Combating insurance fraud with Entity Analytics
Combating insurance fraud with Entity Analytics

Fraud has traditionally accounted for 10 percent of insurance company costs—but that percentage is rising: according to a FICO PCI Insurance Fraud Survey, 32 percent of insurers say fraud costs as much as 20 percent of their claims volume.1 While challenging economic conditions spur more individuals to pursue fraudulent activities, organized fraud rings are taking advantage of overworked insurance employees and a clogged court system to implement increasingly complex schemes. Insurance companies are inadvertently paying out more fraudulent claims while having to divert more resources to the identification, investigation and prosecution of fraud.

Addressing these trends is critical. With operational costs already cut and low interest rates limiting investment returns, insurance companies cannot afford to ignore the cost of fraud. They must identify fraud before a claim is paid in order to control loss in a highly competitive global market. Fortunately, advanced analytics technologies available today can help companies better predict, discover and prevent fraud while helping to expedite fraud investigations and prosecutions.

The Entity Analytics (EA) capabilities incorporated into the IBM® Anti-Fraud, Waste and Abuse Signature Solution for Insurance play a key role in combating insurance fraud by accurately identifying individuals, discovering complex relationships and finding links to fraudulent activity. This paper explores EA capabilities in the IBM solution and presents real-world use cases that highlight the value of EA in fighting fraud.

Envisioning the power of Entity Analytics

Entity Analytics can have a strong impact in preventing fraud across the claim lifecycle.

What if you could...

• Determine whether an individual is hiding his or her true identity at the point of interaction?
• Immediately discover hidden relationships among claimants, witnesses and medical personnel?
• Deploy automated alerts to underwriters and claims intake specialists to stop fraud before it happens?
• Gain new insight with each interaction to build a knowledge repository that can be used to predict and prevent fraud in the future?

Thwarting fraud with IBM Anti-Fraud, Waste and Abuse Signature Solution for Insurance

The IBM Anti-Fraud, Waste and Abuse Signature Solution for Insurance draws on a proven portfolio of IBM software, combining several advanced technologies and tools that enable insurance companies to:

• Correctly identify people and organizations, and determine how they are linked to one another and to possible fraudulent cases
• Prevent fraud at the time of policy submission and claims intake by providing alerts for suspicious people or activity
• Discover and predict fraud by examining behaviors and comparing normal actions to abnormal actions
• Visualize patterns, hotspots and relationships among people, policies, claims, vehicles and other entities to streamline investigations, build fraud cases and continuously improve antifraud efforts
Unlike point solutions that address only a single step in the process or provide a simple score, the IBM solution integrates multiple capabilities in an end-to-end solution for addressing fraud across the entire claim lifecycle.

**Defining Entity Analytics**
EA is an essential component of the IBM solution. Provided by IBM InfoSphere® Identity Insight, EA is the methodical process of detecting like and related entities across large, sparse and disparate collections of data—including both new (just arriving) and old (already stored) data—to perform analytics on information about people, events, things, transactions and relationships. Advanced technologies establish nonobvious connections among those entities and then provide real-time insights needed to make informed decisions rapidly.

**Detecting like entities**
Through an ongoing process of collecting and incorporating new information, EA helps organizations determine whether two records are really the same entity.

**Detecting related entities**
EA also discovers relationships among entities, whether those entities are people, policies, claims, cars or something else, out to multiple degrees of separation.

**Analyzing large, sparse and disparate data**
IBM EA capabilities can analyze large volumes of data with up to billions of records. These capabilities can also analyze data from sparsely populated records and disparate systems. By integrating all that data, organizations can gain a fuller picture of identities and relationships.

**Including old and new data**
IBM EA capabilities are designed to operate in real time, analyzing information as it is received by an organization to support in-line processes. At the same time, the EA capabilities analyze data from legacy or stovepipe systems to provide the context needed for understanding and managing the newly received data.

**Performing analytics**
The IBM solution doesn’t just stop with a map of entities and networks. Analytics such as collusion detection, role alerts and event alerts direct your attention to behaviors in the information. Those behaviors can be whatever you are interested in viewing, such as:

- If a person is reported as a victim or a witness across multiple claims
- If there is a relationship among several individuals across several claims
- If a claims officer is involved in a claim in a collusive manner

**Building knowledge with Context Accumulation**
EA depends on a process called Context Accumulation to determine like and related entities. As information is collected, the software relates new data to existing data, providing a way to learn from each new bit of information received. Context Accumulation enables organizations to improve the accuracy of entity identification, the understanding of social networks and the predictive modeling that draws on entity information.
The value of context accumulation is clear when compared to traditional matching or merging. With traditional matching, a system might examine the name, address, date of birth, social security number or other information from two records. Depending on whether the two records meet particular criteria for a match, the two records might be linked—and designated as a single entity—or not. In either case, the matching process ends until a new event triggers it again. Any variations on the name, address, date of birth, social security number or other attributes that are deemed to be incorrect are eliminated from the record.

By contrast, context accumulation collects information with every match attempt and system lookup. For example, the software might determine that two entities are the same, despite a variation of the first name or a transposition of numbers in the date of birth. When the records are linked or merged, all of the variations are retained, as is any additional information—such as information pertaining to associations with other people or events. When this is done, the two records together will form a greater context that might allow a third or fourth record to link in as well. All of this information may become useful over time.

Self-correcting false positives
As the software collects information, it automatically corrects previous false positives. For example, a company might have two records for men who share the same name, address and phone number. The software makes the assertion that these records represent one person and links the records together. At some future point, however, the company might receive information that the men in each of these records have two different dates of birth. The software automatically corrects the previous assertion that these records reflect the same person, creating two distinct entities and establishing a father/son relationship between the two. This continuous process of making assertions and correcting previous assertions based on newly acquired information happens automatically, without administrator intervention.

Crossing cultural boundaries with IBM InfoSphere Global Name Management
InfoSphere Identity Insight uses InfoSphere Global Name Management to help identify names of people and businesses. InfoSphere Global Name Management draws on a patented linguistics-based approach to name matching. It incorporates culture-specific rules about how names are parsed and spelled, performs name matching against lists and other data sources, and scores results that consider the similarity of pronunciation. It also handles transliteration from a variety of languages that do not use a Latin alphabet. These capabilities enable organizations to correctly identify individuals and resolve aliases even when administrators are unfamiliar with typical nicknames, gender associations with certain names or the use of surnames in place of first names in certain cultures.

Establishing relationships
In addition to determining the identity of individuals, groups and businesses, IBM EA capabilities help chart social networks. The software extends social networks to multiple degrees of separation and automatically presents this intelligence to IBM i2® Analyst’s Notebook®, providing an easy means of visualizing those networks for investigators (see Figure 1). Insurance companies can quickly find associations with suspicious individuals—including known fraudsters or other criminals—and find nonobvious connections among individuals.
Incorporating event information

As insurance companies receive new information about entities and their social networks, InfoSphere Identity Insight goes beyond basic EA by collecting additional contextual information, including information pertaining to noteworthy events and activities. InfoSphere Identity Insight automatically reassesses the data and draws new conclusions in real time, giving all users access to the most current insights. Using complex event-processing capabilities, insurers can track activities and discover suspicious patterns that might indicate fraud.

Figure 1: InfoSphere Identity Insight provides deep and broad real-time intelligence for visualizations of social networks that help organizations quickly determine whether a policy applicant or claimant is associated with suspicious individuals or known fraudsters.
Seeing Entity Analytics in action
With Context Accumulation, each new bit of information is like a piece of a puzzle. Taken alone, one puzzle piece might not be very helpful. But as additional pieces are collected, the relationships among puzzle pieces start to become clearer and the full picture begins to emerge. Organizations can improve the accuracy of identities, gain insights into key relationships and improve predictive modeling.

EA can help prevent and detect fraud at multiple points in the insurance claim lifecycle.

Underwriting
Suppose that “Bobette Lawry” applies for an auto insurance policy. As shown in Figure 2, the software immediately examines the input information and determines whether there are similar entities already in the system. In this case, the software recognizes that “Bobette” is a frequently used Latin nickname for “Roberta.” It finds that a record already exists for Roberta Lawrence (similar to “Lawry”) with the same phone number and date of birth. The existing record also notes that Roberta Lawrence’s policy was cancelled three months previously due to a conviction for driving under the influence (DUI).

Some information between the two records is not the same. For example, a few numbers in the vehicle identification number (VIN) have been transposed in the new record. InfoSphere Identity Insight links the two records, since they likely represent the same person, but retains the information about the nickname, last-name alias and distinct VINS. This process occurs in real time and generates an alert that is delivered to an underwriter before a new policy is created.

Entity Analytics: Putting the puzzle pieces together

Bobette Lawry requested auto policy

Bobette Lawry has shared the same phone number, date of birth and vehicle ID number as Roberta Lawrence

Bobette is a common Latin nickname for Roberta

Roberta Lawrence’s policy cancelled three months ago due to DUI

Figure 2: Taken alone, an insurance policy application from Bobette Lawry might not suggest fraud—but viewed in the context of other information, a new picture emerges.
Envision the benefits of Entity Analytics

A large insurance company processes more than 25,000 automobile insurance claims every month. The company wanted to speed the processing of non-fraudulent claims for valued customers while increasing the efficiency of fraud detection.

By implementing technologies designed to thwart fraud from IBM, the company:

- Increased subrogation recoveries by USD10 million
- Reduced time required for referring questionable claims for investigation by 75 percent
- Increased the success rate for fraudulent claims cases from 50 percent to over 80 percent
- Kept 25 percent of claims within the company’s first notice of loss area and sharply improved loss-adjustment expenses (LAE) ratio

Claim intake

Suppose that Drew French submits a USD35,000 claim on Mickey Sampson's homeowner policy due to a fall from Sampson's roof. The software finds a possible match with Andrew Thomas French, who has the same date of birth and phone number. Andrew Thomas French submitted a claim three months earlier for USD25,000 related to a fall from a roof.

The streets for the accident locations are different, but using geospatial analysis, the software determines that the two houses are in fact back-to-back in the same neighborhood. The software also finds that the treating doctors have the same last name, despite different first names.

A real-time alert is sent to the claims intake specialist, noting that “Andrew/Drew” has made more than one claim against related policies. The claim information is also sent to the fraud special investigation unit (SIU). During the investigation, the EA capabilities discover that the doctor has used various names for practices on other claims, signaling possible collusion in fraud.

Achieving a rapid return on investment with Entity Analytics

Insurance companies can begin seeing the benefits of EA even before the IBM Anti-Fraud, Waste and Abuse Signature Solution for Insurance is fully implemented. For example, organizations can quickly identify a large number of duplicate entities as soon as data is loaded. They can rapidly establish nonobvious relationships among entities and spot potential suspicious associations with fraudsters they have previously identified.

The value of EA grows when these capabilities are employed as part of the integrated, end-to-end Anti-Fraud, Waste and Abuse Signature Solution. Organizations can use the predictive analytics capabilities to identify behavior patterns and present anomalies compared with normal claims. They can use visualization and reporting capabilities to accelerate and streamline investigations by SIUs, which need to enhance their efficiency in order to successfully investigate the new fraud cases that EA will help identify.

Through Context Accumulation, InfoSphere Identity Insight gains knowledge as additional information is collected. As a result, the value of the solution increases over time as insurers gain the ability to better predict, discover and prevent fraud. At the same time, automation capabilities help reduce administrative costs associated with managing records and conducting investigations. And by better identifying fraud, organizations can accelerate processing of non-fraudulent claims, delivering a better experience for valued customers.
Getting started
Contact your IBM representative to arrange for a live demonstration of the IBM Anti-Fraud, Waste and Abuse Signature Solution for Insurance, and consider undertaking a proof of concept (POC) to see the identities and relationships hiding in your data.

For more information about the IBM Anti-Fraud, Waste and Abuse Signature Solution for Insurance, please visit: ibm.com/software/data/industry/insurance.html