that clearly documents people, places, entities, relationships, communications, and information flows.

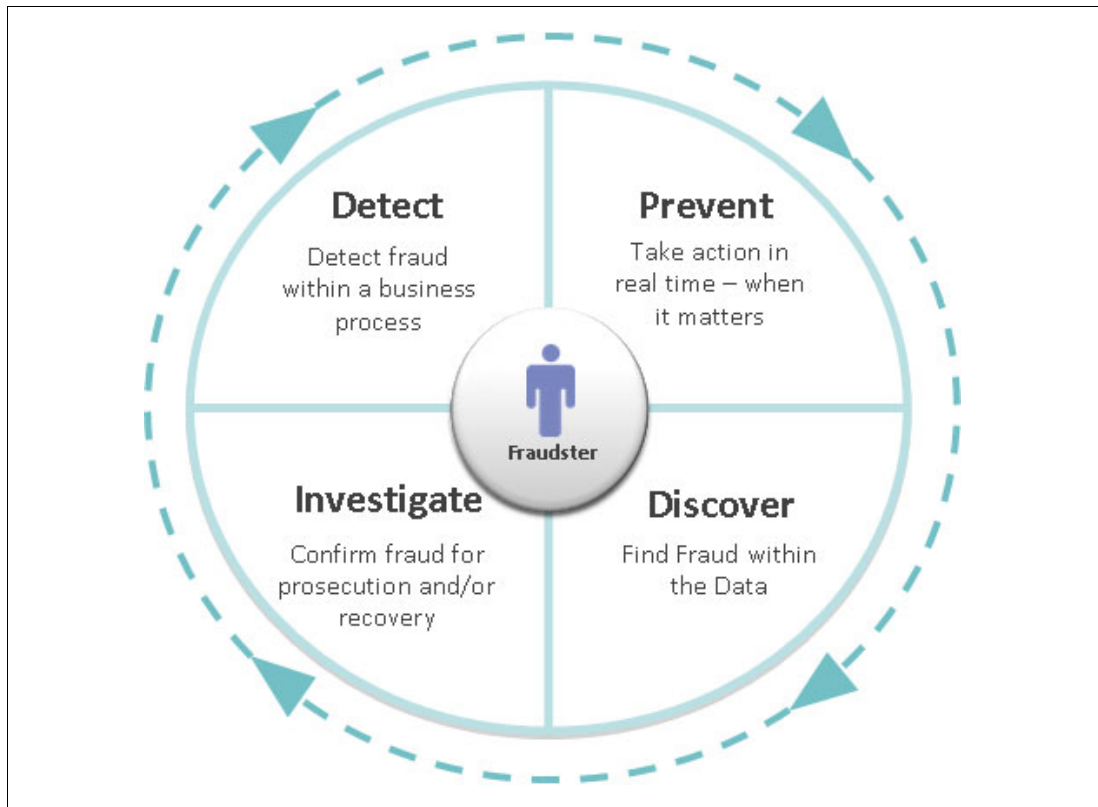


Figure 3 Areas of fraud analysis

## Using analytics

As the industrialization of fraud activities leads to increased complexities, a wide range of analytical approaches are essential to provide a complete solution:

- ▶ Data analytics to connect, extract, and fuse data from different sources into a unified, “analysis ready” form
- ▶ Entity analytics to determine who-is-who and who-knows-who across fragmented data sets
- ▶ Detection analytics to automatically uncover potential fraud
- ▶ Search, query, and alert analytics to get to the right information, quickly and effectively
- ▶ Link (network) analytics to understand and uncover relationships between people, organizations, and events
- ▶ Social network analysis to determine key players in large networks
- ▶ Reporting analytics to get the right information to the right people, in the right format

As shown in Figure 4, Fraud Intelligence Analysis focuses on the investigation and discovery phases of the counter-fraud lifecycle. Fraud Intelligence Analysis also integrates and interacts with detection, prevention, and case management solutions that are often deployed as part of a larger project.

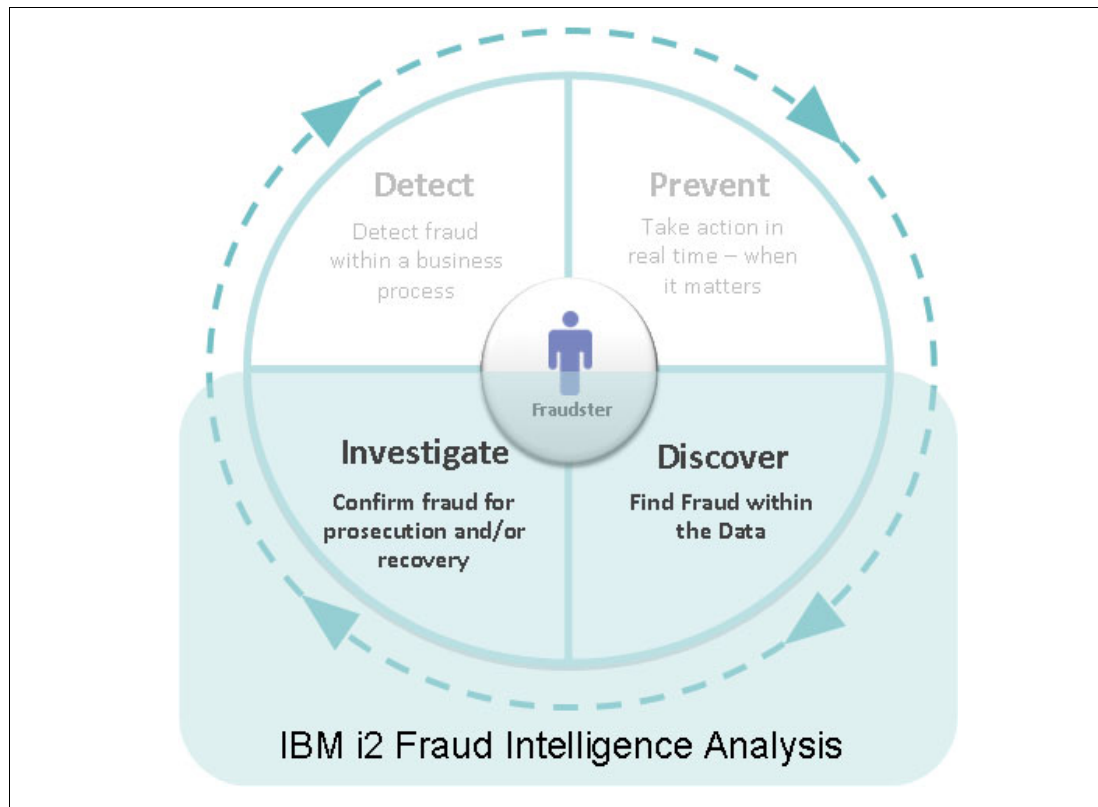


Figure 4 Focus areas of fraud analysis

The investigation process is considered complementary to detection and uncovers and documents the means and method of the fraud. This information is invaluable feedback to tighten system process and policies.



As shown in Figure 5, existing detection analytics and rules are used to define outcomes that improve detection.

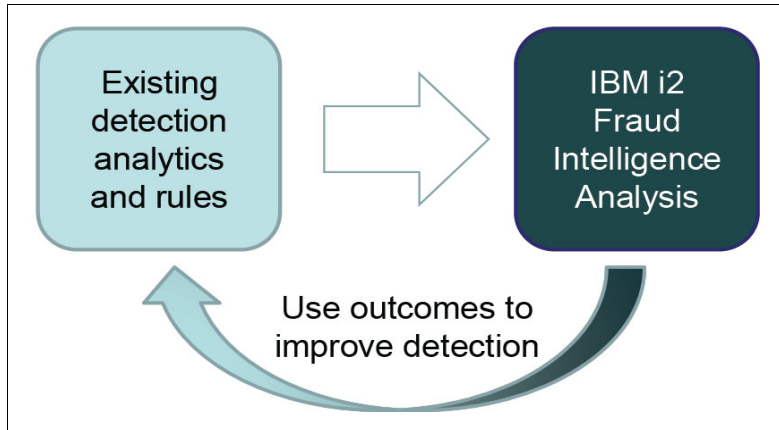


Figure 5 Output from investigation helps to define selection values

The remainder of this guide focuses on the Fraud Intelligence Analysis solution and its capabilities to support and complement a broader counter-fraud management.

## IBM i2 Fraud Intelligence Analysis

IBM i2 Fraud Intelligence Analysis helps to investigate complex incidents, produce actionable visualization of critical people and events, and document results for repudiation and potential litigation.

As shown in Figure 6 on page 8, Fraud Intelligence Analysis provides distributed investigative, collaborative, analysis, and visualization capabilities to represent fraud networks.

Fraud Intelligence Analysis provides significant value as a stand-alone solution. It can also be readily integrated into additional existing or planned investments to address a broader need. Industry-dependent key attractors are used to create rules and models that highlight higher risk transaction, and identify anomalies. Detection can be done in real time or in batch, depending on the industry and transaction type.

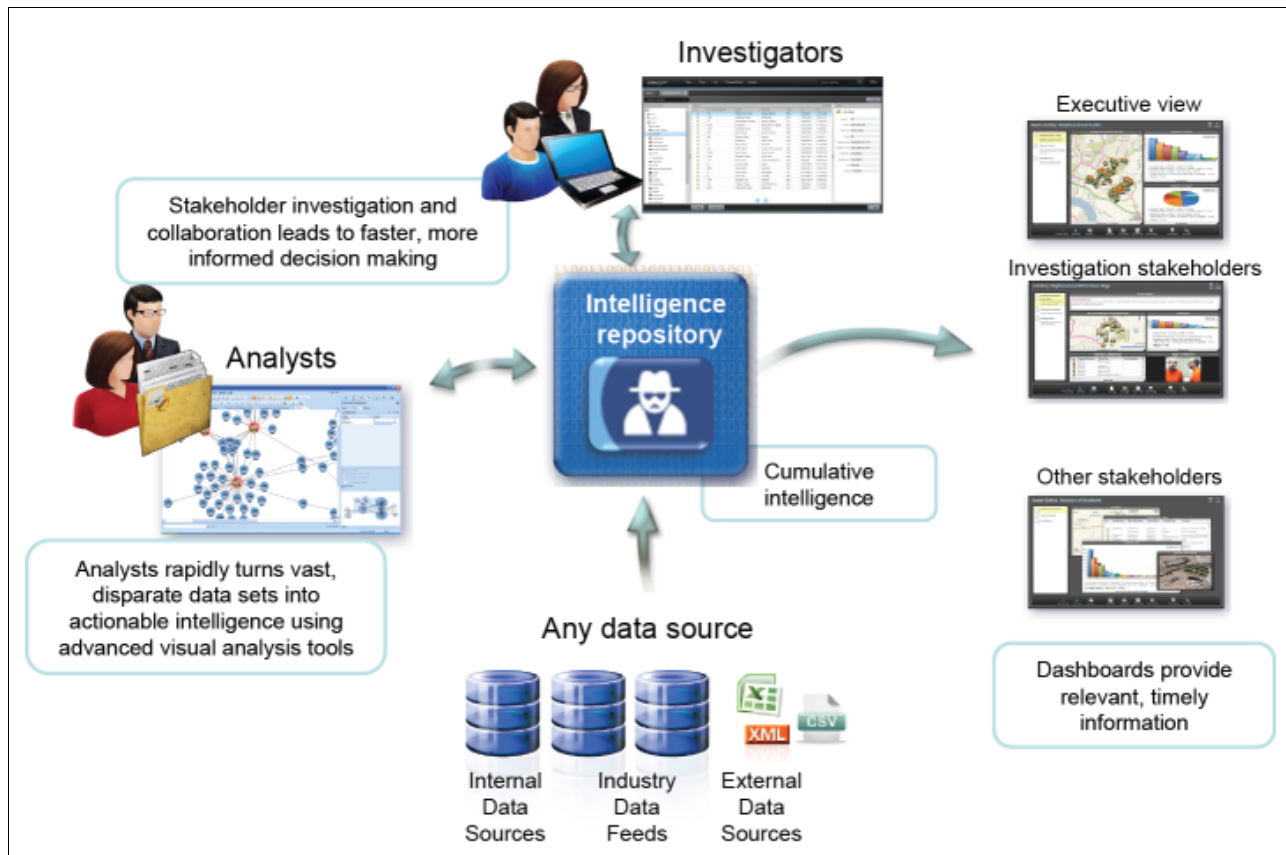


Figure 6 Fraud Intelligence Analysis

## Connecting to the data

Data is the lifeblood of an investigation. It is vital to connect the team to the data in as expedient a manner as possible. This approach enables them to focus on the task of uncovering and documenting suspicious activity. Fraud Intelligence Analysis connects directly to the required data in various ways to enable the inclusion of structured and unstructured data sources:

- ▶ Data on demand through the Intelligence Analysis Platform (both external and internal) data sources can be connected directly to the investigation process. Data sources can be individually searched, filtered, and expanded by analysts and investigators and data relevant to the investigation is saved to add to the cumulative intelligence.
- ▶ Data on demand through a federated search: Data sources can be grouped and searched selectively and simultaneously through a single search. This approach further increases the efficiency of the investigation process. Search results are ranked and further pre-analysis maximizes valuable analyst time.
- ▶ Data loading (extract, transform, and load) or “in advance” loading of data sets, which are ready for analysis.
- ▶ Ad hoc file import is used when occasional or infrequently accessed data can be easily included in the investigation through a flexible and intuitive importer. Data formats can be *one-of-a-kind* or parsed through a previously prepared import specification (which is created by the analyst) if more regular imports are anticipated.

## Working with external data

Investigation almost inevitably requires the inclusion of external data. The type and sources of data are too numerous to list but include the following data:

- ▶ Watchlist, sanctions, and Politically Exposed Persons (PEP)
- ▶ Public records data
- ▶ Credit risk and identities
- ▶ Vehicle and licensing information
- ▶ Industry provided databases, such as the Insurance Fraud Investigators Group (IFIG), National Insurance Crime Bureau (NICB), and Insurance Fraud Bureau (IFB)
- ▶ Open source intelligence (OSINT)
- ▶ Social media, such as Facebook and Twitter

Flexible data ingestion models ensure that data is readily connected to the investigation process, ensuring that the investigation team has immediate access to the information that they need.

Using IBM products, Fraud Intelligence Analysis can also be extended to deal with other data challenges:

- ▶ IBM Identity Insight provides entity resolution and non-obvious relationship generation across data.
- ▶ IBM Content Analytics extracts key information from high volumes of unstructured data, such as documents and web pages.

## Turning data into intelligence

The ultimate outcome and objective of the investigation is to document suspicious activity for repudiation and prosecution. The solution enables the investigation unit to rapidly turn seemingly overwhelming data into actionable insight.

Here are some key stakeholders:

- ▶ Analysts
- ▶ Investigators
- ▶ Head of Investigation

### Analysts

The analysts perform deep, analytical investigation to collate, analyze, and visualize information, reducing the time that is required to discover key information in complex data.

There are three types of analysts that are interested in fraud analysis:

- ▶ Standard analyst

The standard analyst supports the departmental research, analysis, and presentation of information. The standard analyst defines and executes an analytical strategy for providing reactive investigative data support in all assigned conventional and complex fraudulent claims by using specialized analytical tools, data mining, analysis, and electronic claims file review.

- ▶ Internal fraud analyst

Internal fraud analysts are tasked with identifying fraud that is perpetuated by members of the company's employee base. Internal fraud analysts routinely act on employee tips, exception reports, and irregularities that are found in compliance and sales audits. The internal fraud analyst is responsible for gathering evidence, writing detailed reports, and interviewing employees. Internal fraud departments are often responsible for developing preferred practices and educating employees about fraud awareness.

- ▶ External fraud analyst

An internal fraud analyst is primarily concerned with monitoring a company's own employees, but an external fraud analyst deals with outside fraudsters, many of whom conduct schemes in collusion with current or former employees. External fraud commonly occurs with vendors and subcontractors running various billing or sales schemes against a company. External fraud analysts also investigate instances of pretexting and social engineering that is intended to steal sensitive information. Additionally, external fraud analysts are sometimes involved in examining various forms of cyber crime, including phishing or hacking attempts.

For each of these types of analysts, Fraud Intelligence Analysis offers the following key features:

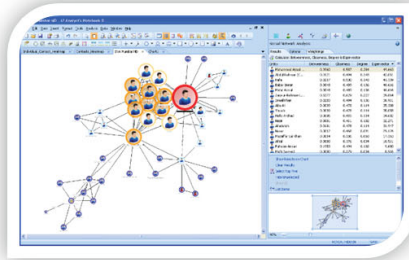
- ▶ Notification of and access to new fraud cases (manual or triggered through detection system).
- ▶ Ability to rapidly acquire, collect, and combine disparate data that pertains to the fraud case.
- ▶ Ability to explore and understand the what, who, where, and when for the fraud case. This is accomplished by using various visual analysis tools to develop an understanding of and derive new intelligence from the fraud case.
- ▶ Ability to act on “what if” hypotheses and make deductions from information.
- ▶ Ability to share and disseminate investigative findings with investigators and the broader stake holder community.

IBM Fraud Intelligence Analysis provides actionable intelligence in several visual formats to support the overall investigation and remediation process:

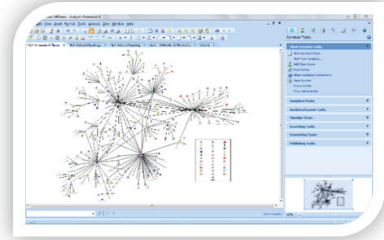
- ▶ Timeline analysis: Quickly shows complex temporal transactions.
- ▶ Association chart analysis: Visualizes the relationships between people, places, and objects.
- ▶ Geospatial mapping: Maps entities (for example, people or vehicles) on to maps.
- ▶ Histograms and heat maps: Highlights spikes and identify regular event patterns.
- ▶ Social network analysis: Quantifies and charts relationships to support the understanding of complex fraud and fraud rings.

Some examples of visual analysis are shown in Figure 7 on page 11. These charts increase the understanding of the structure, hierarchy, and method of operation of criminal, terrorist, and fraudulent networks. They also simplify the communication of complex data to enable timely and accurate operational decision making and escalation to law enforcement.

## Unlock the data with visual analysis

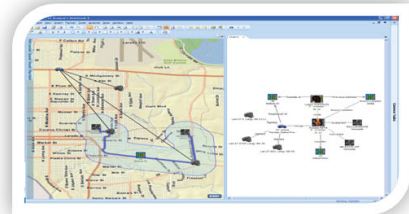


**WHO**  
Identify fraud rings and key players



**WHAT**  
Find complex networks and schemes

**WHERE**  
Identify non-obvious geospatial connections



**WHEN**  
See relationships between transactions

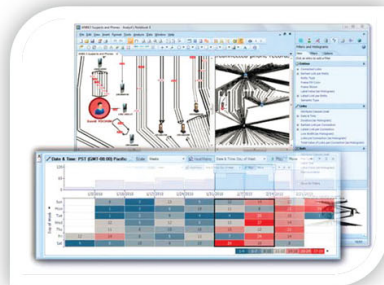


Figure 7 Unlocking the data with visual analysis

### Investigators

Investigators organize, perform, and track the investigation of claim activity that involves policy coverage issues and suspected fraud. Investigators might spend some of their time driving to various locations to collect evidence and perform field investigations and inspections. They also report the status and results of their investigations to adjusters and pertinent third parties on a regular basis according to established deadlines.

The Intelligence portal of Fraud Intelligence Analysis enables investigators to actively and collaboratively participate in the investigation. Users can search and explore case data and related information through a simple interface and view light visualizations.

Investigators can also:

- ▶ Be notified of new fraud cases.
- ▶ Acquire, collect, and combine disparate data that pertains to the investigation.
- ▶ Share and disseminate investigative findings with analysts.

### Head of investigations

The head of investigations manages the special investigation function for the claims department, trains adjusters in fraud awareness, and coordinates with claims personnel and legal on litigated cases.

## The power of collaboration

Complex fraud can touch many operational processes and systems, and the ability to identify collusive activity quickly aids the fight against complex, organized attacks. Fraud Intelligence Analysis enables the investigation team to create and subscribe to informational sets and to receive notifications when intelligence is added or modified. Items within the repository include a full version and change history to enable further consultation if appropriate.

## Building and using cumulative intelligence

Fraud Intelligence Analysis stores information throughout the investigative process. Intelligence can be compartmentalized and access can be provided based on role, investigation, and permissions to support sensitive investigations, for example, an internal fraud. Having a single source of the truth, which is combined with alerting capabilities, enables the investigation team to share intelligence.

Breaking down the investigation silos results in a rich, constantly refreshed source of intelligence that can be used to:

- ▶ Shorten future investigations.
- ▶ Identify collusion and fraud rings.
- ▶ Support the detect and prevent process by surfacing intelligence in business systems and process.

## Measuring progress, success, and outcomes

Fraud Intelligence Analysis includes the ability to create reports and dashboards to support the operational process and demonstrate outcomes to the wider business. These reports and dashboards are used by various stakeholders:

- ▶ Investigators and analysts: List of current investigations, individual performance versus Service Level Agreement (SLA), and team average.
- ▶ Head of investigation: Oversight of team and individual performance, trends by investigation type, investigator / analyst utilization, and investigation performance versus SLA.
- ▶ C-suite/management reporting: Overall oversight, performance, and trends, and financial analysis. Although the objectives vary, the ability to demonstrate a stance against fraud and financial crime is an established theme across the board of many organizations.

Table 2 shows examples of the various management officials that Fraud Intelligence Analysis supports.

Table 2 Officials that are supported by Fraud Intelligence Analysis

| Official  | Activity   |
|---|--|
| Chief Risk Officer  | Risk reduction and improved stance against fraud pushes fraudsters to other insurers or sectors. |
| Chief Financial Officer   | Improved financial ratios, operational, and efficiency improvements.                             |
| Chief Compliance Officer  | Support for compliance objectives, and improved relationship with regulators.                    |
| Chief Security Officer (Investigations)<br>Chief Information Security Officer (Cyber Crime) | Greater understanding of cyber threat and attack vectors.  |
| Head of Fraud   | Improved investigation metrics and increased likelihood that fraudsters move to softer targets.  |

| Official   | Activity   |
|--|--|
| Head of Claims   | Reduced payments to fraudulent claims, and improved bottom line.         |
| Money Laundering Reporting Officer (MLRO)<br>Chief AML Officer | Ensuring entity resolution across business groups to achieve compliance. |

Providing operational, performance, and financial visibility is important not only for the day to day management of the process, but to also raise awareness to the board level and therefore across the enterprise.

Figure 8 shows a summary of Fraud Intelligence Analysis activity. This activity is displayed as reports, plans, and scorecards in dashboards.



Figure 8 Fraud Analysis output reports

## IBM i2 Fraud Intelligence Analysis core components

Fraud Intelligence Analysis is designed to serve three main processes and workflows:

- ▶ Analyst workflow

The analyst workflow acquires, collects, analyzes, shares, and disseminates intelligence for fraud investigations.

- ▶ Investigator workflow

The investigator workflow is a “lighter touch” (field-based) workflow, including intelligence lookup and exploration and intelligence entry from a web portal.

- ▶ Manager and executive workflow

The manager and executive workflow coordinates investigations, monitors progress of investigations, and receives intelligence reports, updates, and trends.

Fraud Intelligence Analysis is designed around three core components:

- ▶ IBM i2 Intelligence Analysis Platform
- ▶ IBM i2 Analyst's Notebook Premium
- ▶ Intelligence Portal

## **IBM i2 Intelligence Analysis Platform**

The IBM i2 Intelligence Analysis Platform is an enterprise class and service-oriented solution. It is designed to provide investigation and analysis capabilities. Here are key characteristics of the Intelligence Analysis Platform:

- ▶ High scalability in terms of numbers of users, data volumes, and analytics performance.
- ▶ Data format and schema flexibility that is based on a powerful and flexible Entity, Link, and Property (ELP) data model. This includes support for structured and unstructured information.
- ▶ Increased reliability with full event audit recording and playback. Also includes the ability to instantiate new analytic services.
- ▶ Improved extensibility and integration by using open standards for service APIs and data, an extensible application framework, and plug-in client functions.



As shown in Figure 9, within the core platform of the Intelligence Analysis Platform, four distinct classes of services exist.

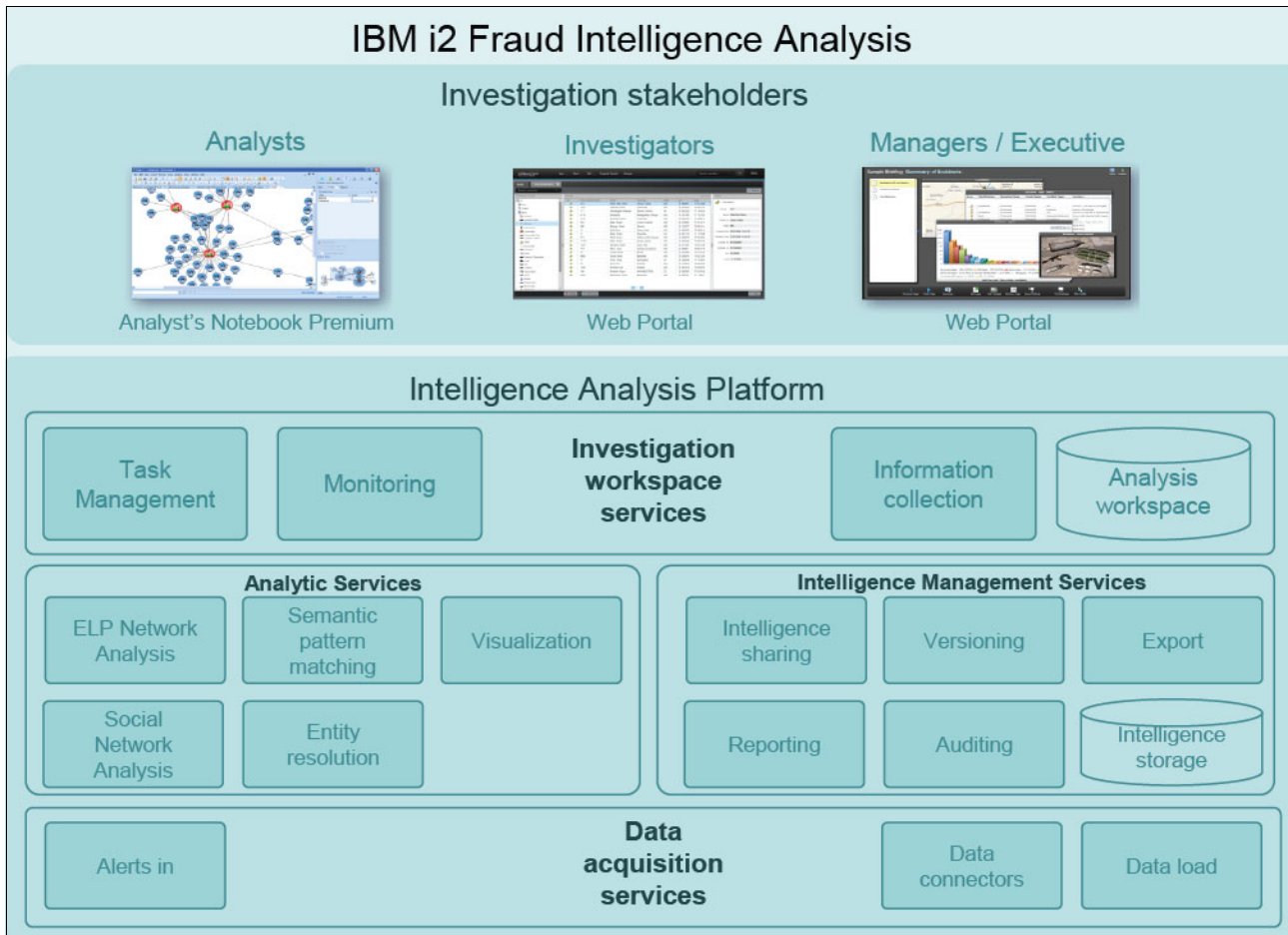


Figure 9 Intelligence Analysis Platform architecture

► Data acquisition services

Data acquisition services get information into the Intelligence Analysis Platform. There are two available approaches:

- Data connection services support on-demand access to data in external sources. The user requests information from the data source as required through search, retrieve, and expand operations. Fraud Intelligence Analysis supports federated access across multiple data sources.
- Data load services support “in advance” ingestion of information into the Intelligence Analysis Platform. Information is pre-populated into the Intelligence Analysis Platform.

► Analytics services

Analytics services augment and assist in exploring, understanding, and analyzing information:

- Entity, Link, and Property (ELP) network analysis services support core information interaction and analysis commands, such as exploring and finding paths through the network.
- Semantic pattern matching services provide rich ELP query matching in information within the Intelligence Analysis Platform.

- Visualization services provide interactive, visual representations of information to aid understanding and analysis.
- Social network analysis services analyze ELP networks to determine “key players” within them.
- Entity resolution services find matching entities and non-obvious relationships in ELP networks.
- ▶ Investigation workspace services
 

Investigation workspace services support the investigator and analyst in performing investigative and analysis activities with Fraud Intelligence Analysis:

  - Task management services support the organization and tracking of activities within Fraud Intelligence Analysis. This can be integrated with a Case Management System for broader operational orchestration.
  - Monitoring services provide investigation key performance and progress indicators.
  - Information collection services provide the means to collect, collate, and analyze information about investigative activities.
- ▶ Intelligence management services
 

Intelligence management services support the following sharing and publication of investigative and analysis activities in Fraud Intelligence Analysis.

  - Intelligence sharing services share, correlate, and reuse intelligence that is gathered through investigation and analysis.
  - Version services provide a full history of updates to shared information.
  - Export services allow intelligence information to be pushed or pulled into other systems.
  - Reporting services provide reports and dashboards to communicate intelligence that is gathered through investigation and analysis.
  - Auditing services record user interaction and data changes within Fraud Intelligence Analysis.

## IBM i2 Analyst’s Notebook Premium

IBM i2 Analyst’s Notebook Premium is a desktop application that provides a rich, interactive visual analysis environment. Analyst’s Notebook Premium connects to the Intelligence Analysis Platform to enhance and extend its capabilities.

Analyst’s Notebook Premium builds on the capabilities of IBM i2 Analyst’s Notebook, providing access to intelligence data. Analyst’s Notebook Premium collects, manages, and organizes information and intelligence. Data in the repository can be viewed and edited without needing to put the content into a chart first. Using the analysis repository, it is easy to uncover relationships, pathways, and networks across data types.

## Intelligence Portal

The Intelligence Portal provides complementary capabilities to Analyst’s Notebook Premium for investigators, managers, and executives. It is driven through a connection to the Intelligence Analysis Platform.

## Performance and scalability

The Fraud Intelligence Analysis solution uses IBM DB2®, IBM WebSphere® Application Server, and IBM WebSphere MQ. This middleware, along with the solution architecture, enables the scaling of the solution both vertically (adding processes within a server) and horizontally (load balancing across servers).

The solution components are extensively tested in high volume scenarios and are deployed in some of the largest financial institutions in the world. High volume capability is possible because of the scaling flexibility and internal architecture of Fraud Intelligence Analysis.

## Availability

The Fraud Intelligence Analysis solution architecture enables the definition of a deployment architecture that eliminates single points of software failure. Solution components can be distributed across a cluster, so that if a member of the cluster fails, other members of the cluster continue to operate.

A fully clustered solution takes advantage of the workload management and balancing provided by WebSphere. WebSphere Application Server achieves high availability through active processing of clustered nodes, while DB2 provides high availability through heartbeat monitoring and automated disk takeover.

All backup and restore schedules are handled through utilities such as IBM Tivoli® Storage Manager. IBM has extensive experience in delivering disaster recovery architectures that are tailored to client requirements. In general, clients tend to adopt a common strategy for disaster recovery across all their operations and the goal is to align with that strategy.

## Security

Information is important, and there might be a business need to classify that information to restrict access on a need-to-know basis. The information in the Intelligence Analysis Platform repository can be classified into four levels:

► Public

Information that is non-sensitive that would not harm the business if it were publicly disclosed. For example, the names of the company directors of a public limited company.

► Internal

Information that is widely accessible by all employees. This information is not for public disclosure. For example, a referral process for handling suspected fraud insurance claims.

► Confidential

Information that is sensitive to the company and should only be accessed on a need-to-know basis. For example, suspected targets of a fraud insurance investigation.

► Restricted

Information that represents the highest value to the company and would damage a business if the information were publicly disclosed. For example, suspected internal fraud carried out by senior employees in the company.

These classifications have an inheritance relationship, which means if an individual has access to information that is confidential, they also have access to information that is classified as internal and public.

# Fraud Intelligence Analysis integration

Fraud Intelligence Analysis can be integrated into an existing client or into a broader IBM counter-fraud management solution. There are a number of integration areas for consideration, as shown in Figure 10.

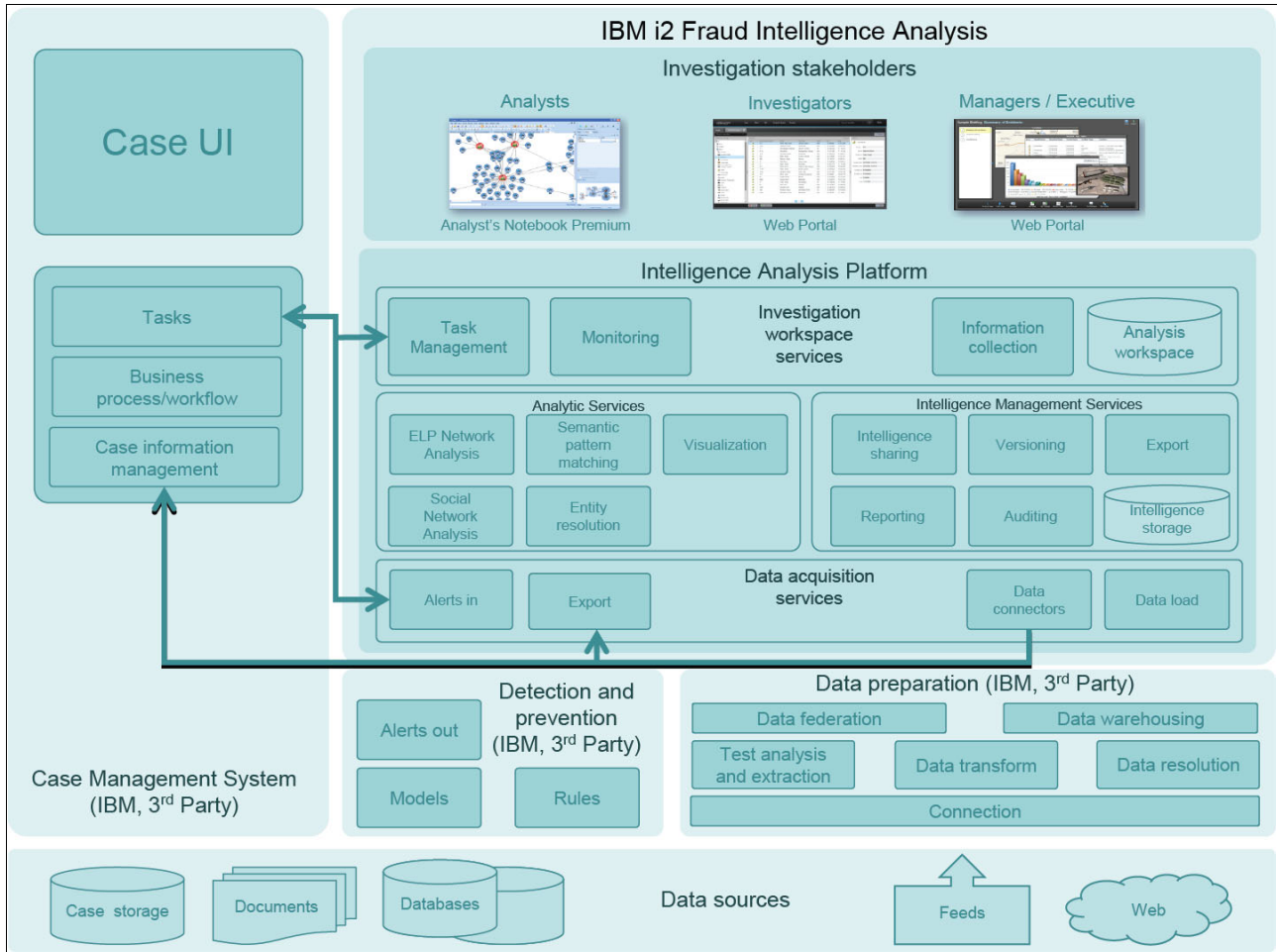


Figure 10 Fraud Intelligence Analysis integration areas

## Case management integration

Fraud Intelligence Analysis can be integrated with an external (IBM or third-party) case management system to provide coordination, workflow, and case material management support. There are three integration points:

- ▶ **Task integration**  
Task integration is the synchronization between tasks that are created in the case management system and the handling and tracking of those tasks in the Fraud Intelligence Analysis solution.
- ▶ **Information integration**  
Information within the case management system can be accessed within Fraud Intelligence Analysis for investigation and analysis. The resulting intelligence that is generated within Fraud Intelligence Analysis can also be exported to the case management system.

- ▶ Alert integration

Fraud Intelligence Analysis alerts can be generated from the case management system when a new task or information is created.

## Detection system integration

When a potential fraud case is detected through a detection system, the system can be used to initiate investigative and analysis work in Fraud Intelligence Analysis. Integration points include the following items:

- ▶ Alert integration

When detection occurs, an alert can be sent to Fraud Intelligence Analysis to inform the investigator. Information in the alert can be used to identify the key information that surrounds the alert to aid acquisition.

- ▶ Information integration

Information surrounding the detection can be loaded into Fraud Intelligence Analysis through a data load service or accessed on demand through a data connection service.

Where a case management system is available, the detection system might be integrated into it instead of being integrated into Fraud Intelligence Analysis. Here, alerts and tasks are generated in the case management system as a result of the detection. The integration between the case management system and Fraud Intelligence Analysis can then be used to connect the investigator and analyst to the workflow.

## Data source integration

Fraud Intelligence Analysis can be connected to line of business or external data sources to provide the investigator and analyst with the information that they need. Information can be acquired on demand or preinstalled, as described in “IBM i2 Analyst’s Notebook Premium” on page 16. The individual needs and data environment of the client dictates the best data source integration approach, potentially requiring more products to prepare information for use.

## Data preparation integration

IBM offers a number of technologies to assist with the preparation of information to make investigation and analysis more effective and efficient. Common needs in this area include the following items:

- ▶ Unstructured data

IBM Content Analytics provides powerful tools to mine and extract knowledge from text.

- ▶ Fragmented data

Where fragmented or overlapping information exists in multiple sources, IBM Identity Insight provides a means to resolve and consolidate the information.

- ▶ Big data

Where the client has high volumes of information, IBM InfoSphere® can help.

## Extending Fraud Intelligence Analysis

Fraud Intelligence Analysis can be easily extended with a range of IBM or third-party technologies to increase its functionality:

- ▶ Facial recognition in the investigation

Although much fraud and financial crime is perpetrated online, personal interaction is a key stage in many crimes, for example, in the retail and banking sectors. Fraud Intelligence Analysis can be readily extended to harvest faces from cameras and match them to a database. This can be done after the event to support an investigation or in operational real time to support crime prevention.

- ▶ Enforcing process compliance

Fraud Intelligence Analysis includes IBM Operational Decision Manager, which integrates business events and rules to automate decisions across processes and applications. It improves the quality of transaction and process-related decisions that are made repeatedly, determining the appropriate course of action for each client, partner, and internal interaction.

- ▶ IBM SPSS® is used to identify suspicious and anomalous activity and prioritize investigation. IBM SPSS combines domain expertise and advanced analytics to look for suspicious and anomalous transactions as they occur. When it is integrated into your operational processes, IBM SPSS strengthens the prevention of unwanted transactions and drives high risk interactions to your investigation team. Information that is related to an alert is combined with extra, relevant content to completely uncover and visualize the fraud. Additionally, non-suspicious transactions can be identified and processed quickly to keep down operational costs and exceed client expectations.

- ▶ IBM Q1/QRadar® is used for detecting internal and collusive fraud, and cyber attacks. Internal fraud and misuse of systems and privileges is a major source of loss, possibly attracting regulator investigation. QRadar is a leading security information and event manager. It effectively combines log records from across your business in real time and correlates these records with business rules to identify threat, risk, and anomalous behavior. These alerts relate to insider and collusive criminal activity and can be connected to the investigation team in addition to traditional external system and network threats.

- ▶ IBM Advanced Case Management provides a mechanism for storing documentary evidence, preparing cases, and ad hoc workflows that are dependent on the investigation. Advanced Case Manager supports the investigation and complements Fraud Intelligence Analysis as part of the Investigate and Discover subsystem.

- ▶ IBM Identity Insight provides real-time help to predict and preempt financial crime by providing a comprehensive picture of who a person is, who they know, and what they do. Advanced recognition algorithms are used to extract entities from corporate transactional data and combine these entities with other data (watchlists, social security records, and so on). This provides a statistically referenceable identity in situations where criminals are attempting to conceal their identities. This data provides alerts early in the transaction, preventing high risk transactions. This data is also invaluable to the investigation process, enabling the team to focus on the process of combining the high-quality entity information with other related content to document criminal activity.

- ▶ IBM Content Analytics uses unstructured data that forms up to 80% of the total enterprise content that is held in the notes field, emails, CRM systems, and other line of business applications to capture essential information. This content contains significant amounts of high value intelligence to support fraud and financial crime investigations. Connecting your analysts and investigators directly to this content provides real operational advantages and enables the team to turn this vast, unstructured data into actionable insights to support their investigation.
- ▶ IBM InfoSphere Streams enables the ingestion, analysis, and correlation of data from multiple real-time data streams.

## Summary

Fraud Intelligence Analysis provides critical insights to help investigate complex incidents. This produces actionable visualization of critical people and events and documented results for repudiation and potential litigation. Distributed investigation, collaboration, and visible outcomes help to optimize and demonstrate the value of the investigation team.

The Fraud Intelligence Analysis solution adds immediate operational value as a stand-alone solution, but offers a far greater advantage when it is integrated into a holistic solution by using existing investments.

## Other resources for more information

- ▶ IBM Fraud Intelligence Analysis product page  
<http://www.ibm.com/software/products/us/en/fraud-intelligence-analysis/>
- ▶ IBM i2 Intelligence Analysis Portfolio Publications  
<http://www.ibm.com/support/docview.wss?uid=swg27024896>
- ▶ IBM Offering Information page  
[http://www.ibm.com/common/ssi/index.wss?request\\_locale=en](http://www.ibm.com/common/ssi/index.wss?request_locale=en)

On this page, enter IBM i2 Fraud Intelligence Analysis, select the information type, and then click **Search**. On the next page, narrow your search results by geography and language.

## Authors

This guide was written by a team of IBM i2 specialists in collaboration with the International Technical Support Organization (ITSO).



**James Luke** is a Chief Architect in the United Kingdom. He has 20 years of experience in the analytics field. He holds a PhD in Artificial Intelligence and Information Operations from the University of Southampton. His areas of expertise include data mining, data fusion, artificial intelligence, and text analytics. He has written extensively on the practical applications of analytics.



**Tim Cooper** is a Product Line Manager in the United Kingdom. He has over 20 years of experience in the IT Industry. He holds a degree in Computer Science and Psychology from the Open University. His areas of expertise include internet technologies, network security, systems, and process change and solutions to investigate fraud and financial crimes.



**Rob Tucker** is Head of Product Advancement for Intelligence Products at IBM i2 Cambridge, UK. He is an experienced software architect, user experience designer, and business analyst specializing in visually and analytically rich software. He also has experience in lead development, user experience, and business analysis teams. Rob has been working at IBM for 13 years, producing intelligence analysis and investigation management software that is used by the law enforcement, military, national security, and commercial industries.

Thanks to the following people for their contributions to this project:

Esther Boal and Joanna Lockhart  
**IBM Software Group, Industry Products**

Marcela Adan and Debra Landon  
**International Technical Support Organization, Rochester Center**

## Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and client satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## Stay connected to IBM Redbooks

- ▶ Find us on Facebook:  
<http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter:  
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:  
<http://www.linkedin.com/groups?home=&gid=2130806>



- ▶ Explore new IBM Redbooks® publications, residencies, and workshops with the IBM Redbooks weekly newsletter:  
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:  
<http://www.redbooks.ibm.com/rss.html>



# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

## COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-5037-00, was created or updated on November 11, 2013.




## Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>



The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

|             |   |            |
|-------------|---|------------|
| DB2®        | QRadar®   | SPSS®      |
| i2®         | Redbooks®   | Tivoli®    |
| IBM®        | Redguide™   | WebSphere® |
| InfoSphere® | Redbooks (logo)  ® |            |

The following terms are trademarks of other companies:

QRadar, and the Q1 logo are trademarks or registered trademarks of Q1 Labs, an IBM Company.

Other company, product, or service names may be trademarks or service marks of others.