Aite PARTNER. ADVISOR. CATALYST.

Investigation Management for Insurance: Catch More Fraud More Efficiently

TABLE OF CONTENTS

INTRODUCTION 3

THE PROBLEM: A NEED FOR BETTER INVESTIGATIVE TOOLS 3

WHY SOLVE THE PROBLEM: THE CHALLENGES OF LEGACY SYSTEMS 4

ENTERPRISE INVESTIGATION MANAGEMENT: AN ENABLING TECHNOLOGY 5

INVESTIGATIVE LIFECYCLE 5

INVESTIGATION MANAGEMENT SYSTEM CAPABILITIES 7

ALERT MANAGEMENT 7

CASE MANAGEMENT 7

DASHBOARD MANAGEMENT 8

LINK AND PATTERN ANALYTICS 9

TEXT ANALYTICS 9

BENEFITS: THE BUSINESS CASE FOR INVESTIGATION MANAGEMENT 10

IBM INTELLIGENT INVESTIGATION MANAGER: INTEGRATED INVESTIGATION MANAGEMENT SOLUTION . 11

CASE MANAGER 12

CONTENT ANALYTICS 12

I2 FRAUD INTELLIGENCE ANALYSIS 13

INTELLIGENT INVESTIGATION PLATFORM USE IN INSURANCE 15

CONCLUSION 16

ABOUT AITE GROUP 17

AUTHOR INFORMATION 17

CONTACT 17

LIST OF FIGURES

FIGURE 1: INVESTIGATIONS LIFECYCLE 6

FIGURE 2: SAMPLE IBM CASE MANAGEMENT SCREENSHOT 8

FIGURE 4: FRAUD MANAGEMENT LIFECYCLE 11

FIGURE 5: IBM'S I2 LINK ANALYSIS CAPABILITY 13

FIGURE 6: IBM SMARTER ANALYTICS SIGNATURE SOLUTION—ANTI-FRAUD, WASTE AND ABUSE 14

INTRODUCTION

Insurance fraud impacts every consumer and taxpayer. The global insurance industry comprises thousands of companies and collects trillions of dollars in premiums annually, both of which make it an attractive target for fraud. So too does the fact that insurance fraud currently sees low levels of detection and prosecution.

Insurance fraud in North America, specifically property & casualty (P&C) and life insurance, is currently estimated to exceed US$40 billion annually.[1] While P&C insurance fraud receives the most attention in terms of frequency and media visibility, U.S. healthcare fraud is estimated to total as much as US$115 billion each year.[2] Life insurance fraud frequently involves organized groups of dishonest insurance agents and elaborate schemes that run into the tens—and even hundreds—of millions of dollars in losses. Although auto and property claims counts have declined approximately 2%, [3] the number of questionable P&C claims has risen more than 33% since 2008.[4] Claims fraud in the P&C insurance industry alone is conservatively estimated to cost US$30 billion annually,[4] with workers' compensation and auto insurance fraud leading the way. Detecting and deterring fraud consistently ranks among the top three investment and strategic priorities for P&C insurance industry executives.

THE PROBLEM: A NEED FOR BETTER INVESTIGATIVE TOOLS

An effective, integrated fraud management program requires operational alignment, a well-articulated strategy, and high information quality, all managed and enhanced by advanced technology tools and analytics. Unfortunately, insurers' efforts to improve upon their ability to identify and deter fraudulent activities have typically been fragmented by the absence of a standard, comprehensive enterprise-wide fraud management process. Further, the challenge created by the growth of fraud is magnified by industry reductions undergone in order to reduce overhead in the post-recession, slow-growth period and to survive and grow in a fiercely competitive marketplace. And now, as the internal and external sources, volume, type, and complexity of data becoming available to insurers grow exponentially and across enterprise silos, the desire to use this data in fraud management—and the inability to do so—only adds further complexity and frustration. Add to this the growing sophistication of foreign and domestic criminals aided and emboldened by technology and the relatively low risk of real prosecution, and these factors represent a daunting challenge to insurers. As a result, insurers are making increasing investments in business intelligence and advanced analytics to address the fraud problem. Other promising initiatives include industry cooperation through information sharing and participation in public and private fraud-fighting coalitions.

[1] CAIF (Coalition Against Insurance Fraud), 2012.

[2] National Health Care Anti-Fraud Association, *The Problem of Health Care Fraud*, 2012.

[3] CCC Information Services, Inc. Crash Course, 2012.

[4] NICB (National Insurance Crime Bureau), 2012.

[5] NICB and Deloitte Consulting, *A call to action: Identifying strategies to win the war against insurance claims fraud,* August 2012.

The ability to move beyond fragmented efforts depends in large part upon integrating quality internal and external information in order to identify fraud early. As carriers adopt more innovative and effective fraud-detection solutions in response to the growing threat of fraud, they need equally innovative and powerful investigation management systems to manage the increased volume of complex referrals being generated.

Insurers also require the ability to accurately identify and segment fraudulent activity from legitimate activity in order to improve the productivity of both investigative and detection staff while simultaneously increasing customer service and satisfaction. Most importantly, core insurance processes need to fluidly incorporate investigations; therefore, case management software needs to evolve to investigation management software—a single, dynamic, holistic enterprise repository where all information related to a specific investigation is stored and shared among all authorized users and which incorporates the results of fraud analytics and other investigative tools. This record will include every detail in the entire lifecycle of a potentially fraudulent event, from the moment it is identified through the ultimate resolution, recovery, and closure.

WHY SOLVE THE PROBLEM: THE CHALLENGES OF LEGACY SYSTEMS

Many insurers are on legacy platforms that have long since outlived their useful life. There are a number of reasons why insurers are now looking to upgrade their capabilities:

- **Efficiency and improved detection:** Enterprise fraud management platforms enable detection and investigation groups to more efficiently share data and to collaborate. Given the vast amount of case information to be correlated and analyzed, insurers are also looking to apply analytics to help prioritize workflows and detect correlations and connections among and between cases. This will help increase the productivity per employee and assist insurers in detecting emergent fraud patterns and reducing losses. Most importantly, carriers are working to evolve from a retrospective fraud detection model, in which recovery after the fact is costly and unproductive, to a more proactive model, in which fraud is detected throughout its lifecycle, including prior to payout.

- **Compliance gains:** By using workflows effectively, insurers can automate regulatory compliance—such as an automatic compliance process for filing suspicious activity reports (SARs)—with the appropriate review and approval steps. Additionally, analytical workflow and process tools can make mandatory reporting obligations to state and federal agencies and multiple fraud bureau databases cost less and happen more quickly.

This white paper covers the ways in which insurers are embracing enterprise investigation management technology, describes the characteristics of best-in-class platforms, and concludes with an overview of IBM’s approach to enabling insurers to be more effective and efficient with their fraud investigations.

ENTERPRISE INVESTIGATION MANAGEMENT: AN ENABLING TECHNOLOGY

Enterprise investigation management platforms provide for the aggregation of all data, rules, 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 central data repository for aiding law enforcement investigations. Investigation management tools also help manage workflow, support collaboration amongst the investigative team, and assist in the appropriate classification of fraud events.

A number of drivers are pushing insurers to invest in enterprise investigation management platforms, chief among them the ability to enable detection and investigations groups to more efficiently harvest insights, share data, and collaborate.

INVESTIGATIVE LIFECYCLE

Insurance fraud investigations include a series of actions, each of which a best-in-class investigation management solution should have the ability to support (Figure 1).

- **Detect:** A preliminary step includes discovery in which carriers identify, study, and prepare the data to which rules will be applied and on which analytics will be performed, followed by detection of an anomalous behavior. Insurers have myriad systems in place to accomplish this task, from rules-based triggers to sophisticated behavioral analytics. Fraud analysts work the alerts generated from these systems to determine whether they are genuine indicators of fraud or false positives.

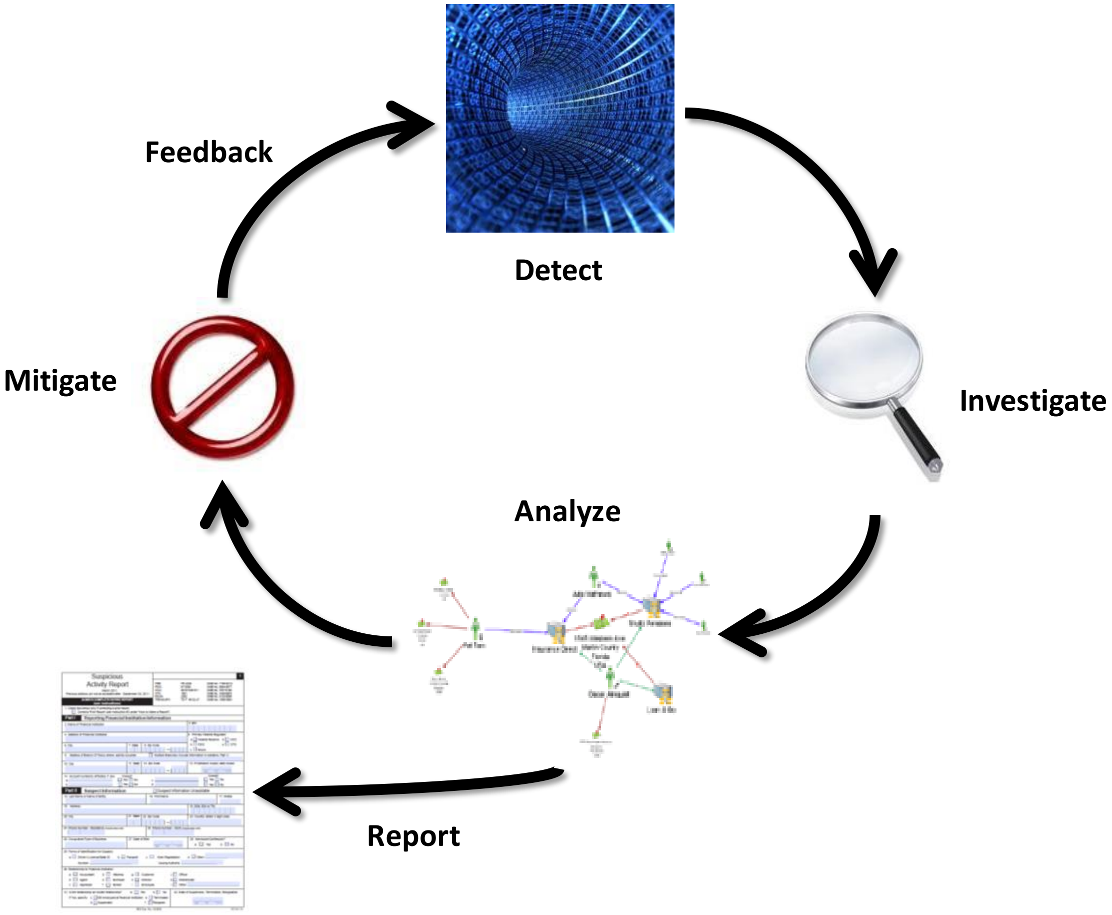
- **Investigate:** Once the fraud analyst determines that there is a likelihood of fraud, a case will be created and investigation will begin. The enterprise investigation management solution aids investigators in completing necessary tasks while enhancing their requisite judgment and expertise. As the investigation proceeds, investigators will add data to the investigation management system as it is 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. Investigation and analysis actions are dynamic and not always linear over the course of a case.

- **Mitigate:** The mitigation approach will vary depending on the line of business and whether the incident is related to policyholder, claimant, vendor, or internal or information security fraud. Mitigation procedures can range from requests for additional information and investigative referral to outright denial of the claim. Prompt and appropriate action will be taken to minimize or prevent losses to the insurer. Several types of fraud also require filing of reports with industry agencies, external databases, and law enforcement.

- **Report:** A suspicious-activity report needs to be filed in the appropriate format for the country or jurisdiction. Depending on the nature of the fraud, law enforcement may also be contacted, although law enforcement will not always have the ability to pursue the case due to limited bandwidth.
- **Feedback:** A feedback loop is essential, feeding the results of the investigation back into the front-end tools in order to optimize their ability to deliver better results with fewer false positives going forward.

Figure 1: Investigations Lifecycle



Source: Aite Group

INVESTIGATION MANAGEMENT SYSTEM CAPABILITIES

Best-in-class investigation management systems have the ability to support each step of the investigations lifecycle. The following sections provide an overview of each component of such systems and the features and capabilities that insurers should be looking for as they evaluate new vendors.

ALERT MANAGEMENT

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

- Ability to aggregate alerts from multiple fraud tools
- Ability to control distribution of alerts in order to distribute the workload evenly, prioritize highest-risk alerts, and leverage worker expertise
- Ability to notify users when alerts requiring attention have entered the system
- Automatic disposition of alerts based on rules or analytics

The escalating threat environment has resulted in multiplying fraud tools, all of which produce alerts that must be worked, along with some level of false positives. Insurers are looking for an alert management system that can apply analytics and self-learning to help maximize the efforts of already overburdened detection and investigations teams.

CASE MANAGEMENT

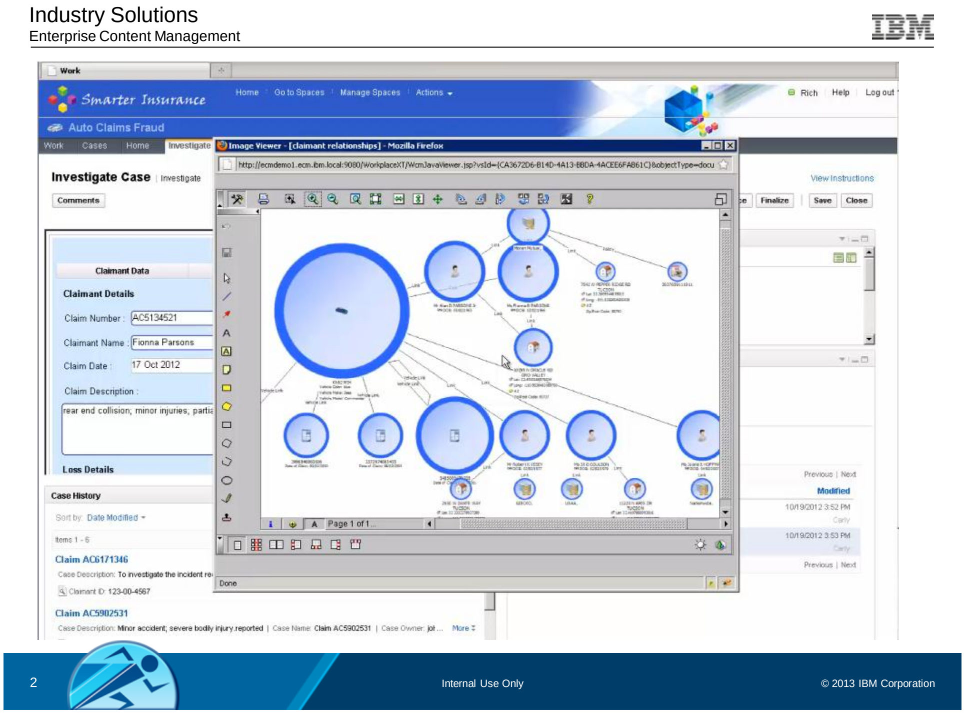
The case management layer of an investigation management system helps insurers build information over the course of an investigation, share information with colleagues, and compile cross-functional case data. Some case management systems are limited in their ability to retrieve and store relevant documents from across the enterprise, however. 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 corporate fraud group see that there is also a case underway in the personal lines insurance special investigative unit focusing on the same individual. Once the case has been finalized, best-in-class case management systems also provide the ability to classify the loss and identify its root cause.

The classification capability is a very 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 resources. A challenge faced by many institutions that rely on legacy infrastructure is a binary approach to fraud write-offs. Often, the legacy solution charges the fraud loss against the claim type that was used in perpetrating the fraud but loses the root cause of the fraud incident. For example, if a claims adjuster colludes with a vendor to share in a payment for services not rendered or overbilled, legacy systems would classify the loss as “corporate fraud” but fail to note that adjuster/vendor collusion was the root cause. When it comes time to examine losses and determine where to prioritize fraud-prevention budget dollars, this lack of depth in data classification can lead insurers to put their money in the wrong place.

Another important consideration for insurers evaluating investigation management platforms is the degree to which the interface is intuitive and user friendly. All insurers have independently tuned processes and requirements, and the user interface should optimally provide the insurer with the ability to configure the system to its own unique roles or processes. The result should be a user interface that does not display extraneous 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, which adds up and, over time, directly contributes to the expense line (Figure 2).

Finally, a flexible investigative work model is important because of the dynamic, nonlinear and human-centric nature of the process. Investigation teams require the ability to launch, assign, track, and complete their work within the unique context of each case. The work model should combine support for automated, orchestrated work with support for user-created, evolving work.

Figure 2: Sample IBM Case Management Screenshot



Industry Solutions
Enterprise Content Management

Investigate Case | Investigate

Claimant Data

Claimant Details

Claim Number : AC5134521

Claimant Name : Fionna Parsons

Claim Date : 17 Oct 2012

Claim Description : rear end collision; minor injuries; partia

Loss Details

Case History

Sort by: Date Modified

Items 1 - 6

Claim AC6171346

Case Description: To investigate the incident re

Claimant ID: 123-00-4567

Claim AC5902531

Case Description: Minor accident; severe bodily injury reported | Case Name: Claim AC5902531 | Case Owner: jot ... More

Image Viewer - [claimant relationships] - Mozilla Firefox

http://ecmdemo1.ecm.ibm.local:9080/WorkplaceXT/WcmJavaViewer.jsp?vsId={CA3672D6-B14D-4A13-BBDA-4ACEE6FAB61C}&objectType=docu

Page 1 of 1...

Done

Modified

10/19/2012 3:52 PM Carly

10/19/2012 3:53 PM Carly

2 Internal Use Only © 2013 IBM Corporation

Source: IBM

DASHBOARD MANAGEMENT

Dashboard management tools provide rich sources of management information system reporting that help proffer 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. The software also increases transparency, capturing all activity on the case and providing an audit log and change history. Information is power, and dashboard tools are important contributors to decision-making across the organization.

LINK AND PATTERN ANALYTICS

Through the use of applied analytics, carriers are using technology to reduce fraud through new, powerful capabilities such as link and pattern analyses. Fraud analytics encompasses multiple techniques to detect potential fraud, including automated business rules, predictive modeling, text mining, database searches, exception reporting, and network link analysis. Alerts can be scored and prioritized based on severity, then routed to appropriate case investigators who are able to perform more in-depth reviews to determine whether the claim in question—or any associated historical claims—may be fraudulent.

TEXT ANALYTICS

Content analytics is a powerful tool for discerning important, actionable insights and anomalies and for triggering alerts. The increasing volume of unstructured electronic text pouring into carrier operations include email, applications, call center and claims file records, and social media information. Text analytics software contextualizes these vast and dispersed mountains of data and provides valuable insights, guiding recommended next best steps across multiple operations to accelerate and improve fraud detection, enhance customer experience, streamline workflow, improve product development, and generally enable more informed fact-based decision-making.

Analytics allows carriers to logically manage rules, models, and alerts for their investigators; helps users create and manage business rules, analytical models, and lists of known and suspicious actors; and assists in maintaining simple or complex routing and suppression rules. An important new application of analytics is social network analysis, which provides a network visualization interface that enables investigators to identify linkages among and between seemingly unrelated activities and uncover previously unidentified relationships.

When applied within the context of an intelligent investigation platform, link analysis allows investigators to go beyond just transaction- and account-level views to analyze all related activities and relationships in a holistic network dimension; further, it automatically identifies suspicious networks' behavior in the data. It also provides investigators with ready access to complete details on all related parties and networks and allows for text and image annotation against specific entities in the network.

BENEFITS: THE BUSINESS CASE FOR INVESTIGATION MANAGEMENT

While the investment in investigation management is not insignificant, a number of factors contribute to a successful business case.

- **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. Increased fraud detection translates directly into increased profits through lower claim and fraud costs.

- **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," thereby allowing insurers 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. These may be more difficult to quantify in a business case, but they are important from a usability and workflow perspective.

- **Supervision:** Utilizing the workflow capability enables investigators to forward cases to supervisors automatically when reviews or approvals are required. Supervisors can perform their review and then return the case to the investigator with directions for additional efforts or forward the case on. Granting key managers access based on their role allows them to check the current status of a case and track 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 each investigator to focus on his/her work and handle more cases.

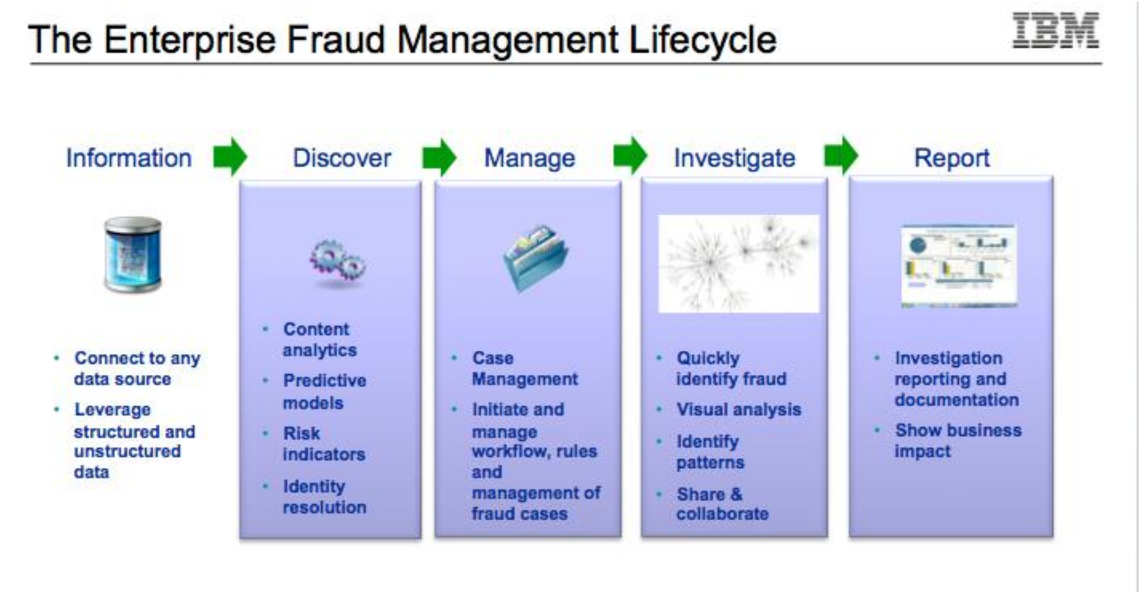
- **Compliance:** The workflow capability can also allow automation of many compliance requirements. Automated suspicious activity reports can be set up to allow internal reviews and approvals prior to the file being sent to reporting agencies. These types of capabilities are extremely important from a compliance perspective and provide the additional benefit of improving operational efficiency.

- **Management reporting:** The investigation management system enables automation of many reports, eliminating the need to manually pull data and manipulate it to create standard daily, monthly, quarterly, and annual reports. If the system allows input by job category of performance matrix data, individuals can monitor their own performance, allowing periodic reviews to become coaching sessions with no unpleasant performance surprises.

IBM INTELLIGENT INVESTIGATION MANAGER: INTEGRATED INVESTIGATION MANAGEMENT SOLUTION

Against this backdrop, IBM has a comprehensive platform for detection, prediction, analysis, and investigation of fraud. The diagram in Figure 3 below is IBM's depiction of fraud management lifecycle.

Figure 3: Fraud Management Lifecycle



The Enterprise Fraud Management Lifecycle

Information
- Connect to any data source
- Leverage structured and unstructured data

Discover
- Content analytics
- Predictive models
- Risk indicators
- Identity resolution

Manage
- Case Management
- Initiate and manage workflow, rules and management of fraud cases

Investigate
- Quickly identify fraud
- Visual analysis
- Identify patterns
- Share & collaborate

Report
- Investigation reporting and documentation
- Show business impact

Source: IBM

Products such as IBM Entity Analytics and SPSS enable fraud detection and prediction. IBM Intelligent Investigation Manager enables analysis and investigation of fraudulent cases.

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 the fraudulent activity and then act upon it.

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 the 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

CONTENT ANALYTICS

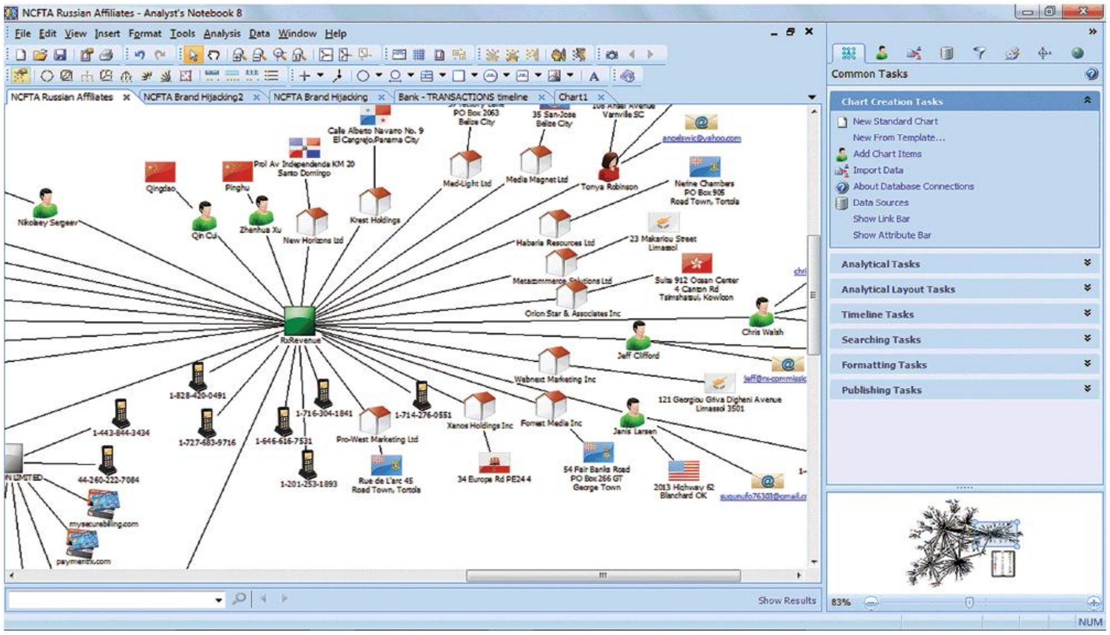
IBM Content Analytics offers the ability to use natural-language processing and other statistical and machine-learning techniques to extract facts, entities, concepts, and objects from vast repositories of unstructured or textual information. It searches and analyzes structured and unstructured information, extracting entities, patterns, and trends that accelerate the discovery process while identifying and investigating fraud. Its capabilities include the following:

- 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
- Analytics on identities and relationships are precalculated and perpetually updated
- Scales to big data volumes and is available for real-time text and content analytics

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 visuals that highlight the scope of the fraud, generate investigative leads, and provide evidentiary documentation (Figure 4).

Figure 4: IBM's i2 Link Analysis Capability



Source: IBM

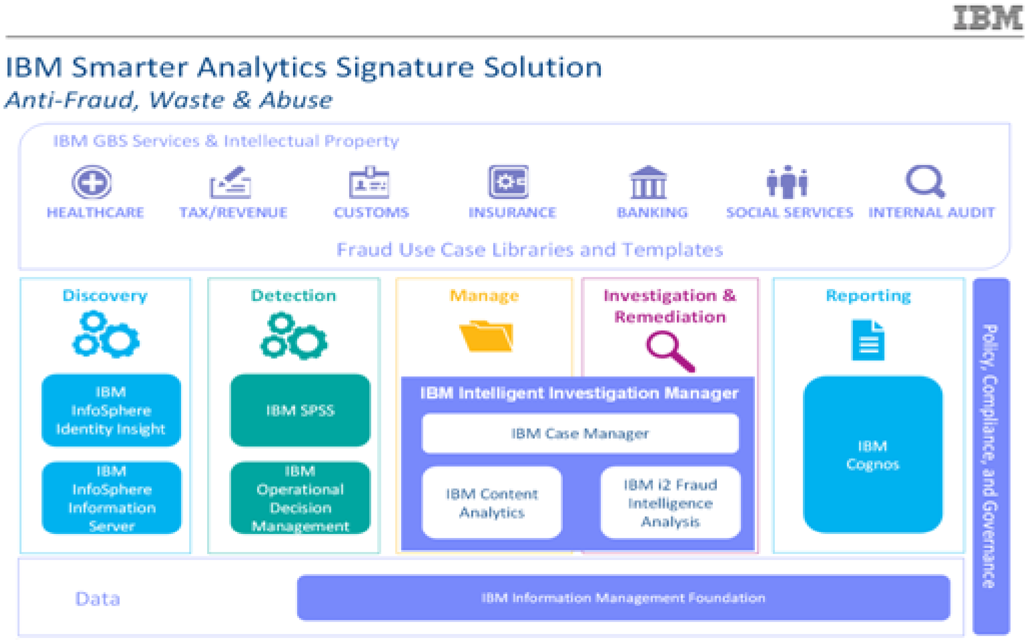
The IBM Investigation Manager can be used on its own, or within IBM's Smarter Analytics Signature Solution—Anti-Fraud, Waste and Abuse suite—to deliver an end-to-end fraud solution (Figure 5).

- **SPSS Threat Detection Analytics:** SPSS' advanced analytics provide insurers with 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 preempt 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
  - Planning and budgeting tools to improve process efficiency

Figure 5: IBM Smarter Analytics Signature Solution—Anti-Fraud, Waste and Abuse


IBM
IBM Smarter Analytics Signature Solution
Anti-Fraud, Waste & Abuse
IBM GBS Services & Intellectual Property
HEALTHCARE
TAX/REVENUE
CUSTOMS
INSURANCE
BANKING
SOCIAL SERVICES
INTERNAL AUDIT
Fraud Use Case Libraries and Templates
Discovery
IBM InfoSphere Identity Insight
IBM InfoSphere Information Server
Detection
IBM SPSS
IBM Operational Decision Management
Manage
Investigation & Remediation
IBM Intelligent Investigation Manager
IBM Case Manager
IBM Content Analytics
IBM i2 Fraud Intelligence Analysis
Reporting
IBM Cognos
Policy, Compliance, and Governance
Data
IBM Information Management Foundation

Source: IBM

INTELLIGENT INVESTIGATION PLATFORM USE IN INSURANCE

The number of use cases for intelligent investigation platforms within the insurance industry is as varied as the growing and constantly changing types of fraud being perpetrated and attempted. But at the highest level, these platforms enable carriers and their agents to more quickly and effectively investigate, predict, detect, and stop fraud before and after it occurs.

An intelligent investigation platform allows insurance users to:

- Consolidate raw data—including notes and customer statements—with related public-domain information and correspondence, including providers' bills
- Improve the productivity and effectiveness of precious investigation workers
- Discover and capture policyholder, claimant, and provider relationships
- Incorporate results of analytics and scoring tools applied to this information
- Add important additional case information collected over time
- Create extracts for central data repositories to enhance insights
- Create an effective, information-rich case referral for forensic analysis and additional field investigation
- Incorporate new case content gathered in such field investigations
- Prepare an evidence-rich package for prosecution

CONCLUSION

Insurers are deploying new and powerful fraud-detection solutions, but the effective management of the resulting tsunami of information requires an equally sophisticated investigation management solution that can consolidate case management, enterprise content management, business intelligence, advanced analytics, internal and external information, and social content. Nothing less than such an intelligent investigation platform will enable insurers to begin reducing the financial cost of fraud by allowing staff to quickly and efficiently triage fraud cases, identify the scope and complexity of the fraud, quantify the insurer's exposure, and distribute investigative referrals to the most appropriate resources. Below are a few recommendations for insurers looking to make this investment.

- **Get keen on quality.** This is a significant investment that will have a big impact on day-to-day operations, so don't compromise on quality. Look for solutions that have the following attributes:
  - Analytical firepower to help prioritize alerts
  - The ability to route cases and prioritize workflow
  - The ability to manage all content and data related to cases
  - A configurable, user-friendly interface
  - Automated regulatory filing for all countries in which your company operates
  - A dashboard that provides key metrics and management reporting
  - A robust link analysis visualization capability to identify costly, ring-based activity
- **Seek commitment.** As financial crimes and regulatory obligations grow increasingly complex, make sure you select a vendor committed to the long haul and willing to make ongoing investments and enhancements to the solution.
- **Include battlefield users.** As you create your vendor selection committee, make sure you're including representation from the investigator and analyst teams. These individuals are on the front lines using the technology every day, and they will be the best equipped to help identify needs and gaps at an early stage.
- **Cull data, enrich skills, and fine-tune workloads.** Ensure that you have (1) the best possible level of data quality to maximize analytics and (2) adequate and properly trained investigative resources. New skills will be required to leverage more sophisticated analytical results, and higher case-referral volumes typically result until proper tuning and workload balance are established.

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

Stephen Applebaum
+1.312.543.7198
sapplebaum@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:

Patrick Kilhaney
+1.718.522.2524
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com