FORCEPOINT
POWERED BY Raytheon

Use Case

Insurance Fraud

BECAUSE OF AUTOMATED CORRELATION AND CONNECTIVITY, INVESTIGATORS ARE BOOSTING THEIR PRODUCTIVITY BY SWIFTLY RECOGNIZING PATTERNS OF LARGE FRAUD NETWORKS, SOLVING MULTIPLE FRAUD CASES IN THE SAME TIME FRAME THAT IT PREVIOUSLY TOOK TO CLEAR A SINGLE CASE.

CHALLENGE

There's a plethora of data out there to help the insurance industry investigate and prevent fraud. However, when it comes to deploying technologies needed to maximize the impact of this data, adoption is hardly universal. According to a September 2014 report from the Coalition Against Insurance Fraud nearly all insurers (95 percent) said they use anti-fraud technology, compared to 88 percent in 2012, so while usage is on the rise, fraud is on the rise as well, and this increase is bolstering the need for fortified technology solutions. While most insurers employ basic anti-fraud tools (81 percent), such as automated red flags, far fewer employ more advanced technology such as link analysis (50 percent), predictive modeling (43 percent) and text mining (43 percent.) The study also found that insurers face a shortage of claims and anti-fraud professional personnel. Insurers today know the value of technology to their often understaffed teams, and cited the top benefits of anti-fraud technology to be referrals (59 percent), higher quality referrals (69 percent) and improved investigator efficiency (41 percent.)

The story of insurance fraud is literally told by the names, addresses, phone numbers, social security numbers and claims compiled within insurance case management and other government-owned systems. But, without big data search and analytics, the story will continue to hide in plain sight. Without enhanced visualization into the wealth of information within the systems, crooks continue to make phony claims while pocketing thousands - if not hundreds of thousands - in illegal payments.

To thwart the growing criminal activity, a major state insurance fraud division took proactive steps to improve their security posture by boosting its big data capabilities. Their goals were:

To better leverage its internal case management data. Case management records contained a wide range of details about individuals, fraudulent claims, investigation summaries and arrests. But, with analysts confined to manual-based search processes, there was very limited opportunity to "connect the dots" within the records and detect criminal patterns linking these cases.

To gain access to external state databases that could elevate awareness. These include databases related to personal injury protection (which accounted for more than 650 false claims in fiscal

year 2012/2013, which is tops in the state), worker compensation (which is second, at nearly 420 claims), health department licenses, business licensees, Medicaid/Medicare fraud and unemployment compensation.

To automate searches of structured and unstructured data in both internal case management and external state sources. Automated queries would significantly reduce the time needed for complex searches. Unstructured data includes email exchanges, documents and social media postings. Also, because criminals often steal the identity of a dead person, access to the publicly available Social Security Death Index (SSDI) was mission critical.

SOLUTION

In 2012 the state insurance fraud division turned to the Forcepoint SureView Analytics platform, a proven big data analytics and information-sharing enterprise application. Its search tools give users immediate access to all existing data which provides a completely inclusive picture of a situation. With leading-edge federated searching, it swiftly connects and correlates any number of data sources – internal, external, structured or not – without duplicating the data. It facilitates interagency information sharing, automates repeatable procedures and rapidly executes queries. The tool is user friendly and adopted quickly across the enterprise as minimal user training and interaction is required for use.

RESULTS

The division is making ground-breaking connections within its case management database. Users easily construct intricate diagrams of related illegal activity, transforming daily tasks from a 'single suspect' focus, to 'networked' incident discovery. If a home address is shared by four different people who have made fake personal injury protection claims, SureView Analytics helps users detect it. If dozens of illicit worker compensation instances emerge within the same small business, users quickly uncover that as well. Because of automated correlation and connectivity, investigators are boosting their productivity by swiftly recognizing patterns of large fraud networks, solving multiple fraud cases in the same time frame that it previously took to clear a single case.

With the Forcepoint SureView Analytics platform, division officials have developed a remarkably efficient and cost-effective way to access information they need from external state databases. Unlike the competition that require the external state data to be captured and moved to a proprietary server, SureView Analytics does not, therefore, users access information from the business licensing bureau on a "read only" basis. No more filling out elaborate and time consuming "memos of understanding" requests to obtain the data. Eliminating this step is saving the division hundreds of thousands of dollars.

Now that queries are automated, what was once a time consuming manual process is now accomplished in a matter of minutes. SureView's "Big Button" dashboard allows users to instantly conduct a search for actionable information throughout every accessible database with one click. This goes for mobile users too, which is mission-critical for the division, given that investigators often must input queries while out in the field on cases.

Forcepoint's SureView Analytics platform, based largely on entity-based analytics, has made a significant contribution to the division's efforts to fight insurance fraud. Optimization of the firm's ability to unearth relationships between perpetrators and organizations, along with the benefits of working with near real-time information helps the division to stay ahead of the acceleration in suspicious activity and fraud.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[USECASE_ANALYTICS_INSURANCE_FRAUD_EN] 300064.030117