saffron

CASE STUDY

Detecting and Reducing Cost of Fraud Rings

BACKGROUND

The insurance industry estimates that 10 to 15 cents of every dollar paid in premiums goes to paying fraudulent claims, totaling more than $1.3 billion each year. In fact, nearly $80 billion in fraudulent claims are made annually in the United States. Within the insurance industry, fraud can span from opportunistic individual claims to organized multi-million dollar rings that involve staged auto accidents and participating medical equipment providers and clinics.

The speed and sophistication at which new fraud techniques are emerging create major challenges for today's fraud detection systems to keep up; it involves building new models, creating new dictionaries, and performing new training. Relevant information to detect and prevent these crimes is more spread out, or "siloed," than ever; such data are found not only on the open web and in insurance databases, but also in social media. In addition, the growing number of parameters used by institutions to identify individual claims increases the difficulty to "match" new claims against existing ones in order to identify possible commonalities.

The current tools available to insurers cause them to miss a significant number of fraudulent claims and cause investigators to expend valuable resources sifting through many alerts that have little to no value. Heavy caseloads and expectations for efficient claim processing often reduce the time adjusters spend with each claim. Today's special investigative teams within insurance companies are overwhelmed with new cases; as a result, these teams detect only 1% to 3% of the 10% of claims that are likely to be fraudulent.

CHALLENGE

A leading insurer contacted Saffron with a challenge: reduce its multi-billion dollar expenditures on auto insurance claims, which is its largest annual expense. Currently, the company avoids paying out only about 0.33% of the predicted 10% of fraudulent claims.

The insurer uses both manual (60-65%) and automated systems (30-35%) to flag questionable claims. These claims are passed on to the investigative case managers who read adjuster and other member notes, explore the fraud watch list, and search the web.

Existing methods prevent the investigative team from detecting fraud rings because they do not have a complete view of the connections between insurance members, providers, claims, and other entities in the data. The inability to view existing claims, while systematically looking across claims from present or past years, further prevents these teams from discovering relevant knowledge of possible colluding entities. As a result, their existing approach cannot easily discover fraud rings or, more importantly, collusion among other fraud rings.

IN LESS THAN A MONTH, SAFFRON EXAMINED 113,000 CLAIMS FROM 1 YEAR IN 1 STATE AND FOUND 3 POTENTIAL FRAUD RINGS.

Moreover, the investigative team typically decides in 30 days or less on whether to pay or deny a claim. This is due to heavy caseloads and expectations for a quick turnaround in claim processing in order to keep customers satisfied.

The insurer asked Saffron to find a more effective way to prioritize questionable claims (i.e. the individual claims with the most financial exposure) and understand the associations across all entities within claims to detect fraud rings.

SOLUTION

Saffron worked with the insurer for ten weeks to find hidden associations and detect fraud rings. The Natural Intelligence Platform ingested data from three states within the last three years, including auto injury claims (structured data) and MSR notes (unstructured data). Composite memories were created for each claim and similarity analysis was used to provide the insurer insight into data they had not previously seen. Saffron's associative memory "learns" from legacy claims and new claims; this allowed investigative teams to see patterns and similarities of providers across all claims and easily identify fraud rings.

For example, Saffron discovered that a radiology clinic from the investigative watch list was actually part of a much larger fraud ring and a common link that connected three potential fraud rings together. The clinic was previously identified as fraudulent for MRI overcharging, but the investigative team could not view the clinic's possible connections with other providers. Using Saffron's "reason by similarity" analysis—where every claim (and associated actors) has a unique, individual signature—Saffron's Natural Intelligence Platform illuminated all hidden connections to that particular clinic as well as the other colluding rings.

RESULTS

Over a 10-week period, Saffron examined 113,000 claims (structured data) from one year in one state and found three potential fraud rings, warranting further investigation, in less than a month. Under further investigation, Saffron detected that these three rings were part of one larger ring that included 38 claims and 42 participants from various provider entities such as psychologists, acupuncturists, physical therapists, physicians, and durable medical equipment providers. From these 38 claims, the insurer paid out approximately $400k to questionable providers of the $700k that was billed.

Saffron forecasts that the insurer can avoid a payout of $10s of millions a year given that Saffron's unique cognitive computing approach can potentially detect multiple fraud rings across each state in a given year. Of the $630 million fraudulent auto injury-related claims that the insurer pays out each year, at least 10% might be fraudulent in nature. According to the insurer, every 0.1% increase in avoidance payouts results in a $10 million addition to the bottom line.

HOW IT WORKS

The insurer provided Saffron with select data sets from disparate sources, both structured and unstructured. Saffron's data ingestion tool carried out an ETL process of unifying diverse data at the individual entity level. This enabled the insurer to see a representation of how each person, place, thing, or event was associated, along with the numeric or semantic context of each of these entity relationships. Importantly, Saffron also illuminated the most relevant interactions. Saffron's network of associative memories (called SaffronMemoryBase, or SMB) stored the knowledge that was discovered during data ingestion and created pre-joined tables that could be queried with immediate results and could provide a template for instant and incremental learning as new data arrived in real-time. The data—represented as individual tables in the MYSQL database or as free text from adjusters' notes—became "associative memories." This enabled reasoning and predictive analytic applications such as "Similarity Analysis" which allowed the insurer to identify questionable claims, view supporting explanatory evidence, and add certain providers or organizations to a "watch list."

At the outset of this use case, Saffron and the insurer identified 42 entities out of thousands of entity categories to begin identifying relevant and unknown relationships in the data, including different providers, demographics, injury descriptions, and payments. To illustrate the high dimensionality of Saffron's network of associative memories, Saffron generated over a billion associations at an entity level, creating a new knowledge store that had never before been done. This allowed the insurer's Property & Casualty business division and its SIU investigators to comprehensively identify relevant associations across claims by the same provider or insurance member in real time as new claims were processed. This unique, nonparametric view of the data in a coincidence matrix also allowed them to query across claims. This novel view of the data enabled the facile identification of attributes used to find collusion rings, including provider names, provider addresses, tax id and social security numbers, and member demographics.

Saffron is also adept at delineating fraud-related aliases by automatically carrying out entity disambiguation. For example, Saffron can identify aliases based on duplicate tax id or social security numbers or detection of other less obvious shared attributes. Saffron makes custom API calls to its memory base to expose claims where two sets of people or organizations have previously worked together. Further, Saffron creates stored procedures of custom APIs, called “thought processes,” to query similar claims to an individual claim.

A “signature” is evidence that shows how claim A is similar to claim B because the same providers appear in both claims. Groups of providers that repeatedly appear in different claims are suspect. Saffron performs an exhaustive search of all claims to identify similar ones and provides the supporting evidence with weighted signatures and referenced content for such questionable claims. The insurer can view the output as an HTML table in Saffron Advantage (UI) or as a sortable CSV file. Saffron identified 14 providers working together on 45 claims as the most number of providers working together. The SIU team was asked to review this activity and check the provider names against the fraud watch list and investigate further.

The Natural Intelligence Platform enabled the insurer to have an “all-source intelligence” view across claims and all providers that are involved in one questionable claim. Saffron worked collaboratively with the insurer’s SIU Investigators to reveal the questionable providers in that claim, what they billed, what the insurer paid out on the claim, and the necessary supporting evidence to further investigate such questionable claims.

ABOUT SAFFRON

Saffron combines the power of computing with brain-like intelligence to make sense of data and help anticipate future trends, events and outcomes. The platform adapts in real time, ingesting data from disparate sources and automatically finding new patterns, similarities, anomalies or sequences, revealing previously undetected knowledge. Saffron enhances the speed and volumes at which data can be processed but also critically improves the accuracy of results. Businesses using Saffron can anticipate market trends, optimize processes, mitigate risk, personalize customer experiences and find new revenue streams. Founded in 1999, Saffron Technology is headquartered in Los Altos, California. For more information, please visit www.saffrontech.com.