splunk>

Unleashing the power of data analytics: **Winning the war on fraud in state benefit programs**

Millions of Americans rely on state and local government-administered benefits to survive. However, since the beginning of the COVID-19 pandemic, these programs have experienced an unprecedented surge in fraud attacks.

As government agencies rushed to distribute funds that provided emergency relief for citizens in 2020, they struggled to balance quick administration with implementing proper controls and payment verifications. It was challenging to hire enough staff to handle and assess the sudden influx of claims, making it easier for fraudsters to exploit the system.

Unemployment insurance was the biggest target, as departments of labor throughout the country received the highest amounts of federal funding to stave off the effects of spiked unemployment rates. So far, the repercussions are troubling. The Government Accountability Office estimated that between 11% and 15% of unemployment payments made by states during the pandemic were fraudulent — a loss totaling around $100 to $135 billion.

"When we look at the total cost of fraud for each state or within each program, we can only quantify the total dollars lost when there's a means to track fraud," explains Tina Carkhuff, public sector industry advisor for Splunk, a leading data software company. "That's disheartening because if an agency doesn't have the controls in place to detect fraud, they may not know how much money is being lost."

Fast-forward to today: Threat actors and organized groups not only continue to defraud critical benefits programs like unemployment, pensions, Medicaid, senior services, and food assistance, but their methods become increasingly sophisticated.

Unfortunately, organizations often operate with incomplete or outdated constituent data, making it difficult to determine payment eligibility. Additionally, a lack of visibility between federal agencies and states can result in duplicate benefits claims and overpayment.

"Resource constraints can force agencies to make decisions about whether to pay a claim before they should," states Carkhuff. "They can't always explore all of the information about a claimant because they simply just don't have the staff to do it."

Moving forward, it's critical for state and local governments to equip themselves with the right tools to properly detect and prevent schemes. Carkhuff states that the key to lifting the burden off swamped employees and bolstering program integrity — or, ensuring appropriate use of taxpayer dollars to deliver quality and necessary care while preventing fraud, waste and abuse — lies in data analytics.

"We still have a handful of agencies that are reviewing data with only humans, and it's almost impossible for them to keep up," says Carkhuff. "Data analytics decreases the time it takes to detect fraud at scale."

When we look at the total cost of fraud for each state or within each program, we can only quantify the total dollars lost when there's a means to track fraud. That's disheartening because if an agency doesn't have the controls in place to detect fraud, they may not know how much money is being lost.

Tina Carkhuff, public sector industry advisor, Splunk

Splunk's strategy: Bridging technology and human expertise

Splunk's application for fraud features cutting-edge data analytical capabilities specifically developed to support human counterparts. Splunk's philosophy is that humans must always make the final decision about program integrity, and whether or not a claim meets proper eligibility criteria.

"Academic research has shown that the capability of humans paired with the capability of data analytics is the right foundation for the most effective fraud detection and mitigation strategies that will help governments hold on to their funds, especially those most critical for residents in need," says Carkhuff.

Human investigators can easily examine a single, specific claim for benefits or a resident account to determine if a payment is legitimate. Splunk's data analytics can provide necessary context to that decision-making process by sifting through metadata surrounding that claim and providing additional information, such as the Wi-Fi network used to process the request or the computer that sent the request to better verify the claimant's identity.

Taking it a step further, these tools can also pull in aggregate data to provide, for example, a comparison of all other claims within the same date, week or month, giving investigators the large-scale picture needed to accurately identify suspicious activity.

"The computational abilities of Splunk are designed to search through any type of data, regardless of its source, and find patterns, trends and anomalies in that data that would otherwise be impossible to detect," says Carkhuff.

Splunk's work with the state of New Jersey highlights the power of these capabilities. In April 2020, the state's Department of Labor deployed the company's data services after realizing it was receiving more unemployment benefits claims than residents in the state. Splunk's platform reviewed all claims and provided a risk-based analysis that scored each one so investigators could easily determine which claims had a higher likelihood of fraud.

"What was so useful to the state of New Jersey is Splunk's ability to review data across multiple claims," explains Carkhuff. "So if a bad actor used the same bank account number or other shared data across hundreds of claims, those claims immediately rose to the top for the investigators to review."

Splunk ultimately helped New Jersey save over $7 billion in potential fraud losses.

The company is currently working to implement similar successes and strengthen program integrity for various other public sector organizations, including tax agencies, educational institutions, pension systems, health benefits, SNAP food benefits, among others.

"While fraudsters are more sophisticated in the way that they commit fraud, our technology continues to grow in ways that we're detecting it," says Carkhuff. "We're not on the losing end of this. It's a complicated problem, but it's certainly one where data analytics is the answer to the problem."

Learn more about how Splunk can help your organization combat fraud and strengthen program integrity.

Academic research has shown that the capability of humans paired with the capability of data analytics is the right foundation for the most effective fraud detection and mitigation strategies that will help governments hold on to their funds, especially those most critical for residents in need.

Tina Carkhuff, public sector industry advisor, Splunk