Aite PARTNER. ADVISOR. CATALYST.

Investigation Management for Fraud: Catch More Fraudsters More Efficiently

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

Financial institution fraud teams have an incredibly difficult job that is growing more complex and challenging by the day. The electronification of payments and other banking functions has created vast new opportunities for criminals to compromise the financial system. Corporate account takeover attacks will cost financial institutions (FIs) around the globe US$523 million in 2013 (Aite Group, 2013), while database breaches are contributing to sharp rises in counterfeit card fraud and consumer account takeover.

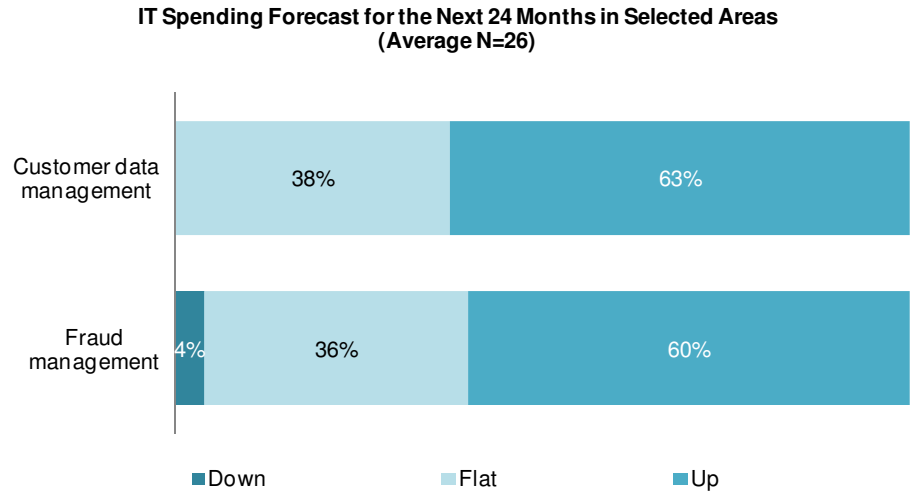
The vast majority of these attacks are deployed by international organized crime rings, which study their targets and deploy operatives who work together to maximize their financial gain. Some attacks are rapid, such as a flurry of Trojans targeting an institution's customers to capitalize on a weakness in the FI's defenses. Others are developed over time, such as complex networks of "sleepers" lying in wait for two years or more before busting out and causing tens of thousands of dollars' worth of losses. All of this is set against the backdrop of FI product innovation and faster payments, both of which reduce the time that FIs have to analyze and respond to emerging risks.

A NEED FOR BETTER INVESTIGATIVE TOOLS

In response to the mounting threats and customer concerns for safekeeping of their assets, FIs must be able to demonstrate that they are keeping pace with the criminals. Many FIs are taking a combined approach to fraud and anti-money laundering (AML) investigations, bringing them under a central "financial crimes" umbrella, gaining incremental efficiencies, and rendering them better able to respond to both the threat environment and regulatory pressure. To support these efforts, FIs are searching for faster, more nimble and intelligent detection and investigation technology. FIs need new tools that can help them efficiently sift through massive amounts of data and discover patterns that are indicative of fraud.

Legacy system functionality designed to prevent, detect, and investigate financial crimes has been overtaken by new technology-enabled use cases that move information and facilitate transactions faster than these systems can keep pace with. Accordingly, a new generation of intelligent investigation management solutions is required to assist, guide, and augment analysts' and investigators' activities. Combating financial crimes is difficult enough for a single line of business, but the data challenge and complexities multiply as FIs seek to implement an integrated financial crimes investigation solution across products and channels, searching through voluminous amounts of both structured and unstructured data sources. Moreover, FIs need to correlate alerts from multiple third-party and in-house detection systems to eliminate redundancy on overlapping cases. To solve the myriad challenges, many FIs are turning to technology. In a Q2 2012 global survey of large FIs, 60% of IT executives indicated that investments in fraud mitigation technology will increase, and 63% of respondents expect to increase their investment in customer data management technology (Figure 1).

Figure 1: Bank Investments in Fraud and Data Management Technology



Source: Aite Group's global survey of banks with more than US$10 billion in assets, Q2 2012

A key technology that many FIs are turning to in their quest for greater speed, efficiency, internal collaboration, and increased detection is the investigation management system. Best-in-class investigation management systems help FIs share information across functions, compile data to discover fraudsters who are hitting the FI in disparate silos, and facilitate collaboration, communication, and oversight during the investigative process.

WHY SOLVE THE PROBLEM

Simply stated, being one step behind the bad guys is not an acceptable option. Combating financial crime is a perpetual battle, with criminals leveraging the latest technology to find new ways to circumvent FIs' defenses. The future viability of banking hinges upon FIs' ability to build and maintain a high level of trust and security in its service offerings. Many FIs today rely on legacy investigative platforms that have long since outlived their useful life and are overwhelmed by the rate of fraudsters' innovation. As a result, FIs are looking to upgrade their capabilities to address the following:

- **Lack of a holistic customer view:** A key driver of FIs' push toward enterprise investigation management systems is the desire to obtain a holistic view of the consumer. Fraudsters do not limit their attempts to any particular channel or product, but banks' legacy systems are often siloed by channel or line of business. In the current environment, the view of anomalous activity associated with a single consumer is also siloed, causing each line of business to receive a separate set of alerts and to create its own case and investigation systems. This not only creates operational inefficiencies but also prevents the FI from proactively discovering the multiple issues that may exist with a single customer account, resulting in disjointed customer communication and reduced effectiveness of fraud investigations.

- **Harnessing the power of data:** There is a vast amount of data, both internal and external, that should be, but seldom is, available to the FI to use in detecting fraud. Effectively bringing all of the customer data together and making sense of it in real time but without the latest data analytics and management capabilities is unrealistic and almost unattainable to address. This data must be brought under control and converted into actionable intelligence, however, in order to obtain incremental intelligence and discover fraudulent transactions hidden within it.

- **Improved detection and efficiency:** Enterprise investigation platforms enable detection and investigation groups to more efficiently share data and collaborate. Given the large quantities of case information to be correlated and analyzed, FIs are also looking to apply analytics to help prioritize workflows and detect correlations and connections among cases. This helps to increase the productivity per full-time employee, assist in detecting emergent fraud patterns, and reduce losses.

- **New compliance demands**: The compliance bar is being raised higher and higher, requiring deeper and more intelligent monitoring, audit reporting, and investigation. AML is a good example of an area in which the investigation process has grown in complexity, requiring FIs to track down money movement schemes designed to hide illegal deposits, identify beneficial ownership, and discover previously unknown customer transaction information located within the FIs' LOB systems.

This white paper, based in part upon Aite Group interviews with senior fraud and financial crimes executives at 18 of the top 35 North American financial institutions from June to August 2012, addresses the ways in which FIs are embracing enterprise investigation management technology. It describes the characteristics of best-in-class platforms and concludes with an overview of IBM's approach to enabling FIs to more effectively and efficiently undertake their financial crimes investigations.

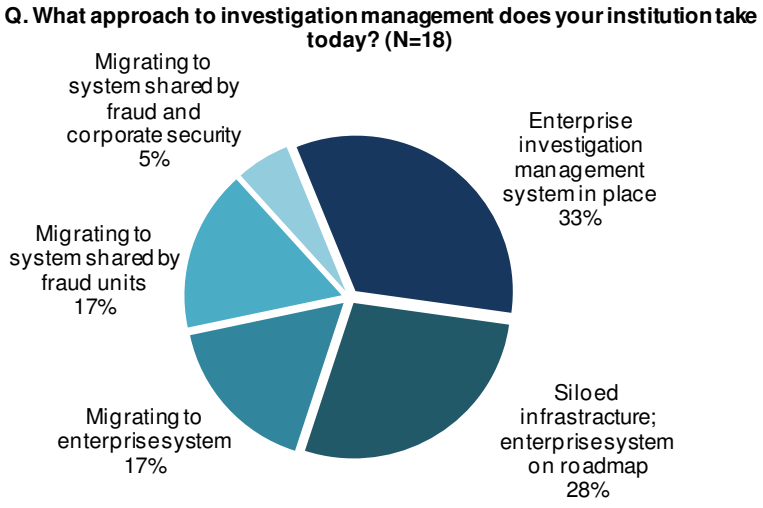
ENTERPRISE INVESTIGATION MANAGEMENT: AN ENABLING TECHNOLOGY

Enterprise investigation management platforms provide for the aggregation, at a logical or physical location, of data, notes, and activities relating to a fraud investigation. This not only aids in the investigation process but also serves as a system of record for compliance purposes and as a data repository for investigations. Investigation management tools also help manage workflow and assist in the appropriate classification of fraud events.

Enterprise investigation management is an active area of investment for FIs, as shown in Figure 2. Aite Group interviews with risk executives at 18 of the top 35 North American FIs find that one-third of respondents have an investigation management system in place today. Twenty-eight percent of FIs still have highly segregated operations with multiple silos, each relying on its own set of legacy functionality. Thirty-nine percent of respondents are in the process of migrating to an enterprise investigation management system, which will be shared by the following parties:

- All fraud units and corporate security
- Just the fraud units
- Fraud, corporate security, and anti-money laundering (AML) units

Figure 2: FIs' Evolving Approach to Investigation Management

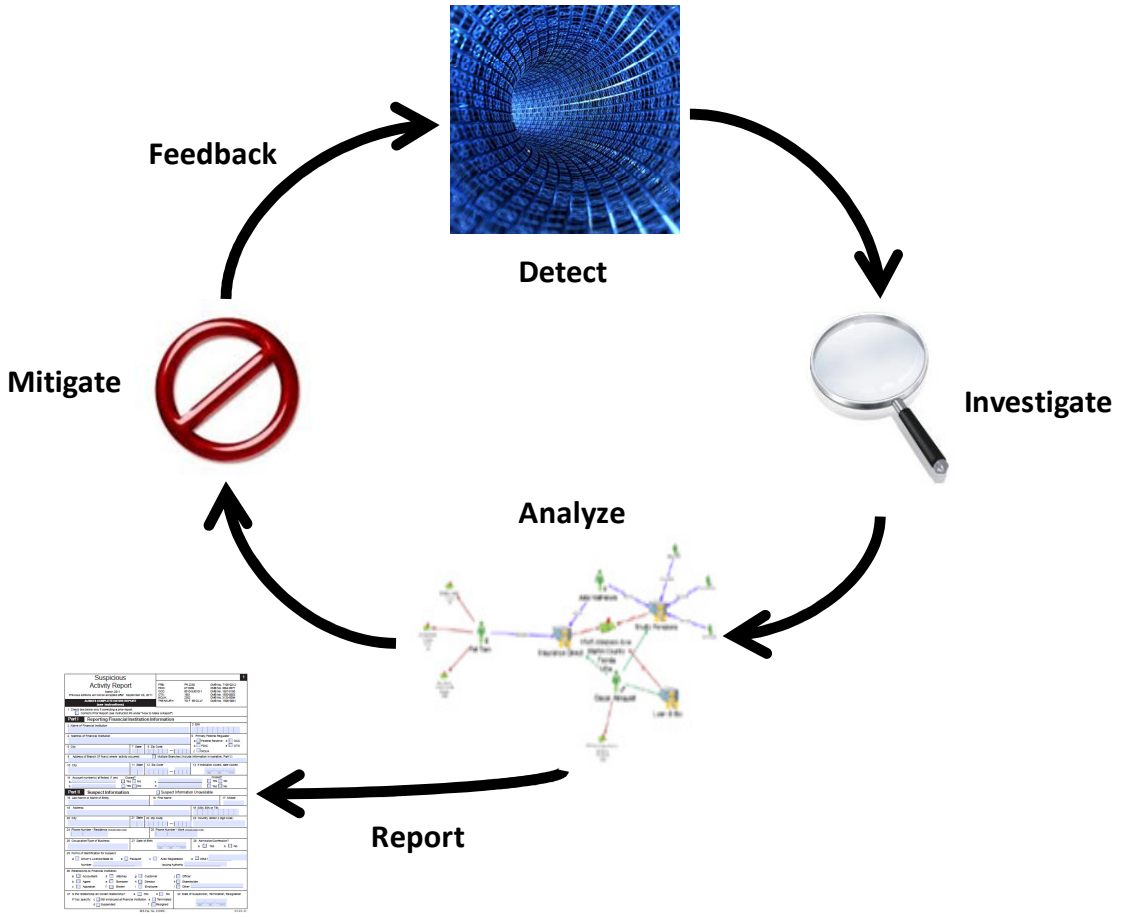


Source: Aite Group interviews with 18 large North American FIs, June to August 2012

INVESTIGATIVE LIFECYCLE

Financial crime investigations include a series of actions—detection, investigation, analysis, mitigation, reporting, and feedback—each of which a best-in-class investigation management solution should have the ability to support (Figure 3).

Figure 3: Investigative Lifecycle



Source: Aite Group

DETECT

The first step is detection of an anomalous behavior. FIs have myriad systems in place to accomplish this task, from rules-based triggers to sophisticated behavioral analytics to channel-specific technologies such as complex device fingerprinting. Fraud analysts work the alerts generated from these systems to determine whether they are genuine indicators of fraud or false positives.

INVESTIGATE

Once the fraud analyst determines that there is a likelihood of fraud, a case will be created, the case type classified and case codes assigned to ensure the right and consistent actions are taken,

and the investigation will begin. As the investigation proceeds, investigators will add data to the investigative system and additional codes as new information and findings are uncovered.

ANALYZE

An investigation management solution should provide the investigations team with the ability to correlate data with specific cases through link analysis and to identify connections between individual cases, as well as incorporate information from other structured and unstructured data sources, such as social media feeds and transactional and enterprise content management databases.

MITIGATE

The mitigation approach will vary depending on whether the incident is related to fraud, AML, corporate security, or information security. If the incident is related to fraud, corporate security, or information security, then direct action will be taken to minimize or prevent the losses to the institution. If AML, then the FI will perform the investigation and file a suspicious activity report (SAR) but will rarely directly perform interdiction unless the incident is watch-list-related.

REPORT

Periodic reports are required, both canned and ad hoc, in order to aid analysts in the performance of their job as well as to help management oversee the process. In addition, SARs need to be filed in the appropriate format for the country or jurisdiction, which the investigative platform should be able to facilitate in an automated fashion.

FEEDBACK

A feedback loop is essential, feeding the results of the investigation back into the front-end production systems in order to optimize their ability to deliver better results with fewer false positives going forward. A feedback loop will also enable the institution to close down the gaps, addressing the weaknesses in current systems…weaknesses that criminals can exploit.

ENTERPRISE INVESTIGATION MANAGEMENT SYSTEMS

Best-in-class investigation management systems have the ability to support each step of the investigative lifecycle outlined above. The following sections provide an overview of each component of such systems and the features and capabilities that FIs should be looking for as they evaluate new vendors: alert management, case management, dashboard management, and link analysis.

ALERT MANAGEMENT

Alert management engines ingest the output of detection systems and help prioritize the workflow for fraud-detection analysts and investigation teams, and ensure consistent execution. Best-in-class alert management tools should include the following capabilities:

- Ability to aggregate alerts from multiple fraud detection systems

- Ability to control distribution of alerts in order to distribute the workload evenly, prioritize highest-risk alerts, and assign alerts based on the skill level of the fraud analyst (e.g., entry-level analysts may only be allowed to work alerts up to a certain dollar value of exposure)
- Ability to notify users when alerts requiring attention have entered the system
- Automatic disposition of alerts based on rules or analytics

The latter point is one of the most important qualities of alert management among FIs interviewed by Aite Group. The escalating threat environment has resulted in myriad fraud-detection tools, all of which produce alerts that must be worked to determine whether they are true indicators of fraud or false positives. Best-in-class investigation management systems have the ability to apply analytics and self-learning to help maximize the efforts of already overburdened detection and investigative teams.

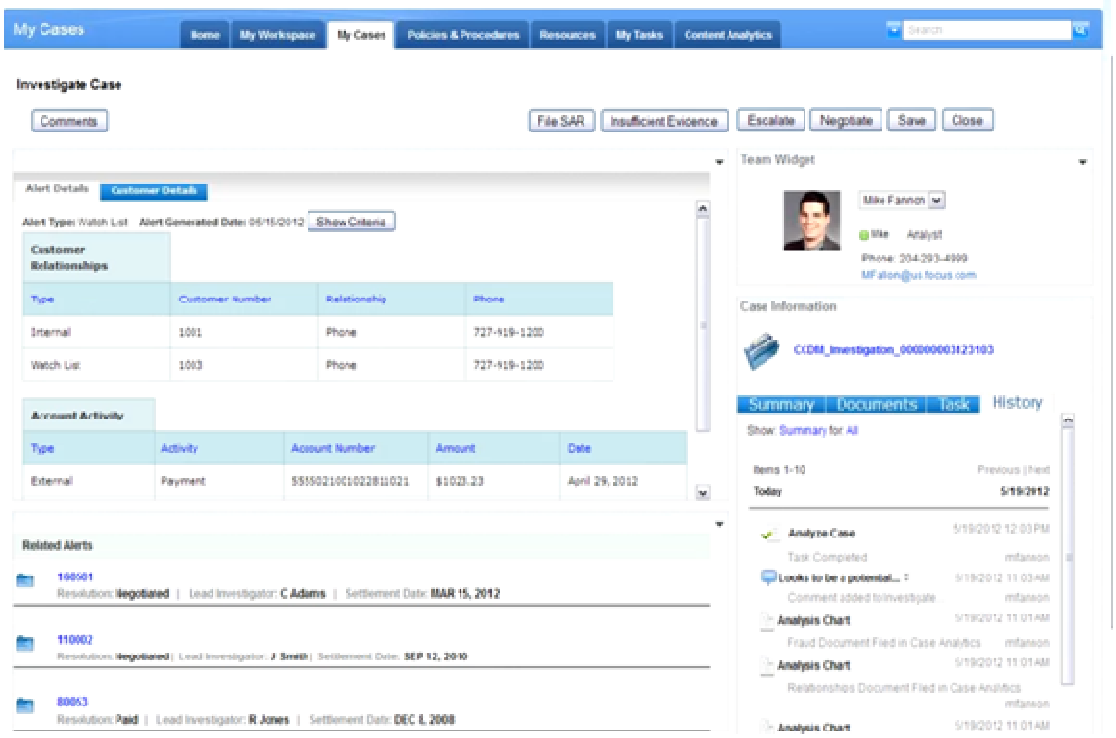
CASE MANAGEMENT

Advanced case management systems help FIs build information over the course of an investigation as well as share information with other parties and compile cross-functional case data. Case management platforms also help bridge the silos that still may be in place in the investigations groups. For example, they can allow investigators in the check fraud group see that there is also a case underway in the credit card group focusing on the same customer or featuring the same protagonists. Once the case has been finalized, best-in-class case management systems also provide a framework to classify the loss and help identify the root cause.

The classification capability is an important attribute, and one that is lacking in many legacy systems. Institutions need to understand their fraud problems in order to accurately prioritize investment in mitigation tools. It is important that the case management system gives the institution the ability to associate the fraud not only with the payment type that was used in perpetrating the fraud but with the root cause of the fraud incident. When it comes time to examine losses and determine where to prioritize fraud-prevention budget dollars, this data classification is necessary to support the business case for the appropriate types of preventative technology.

Another important consideration for FIs evaluating case management platforms is the degree to which the interface is intuitive and user-friendly (Figure 4 provides an example of such an interface). All FIs have slightly different workflow processes and business requirements, and the user interface should optimally provide the FI with the ability to configure the system to its own unique roles or processes. The result should be a user interface that displays only necessary data and which is easy and efficient to navigate. Every additional click that a user has to make to get to the desired screen represents a split second of lost productivity that adds up and, over time, directly contributes to the expense line.

Figure 4: Sample Case Management Screenshot



Source: IBM

Finally, case management systems need to be flexible and dynamic, reflecting the nature of the work itself and the users of the solution. The investigative team needs a system that has the ability to launch, assign, track, and complete the work. It requires a flexible work model that combines support for automated, orchestrated work as well as user-created, dynamic scenarios. It also needs to be able to have configurable workflow management capabilities that allow an FI to easily configure the system to mirror and support its own unique business processes.

DASHBOARD MANAGEMENT

Dashboard management tools provide rich sources of management information system (MIS) reporting that help with oversight, enabling management to evaluate the efficiency of fraud tools, rule settings, and operational personnel as well as to measure the impact of fraud and detect trends. Information is power, and dashboard tools are important contributors to decision-making across the FI.

LINK ANALYSIS

Link analysis tools sift through the data repositories at FIs and discover connections between customers and accounts. Some connections are innocuous, others highly suspicious. Effective link analysis tools can differentiate between these, prioritizing the suspicious networks and providing users with a visualization tool that helps them understand and investigate the linkages. Ring-based activity is one of the most costly types of fraud for an FI and also one of the most difficult to detect without an advanced link analysis capability in place.

THE BENEFITS OF INVESTIGATION MANAGEMENT

While the investment in investigation management is not insignificant, a number of factors make it well worth the effort.

- **Increased detection rate:** The ability to sift through vast quantities of data and uncover patterns and linkages provides fraud teams with the ability to identity more fraud more quickly and to better understand the true scope of the problem. This translates to direct bottom line benefit for the FI, with less revenue lost to fraud and greater profitability.
- **Operational efficiencies:** Application of advanced technology can help to automate the assimilation of overlapping alerts into cases and to reduce the manual effort associated with sifting through vast quantities of data to find the proverbial "needle in the haystack," allowing FIs to do more work with the same amount of resources.
- **Enhanced customer experience:** A holistic view of the customer can provide associates with the data that they need to make better customer-service decisions, minimizing false positives and adverse impact to good customers.

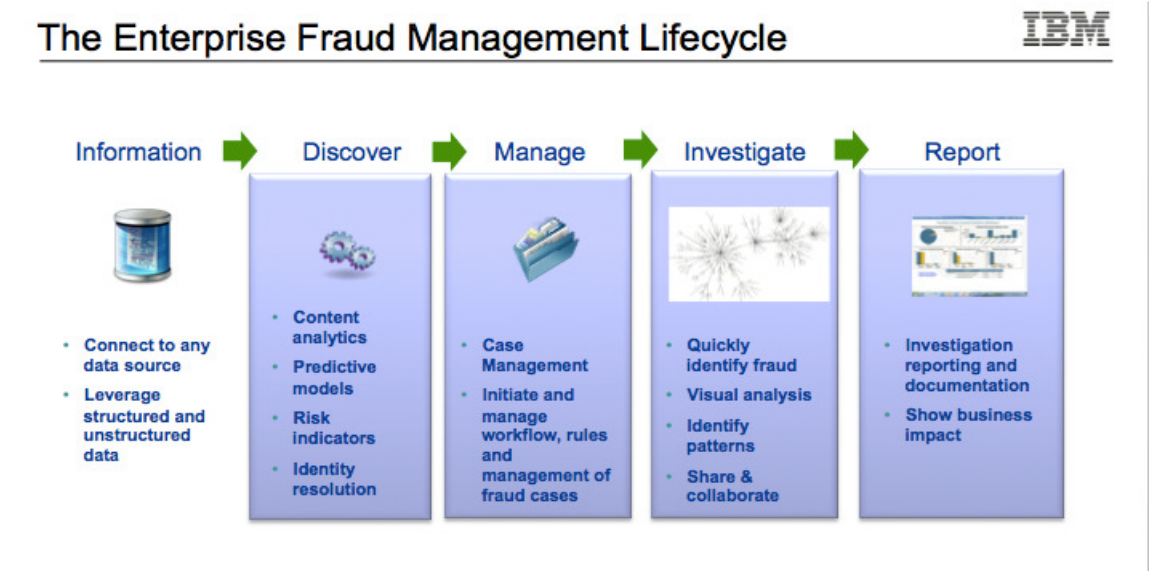
A number of other benefits are offered by best-in-class investigation management systems and are important considerations from a supervision, control, and consistency point of view.

- **Supervision:** The workflow capability enables investigators to forward cases to supervisors automatically when reviews or approvals are required (e.g., a review of all loss-mitigation steps performed may be required by a supervisor before a case over a specified dollar amount is sent to be charged off). Supervisors can perform their review and then return the case to the investigator with directions for additional efforts or forward the case to be charged off. Granting key managers in the FI read-only access allows them to check the current status of a case and the loss-avoidance efforts without calling the investigator. This is vitally important in cases of potential large-dollar losses and in cases involving high-profile clients. Avoiding constant interruptions allows investigators to focus on their work and handle more cases per full-time employee.
- **Compliance:** Investigative systems can automate many compliance requirements; for example, by establishing a defined process with timelines, FIs can ensure and demonstrate compliance to regulators. Automated suspicious-activity investigation and reporting can be established to allow internal reviews and approvals prior to the SAR being sent to the regulatory authority. These capabilities are essential from a compliance perspective and provide the additional benefit of improving operational efficiency.
- **Management reporting:** The investigation management system can enable the automation of MIS reports, eliminating the need to manually pull data and manipulate it to create standard periodic reports. If the system allows input by job category of performance data, individuals can monitor their own performance, allowing periodic reviews to become coaching sessions with no unpleasant performance surprises.

IBM'S INTELLIGENT INVESTIGATION MANAGEMENT SOLUTION

Against this backdrop, the key components of the IBM Intelligent Investigation Manager offering IBM Case Manager, IBM Content Analytics, and IBM i2 Fraud Investigation Analysis provide a powerful, integrated set of capabilities for managing investigations. Because fraudsters' methods change constantly, the offering is designed to react dynamically to changes in workflow and content. Intelligent Investigation Manager helps boost the efficiency and effectiveness of investigations by capturing all the relevant details and actions of each case, enabling investigators to execute and collaborate dynamically. In addition, it incorporates forensic and link analysis into the investigative process, generating evidence that can provide investigators with leads and help them better understand the scope of and then act upon the fraudulent activity. Products such as IBM Identity Insight and SPSS enable fraud detection and prediction; together, these solutions address the entire enterprise fraud management lifecycle (Figure 5).

Figure 5: IBM Fraud Management Lifecycle



Source: IBM

CASE MANAGER

The foundation of the solution is IBM Case Manager, which provides comprehensive case management capabilities, including the following:

- A case model that captures all of the relevant content and activity in an investigation, providing a single, consistent view of the case to all members of the investigative team
- A flexible task model that combines the ability to drive and orchestrate a case with support for ad-hoc, user-created tasks initiated by the investigative team
- Analytics to help prioritize highest-risk incidents
- Widget-based, configurable user interfaces
- An integrated rules system, which can trigger actions once a case has been tagged as fraud
- Granular fraud-classification and reporting capabilities
- Ability to aggregate and consolidate cases to eliminate redundant efforts
- Reporting and analytics capabilities that enable the investigative team and supervisors to view operational and business metrics around the investigative process

IBM CONTENT ANALYTICS

IBM Content Analytics offers the ability to use natural-language processing and other statistical and machine-learning techniques to extract facts, entities, concepts, and objects from vast repositories of unstructured or textual information. IBM Content Analytics provides the following capabilities:

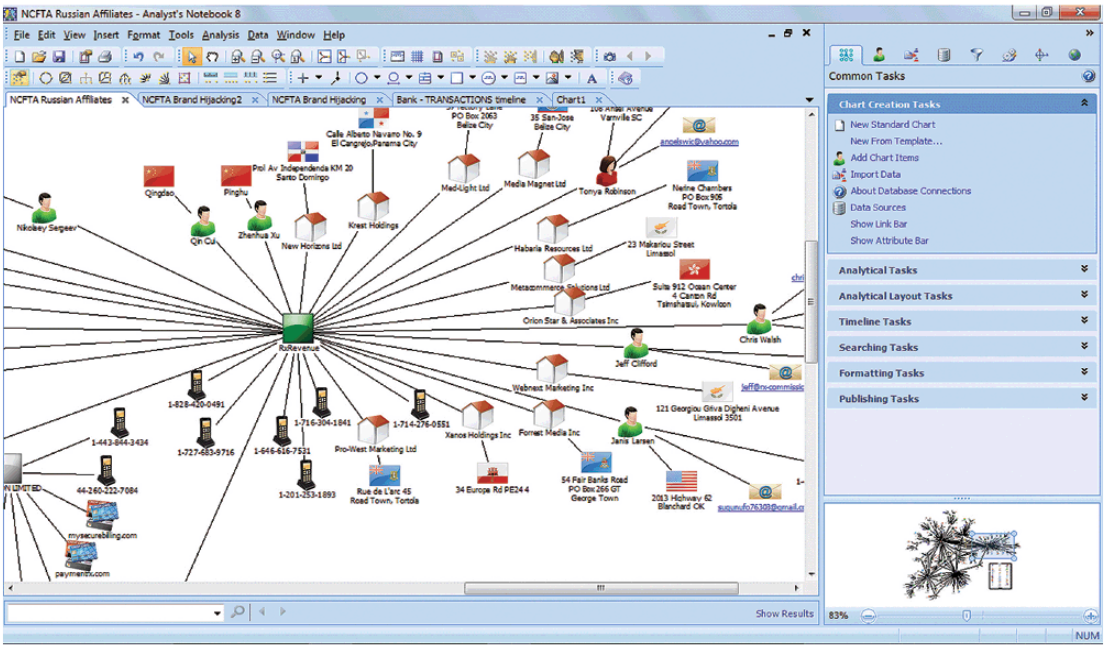
- Helps search, analyze, and extract entities from unstructured data
- Helps discover suspicious patterns in unstructured data
- Offers flexible search, visualization, and exploration across structured and unstructured data
- Precalculates and perpetually updates analytics on identities and relationships
- Scales to big data volume and is available for real-time text and content analytics

IBM I2 FRAUD INTELLIGENCE ANALYSIS

IBM's Investigation Manager also includes an integrated connection to its i2 Fraud Intelligence Analysis platform. This graphic interface provides investigators with the ability to work collaboratively with analysts to identify high-risk networks of individuals and take action to mitigate potential fraud issues. It performs entity resolution, link analysis, transactional analysis, social network analysis, temporal analysis, and geospatial analysis. This enables analysts to move

through massive amounts of structured and unstructured data, even across lines of business, and create visualizations that highlight the scope of the fraud, generate investigative leads, and provide evidentiary documentation (Figure 6).

Figure 6: IBM's i2 Link Analysis Capability

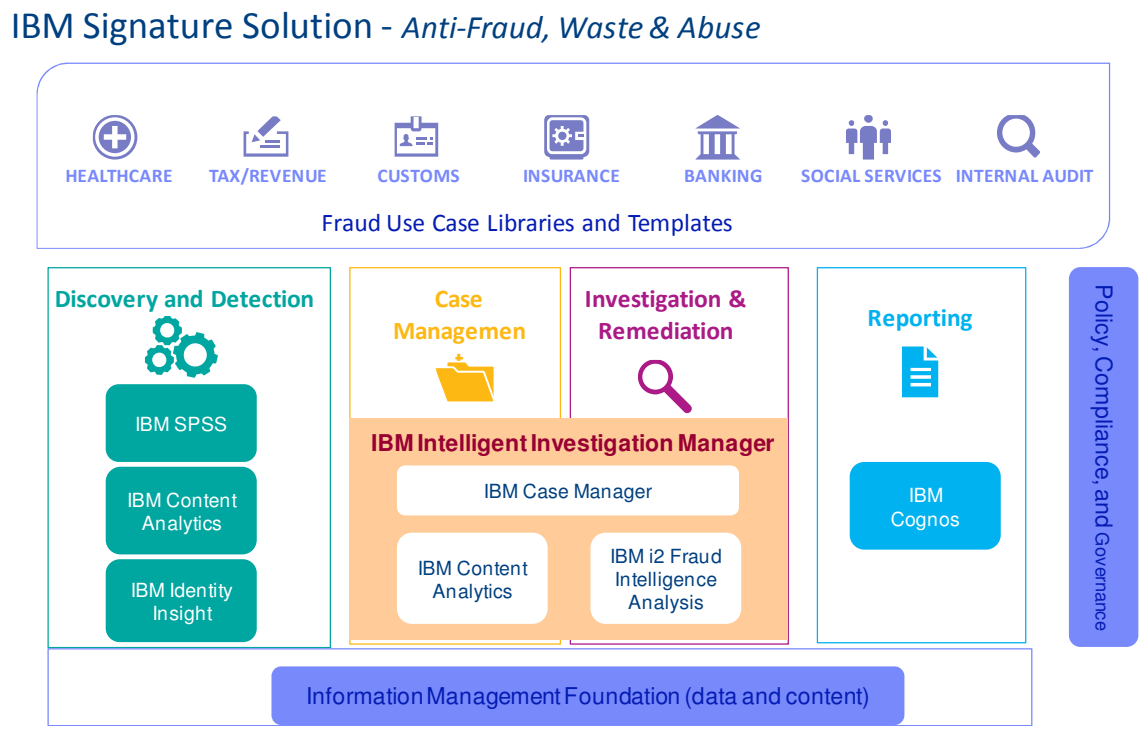


Source: IBM

The IBM Investigation Manager can be used on its own or within IBM's Smarter Analytics Signature Solution to deliver an end-to-end fraud solution (Figure 7).

- **SPSS Threat Detection Analytics:** SPSS' advanced analytics provide FIs the ability to apply analytics and detect suspicious patterns that are indicative of fraud.
- **Identity Insight:** Identity Insight is an advanced entity analytics solution with sophisticated recognition algorithms optimized to help predict and pre-empt criminal activity by providing entity resolution, relationship resolution, and complex event processing capabilities.
- **Enterprise performance management dashboards:** IBM business intelligence software provides dashboards of key metrics and scorecards that managers can use to manage their business; its capabilities include:
    - The ability for users to create their own dashboards without IT involvement
    - Real-time updates to information, enabling users to make informed decisions
    - Leverage planning and budgeting tools to improve process efficiency

Figure 7: IBM Signature Solution



Source: IBM

CONCLUSION

Criminals have access to more data and resources than ever before, and they are mounting highly sophisticated attacks on FIs and their customers. At the same time, FIs are seeking to differentiate their service offerings, fast payments, and quick access to funds. In an environment where time is money, FIs are investing in enterprise investigation management technology in order to find new ways to proactively detect and interdict financial crimes.

Advanced investigation management technology can help FIs with their goals of improving financial crimes investigation processes and efficiency. It accomplishes this by:

- Distilling complex data sets into actionable intelligence
- Facilitating collaboration among analysts and detection teams
- Creating efficiencies through effective workflow management and case management

FIs that have made the organizational and technological investment in an enterprise approach to investigation management have reaped the benefits, seeing robust return on investment through operational efficiency and improved detection capabilities. As FIs increasingly compete on their ability to provide fast, innovative services to their customers, robust enterprise investigation capabilities will not only be the driver of efficiencies, it also will increasingly serve as an enabler of revenue.

ABOUT AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

AUTHOR INFORMATION

Julie Conroy
+1.517.992.5087
jconroy@aitegroup.com

Shirley Inscoe
+1.704.987.5087
sinscoe@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.338.6050
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com