IBM Anti-Fraud, Waste and Abuse Signature for Insurance

Combat insurance fraud using Entity Analytics and Context Accumulation

Highlights

- Detect like and related entities and locate nonobvious relationships
- Collect and retain valuable information using Context Accumulation
- Avoid losses and minimize recovery by predicting and preventing fraud

Insurance fraud is on the rise. Challenging economic conditions are spurring 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. Fraud has traditionally accounted for 10 percent of insurance company costs—but that percentage is rising as companies inadvertently pay more fraudulent claims and direct resources to the identification, investigation and prosecution of fraud.

IBM Anti-Fraud, Waste and Abuse Signature integrates multiple advanced capabilities in an end-to-end solution designed to address fraud across the claim lifecycle. By accurately identifying individuals, discovering complex relationships and finding links to fraudulent activity, this solution helps insurance companies better predict, discover and prevent fraud while expediting fraud investigations and prosecutions.The IBM Anti-Fraud, Waste and Abuse Signature helps insurance organizations do the following:

- Correctly identify people and organizations, and determine how they're linked to one another or to possible fraudulent cases—a critical component in uncovering coordinated fraud rings
- Prevent fraud during policy submission and claim intake by providing alerts about suspicious people or activities, such as multiple claims by the same person for the same injury at similar addresses
- Discover and predict fraud by examining behaviors and comparing normal actions to abnormal actions

- Visualize patterns, hotspots and relationships among people, policies, claims, vehicles, addresses and other entities to streamline investigations, build fraud cases and continually improve antifraud efforts

Correctly identify entities using advanced Entity Analytics

Supported by IBM InfoSphere Identity Insight, Entity Analytics (EA) is the methodical process of detecting like and related entities across large, sparse and disparate collections of data—including new and previously stored data. EA then performs analytics on information about people, events, things, transactions and relationships. EA helps establish nonobvious connections among those entities and provides business leaders with the real-time insights they need to make informed decisions rapidly.

With EA, organizations can do the following:

- **Detect like entities:** Determine whether two instances are truly the same entity through an ongoing process of collecting and incorporating new information.
- **Detect related entities**: Discover relationships among entities—such as people, places, events, accounts, transactions and more—even when there are multiple degrees of separation between entities.
- **Examine large data volumes**: Analyze data volumes having up to billions of records, and analyze data from sparsely populated records and disparate systems. Integrating that data provides a fuller picture of identities and relationships.
- **Include old and new data:** Analyze new data in real time, and data from existing or stovepipe systems that provides the context needed for understanding new data.
- **Conduct advanced analytics**: Examine events, behaviors and the roles of individuals to generate new insights into the relationships among entities.

Build knowledge using Context Accumulation

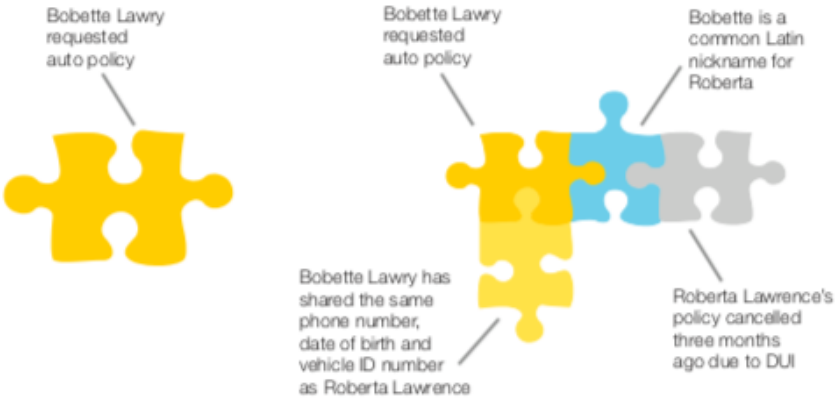
EA uses a process called Context Accumulation to help determine like and related entities. As information is collected, the software relates new data to existing data, learning from each new piece of information received. Context Accumulation enables organizations to improve the accuracy of entity identification, the understanding of social networks, and the predictive modeling that draws on entity information.

Traditional matching and merging examines attributes of records—such as name, address, date of birth or Social Security number—and then determines whether those records should be linked. The matching process ends and is reinitiated when a new event triggers it. Any variations

on attributes deemed to be incorrect are eliminated from a record.

By contrast, Context Accumulation collects information during every match attempt and system lookup. When the records are linked or merged, the variations are retained, along with any additional information—such as information pertaining to associations with other people or events. This information may become useful later. The newly linked or merged records, along with this retained information, provides greater context for linking with additional records.

With Context Accumulation, each new bit of information is like a piece of a puzzle. Taken alone, one puzzle piece might not be helpful. But as additional pieces are collected, the relationships among puzzle pieces start to become clearer and the full picture begins to emerge (see Figure 1). Organizations can use these capabilities to improve the accuracy of identities, gain insights into key relationships and improve predictive modeling.



Taken alone, an insurance policy application from Bobette Lawry might not suggest fraud—but in the context of other information, additional connections emerge to form a more complete view.

Move beyond traditional identification approaches

Organizations can use InfoSphere Identity Insight EA capabilities with Context Accumulation to help them move beyond traditional approaches to identify entities and simplify identity-related business processes.

Automate false positives corrections

As the software collects information, it automatically corrects previous false positives. It will create two distinct entities when necessary and establish a relationship between the two entities if a relationship exists. The continuous process of making and correcting assertions based on newly acquired information happens without manual administrator intervention, saving time and reducing the chance of data entry errors.

Work across cultural boundaries

InfoSphere Identity Insight uses InfoSphere Global Name Management to help identify names of people and businesses from across the globe. The software combines a patented linguistics-based approach to name matching, culture-specific rules about how names are parsed and spelled, and capabilities for handling transliteration from languages that don't use a Latin alphabet. The solution can help identify individuals and resolve aliases even when names are unfamiliar to administrators.

Establish relationships

IBM EA capabilities also 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, which uses linked webs and other graphical interfaces to visualize the relationships between entities.

Incorporate event information

InfoSphere Identity Insight collects a range of additional contextual information, including noteworthy events and activities such as creating new policies or filing new claims. This context enables the software to quickly identify and react to events as they enter the system. For example, if there's a known pattern between a certain fraud ring and the rate at which new policies are opened and new claims are submitted, InfoSphere Identity Insight can detect the associated events, recognize the pattern when it occurs and alert the appropriate investigators and systems. It then automatically reassesses the data, drawing new conclusions in real time and providing all users with access to the most current insights.

Achieve a rapid return on investment using IBM solutions to fight fraud

The IBM Anti-Fraud, Waste and Abuse Signature solution offers insurance companies a partner in the battle against fraudsters. EA capabilities help insurers quickly identify a large number of duplicates, establish nonobvious relationships among entities and spot potential suspicious associations with known fraudsters. Predictive analytics capabilities help organizations identify behavior patterns and present anomalies compared to normal claims. Fraud investigators can

use the visualization and reporting capabilities to accelerate and streamline their inquiries—a valuable benefit that provides organizations with greater efficiency.

The value of the solution increases over time through Context Accumulation. Insurers gain the ability to better predict, discover and prevent fraud by finding previously unseen relationships and connections between people and events in their networks. Automation capabilities help reduce administrative costs associated with managing records and conducting investigations. And by better identifying fraud, organizations can accelerate processing of nonfraudulent claims, delivering a better experience for valued customers.

Why IBM?

IBM offers a comprehensive, scalable Unified Governance and Integration platform and solutions—available on premises, on cloud and hybrid environments—successfully delivering trusted data for insights and compliance to businesses, governments and individuals. Learn more about Unified Governance and Integration at ibm.com/unified-governance-integration. Follow us on Twitter at @IBMAnalytics, on our blog at ibmbigdatahub.com and join the conversation #IBMUGI.

Learn more about IBM Unified Governance and Integration Solutions.

For more information

Contact your IBM representative or IBM Business Partner to arrange for a live demonstration of the IBM Anti-Fraud, Waste and Abuse Signature solution, and consider undertaking a proof of concept 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, visit: **ibm.com**/software/data/industry/insurance.html.

To learn more about Entity Analytics and Context Accumulation for insurance, download the IBM white paper “Combating insurance fraud with Entity Analytics” by visiting: http://ibm.co/13FdLI7