Car re-birthing and insurance fraud

PeerAnalytics.com.au

My passion is solving puzzles. I start with a massive, jumbled heap of data, and I analyze it to identify people to target. I cultivated my expertise in the daunting field of criminal intelligence, where I developed methods for targeting suspects.

Over the years I have been involved in remarkable cases. The challenges have been steep. But the methods I developed were proven. They helped make the world a safer place.

My colleagues and I have started to apply those methods in a very different field—marketing—so as to greatly improve ways to identify people who are best to target for marketing messages. The result is a huge lift in response rates—including sales, product inquiries, clicks, market share, and retention—and therefore marketing ROI.

The methods are based on SNA (social network analysis) and predictive analysis identifiers of who will do what next. The SNA underpinning means we look for connections in the data. We also predict connections and influence flows between people and things such as addresses, phone numbers, websites, locations, and timings.

The analytical principles I developed and used to create SNA software is now used by the marketing departments of companies in telecommunications, apps messaging, finance, FMCG, and manufacturing. But before major companies began using it to effectively target customers, we had a significant presence in the insurance industry, rooting out and identifying the perpetrators of fraud.

Insurance fraud

The U.S. insurance industry pays out billions of dollars annually on fraudulent claims. However, identifying fraudulent claims is not an easy task. Most major insurers in the United States have turned to the software I developed in order to identify fraud cases.

In the matter of identifying insurance fraud, accuracy is crucial. Catching fraudsters is high priority for insurers, but falsely accusing legitimate claimants can be hugely damaging to business. They must identify and predict such criminal behaviour with a high degree of accuracy from vast amounts of data.

Software I developed based on the principles of SNA (as per Peer Analytics' SNA Predictive SaaS service) continues to play a major role in reducing claims fraud.

Before I developed my SNA software, it was not unusual for one person to make multiple claims to different insurance companies. For example, some "slip and fall" claimants would purposely "slip" and "fall" to injure themselves tens of dozens of times, often in retail stores or shopping complexes. Some drivers seemed to run into bad luck constantly—or, more accurately, they ran into other cars constantly (sometimes the same ones).

Those relatively straight-out multiple claims occur much less often nowadays, as computer systems can quickly pick up on the pattern that John Doe keeps injuring himself or crashing his vehicle, or always seeing the same doctor who treats him for injury or whiplash at great expense.

As computer systems evolved, fraudsters did, too. Many became adept at covering their tracks, making them far harder to find. However, an “all claims database” was established to overcome such scams. Nearly all U.S. insurance companies share its contents. The database covers ever-expanding numbers and types of claims, potentially involving almost all claims that occur in U.S. insurance.

This database is the chief source of data for the software I developed. The software combs through data to identify groups of items to red flag. At its simplest, it finds the links between multiple claims and one claimant. It also can determine relationships (often very indirectly) between a person and other fields, such as bank accounts, addresses, phone numbers, names and details of witnesses, claims history, and so on. These connections between the snippets of data and the patterns that connect them are critical for identifying an always-growing range of fraudulent activity.

Fraud rings can get quite complex. I remember a case involving staged auto accidents. For example, an innocent victim would be hemmed in by an outside car as the car in front of it braked suddenly, causing the rear car to run into it and be at fault.

The staging of the accidents was done by a gang of mainly Middle Eastern youth who, as the case unfolded, were found to be pretty small-fry. The staged-accidents racket was just a cog in a larger criminal organization. To wit, cars from staged accidents sometimes were directed to specific body shops for repairs. However, the body shops were actually chop shops—illegal “garages” where cars were disassembled and sold for parts. (Roughly half of all stolen cars are stolen for parts. If they’re found, what remains are mere skeletons. But many of them simply disappear altogether.)

In this case, cars at the body shop were given the identity of another vehicle, sometimes a stolen one but often one sold at an auto auction as a “write off” following an accident. The cars stolen for parts were stripped of their parts, which were either sold or used to create “new” cars. The “new” cars were sold at a considerable profit, often as luxury vehicles with low mileage to unsuspecting buyers.

The organization was impressive. The criminals had set up a web of fake documents (receipts, owners’ log books, VIN numbers) to submit to licensing authorities, along with parties willing to testify if needed.

But the operation, however complex and sophisticated, could not elude the software. The operatives in this case were successfully convicted.

Insurance of all types is subject to a percentage of fraudulent claims and payouts. But the software I developed continues to help reduce such instances of fraud—thereby keeping premiums affordable for the rest of the community.