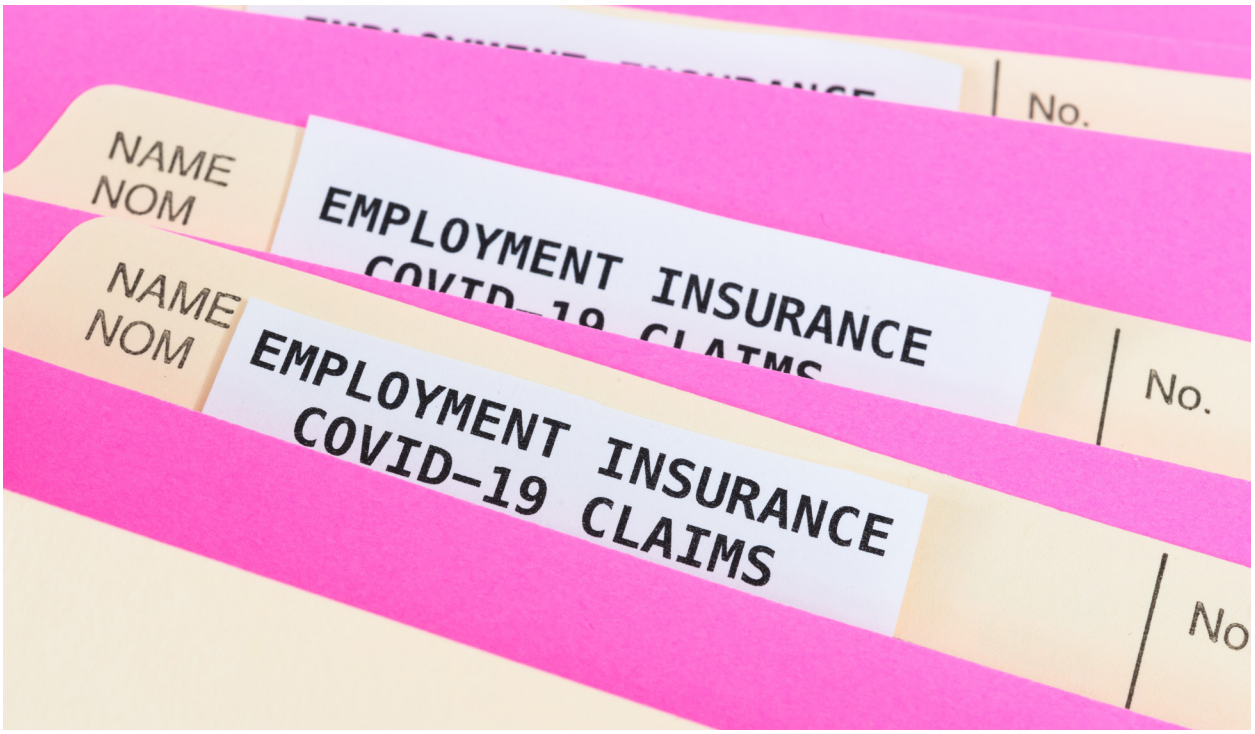
Protecting the Payments

As unemployment insurance claims increased dramatically because of pandemic job losses, so did incidents of fraud grow exponentially in federal and state government systems

With the increased number of unemployment claims and the CARES act changes, identity theft cases have skyrocketed over the last two years. Organized gangs of international hackers targeted state agencies and their aging IT systems. Estimates of the amount of money lost run close to $90 billion.

The solution for many state agencies has been the use of artificial intelligence and data analytics to identify suspicious behavior and flag questionable accounts. States are also sharing UI claims data in an online exchange system, and others are requiring a dual authentication process to reduce fraud and abuse of the systems. But they all recognize the need to be able to monitor large volumes of claims and the patterns of data that signal fraud.

PRODUCED BY: GCN | sas



Yelena Rodriguez Mena / istockphoto.com

'A Significant Wave of Modernization' Coming to Unemployment Systems

More than $87 billion in fraudulent unemployment claims were filed with states nationwide since the pandemic began, which is prompting states to overhaul their antiquated systems.

BY SHARON O'MALLEY FOR ROUTE FIFTY

In February 2020, just weeks before the World Health Organization declared Covid-19 a pandemic, 3,000 Kansans filed unemployment claims. By the end of March, that number jumped to 66,000 and continued to skyrocket over the next year.

Approximately 56% of those claims were potentially fraudulent.

The state paid about 30% of the probable bogus claims—to the tune of $700 million—but caught onto the other 70% before the fraudsters collected any money, potentially saving up to $2 billion. And now, at the behest of the state legislature, the Kansas Department of Labor is overhauling the antiquated computer system that processes its unemployment insurance claims.

"I wouldn't say it's over," Matt Etzel, a principal auditor with the Kansas Legislative Division of Post Audit, said of the increasing and increasingly sophisticated attempts to defraud federal and state governments through phony unemployment insurance claims.

Kansas isn't the only state committed to modernizing the 1970s- and '80s-era code that runs many UI networks, redoubling the use of data analytics to spot telltale patterns in fraudulent claims, and investing in artificial intelligence and other state-of-the-art technology that might outsmart—or at least outpace—those who would cheat the system.

State-by-state forensic work will uncover just how much money was lost to UI fraud during the worst of the pandemic,

although a conservative estimate from the U.S. Department of Labor's inspector general put it at $87 billion-plus nationwide by September 2021, when the federal government stopped adding $600 a week to UI checks.

Meanwhile, states with auditors and lawmakers who believe future disasters could invite a repeat of the record-setting fraud will invest millions of dollars in technology to prevent it, predicted Shaun Barry, director of fraud and security intelligence for government and health care for data analytics vendor SAS.

"Many of them use … four to five generations of technology removed from state-of-the-art today," Barry said. "Those systems are fragile and brittle and so old that they don't have the robust accounting controls that are available today. … States have known for many years that they have fragile [information technology] systems."

Over the next five years, Barry said, state UI agencies will embark on "a significant wave of modernization in accounting systems. The pandemic has accelerated this modernization."

It All Started With the Pandemic

In Kansas and elsewhere, in fact, the pandemic got it started.

To determine how much UI fraud occurred during the 2020 and 2021 months at the heart of the pandemic, Kansas auditors dissected 1,000 claims—out of the million-plus it had processed—to detect patterns that could reveal fraud. What they found were multiple claimants using the same complex password; partially duplicated email addresses; and claims supposedly from state employees whose Social Security numbers did not match human resources records, among other red flags.

In the end, auditors identified 26 indicators of potential fraud, and then "trained" a neural network—a computer modeled after the human brain—to spot them.

"It got really good at replicating our ability," said Etzel, who noted that the computer made the same decision as the auditors did at least 91% of the time.

Barry said state systems need to overhaul their outdated equipment with that kind of top-shelf technology to prevent future fraud from occurring during another crisis.

Even the work of organized criminal rings of fraudsters, he said, "can be addressed by modernized accounting systems." He pointed to the success of commercial credit card companies that use artificial intelligence like machine learning, which involves automated systems like the one in Kansas that mimic the decision-making of the human brain, to flag suspicious claims.

As far back as 2013, a U.S. News & World Report survey identified 20 states that were at least dabbling in artificial intelligence to analyze UI claims.

Meanwhile, many states have ramped up their use of data analytics—collecting and analyzing large stores of data to identify suspicious patterns among UI claims. And some are cross-referencing their data with that of the federal government and nearby states to catch serial fraudsters who cross state lines, Barry said.

For example, California Gov. Gavin Newsom in October signed a law requiring the California prison system to share the names and Social Security numbers of inmates—who are not eligible for UI—with the Employment Development Department and ordered cross checking.

Six states—Georgia, Utah, New Jersey, Colorado and Ohio—have created an online data exchange system to share UI claim information. The Alabama Department of Labor, like several in other states, recently rolled out a dual-authentication system that helps to protect the identity of UI claimants.

Paradoxically, Oregon auditors credit the state's ultra-low UI fraud with its outdated computer system.

"It doesn't allow for online web claims like in California and Washington," Ian Green, audit manager for the Secretary of State Audits Division. "It doesn't immediately process stuff. It's a lot more manual and cumbersome, so if you tried to defraud in Oregon, you hit roadblocks … in our old system. In California, you'd get a payment the next day."

Green estimated the state lost "hundreds of thousands of dollars [to fraud during the pandemic] instead of in the hundreds of millions of dollars."

The downside, he pointed out, is that legitimate claimants often wait weeks or even months to get their checks.

Green's colleague, Senior Auditor Kathy Davis, called the reduced fraud "a silver lining to a really unfortunate situation."

Still, Oregon will update its systems by 2024, Green said.

Optimists Versus Pessimists

Barry predicted that some states will shy away from spending hundreds of thousands of dollars—or even millions—on cutting-edge computer systems.

"There are two competing narratives that are emerging on what the future holds for labor agencies," he said. "One is an optimistic view and the other is pessimistic."

The optimists, he said, will view pandemic-induced UI fraud as a one-time hit that will disappear if and when Covid-19 does. The pessimists, on the other hand, will expect a renewed surge of fraud with every future crisis.

"It looks like it will be 50-50 between optimists and pessimists," he said. "But if there's anything that state UI agencies agree with, it's that their UI system is antiquated and needs to be upgraded. But do I replace it with what I had before, or do I replace it and enhance it with UI defenses?"

Chombosan / Shutterstock

‘One-to-one unemployment insurance fraud investigations are over. Here’s what’s next.

BY LUTHER KLEIN, CARL HAMMERSBURG

Imagine for a moment that you’re a fraudster, and unemployment insurance (UI) fraud is your specialty. As the pandemic took hold in the U.S., you watched as unemployment numbers spiked. You took note as the government proposed and passed massive emergency legislation to provide unemployment benefits to millions of those put of out of work. You saw that the dollar amounts involved were enormous. The best part? Due to the contagious nature of the virus, everything had to be done remotely—not only did the government not require in-person signings or verifications, it eliminated them altogether.

This is a recipe for massive fraud—a point that wasn’t lost on those with state- and federal-level responsibility for preventing and uprooting it. They knew this was coming; it was only a question of when and exactly how it would take shape. In short order, government leaders updated their unemployment fraud defenses as best as they could and got ready for the coming tsunami.

That was in the spring and summer of 2020. Now with the benefit of some hindsight, we can see that despite their best defenses, state governments were simply unable to head off fraud at such a large scale. And as we settle into what may be a long haul of constantly fluctuating unemployment and continued uncertainty, it seems clear that a return to old ways of thinking about and managing UI fraud is not going to happen.

What have we learned?

So what have we learned in this period of expanded and accelerated fraud? Probably most important, it is now clear that the era of the “one claim, one investigation” approach to fraud management is over—the scope and volume of fraud cases

> THOSE CHARGED WITH UI OVERSIGHT NEED THE ABILITY TO MONITOR LARGE VOLUMES OF UI CLAIMS, REGISTRATION AND OTHER TYPES OF DATA TO IDENTIFY PATTERNS AND SIGNALS POINTING TO POTENTIAL FRAUD. JUST AS IMPORTANT, LARGE-SCALE ANALYSIS CAN HELP UNCOVER BROADER PATTERNS THAT ARE SIMPLY UNABLE TO BE IDENTIFIED ON A ONE-TO-ONE BASIS.

simply don't allow it. Those charged with UI oversight need the ability to monitor large volumes of UI claims, registration and other types of data to identify patterns and signals pointing to potential fraud. Just as important, large-scale analysis can help uncover broader patterns that are simply unable to be identified on a one-to-one basis.

What's next: Beyond "one claim, one investigation"

Fortunately, this is not a new category of challenge, even if some of these analytics capabilities are relatively new to state governments. Banks, for example, have been deploying large-scale antifraud analytics strategies for years, with positive results. State governments can and should be putting "quick strike" capabilities in place that allow them to begin improving fraud detection in as little as four weeks, drawing from capabilities developed in adjacent industries facing similar challenges. Here are the specific capabilities state governments should be putting in place today, if they haven't already:

Fraud vulnerability analysis

- Use internal and external data to prep rapid UI data requirements.
- Analyze existing processes to identify vulnerabilities.
- Develop recommendations for vulnerabilities for existing and new fraud schemes.
- Set action plans for remediating vulnerabilities.
-

Rapid detection platform

- Analyze internal data across multiple unemployment programs, claims, employer accounts and more, using advanced analytical models.
- Deploy link analysis capabilities for reviewing customer information and identifying clusters of suspicious activities.
- Deliver daily reporting and analytics dashboards to help identify trends, patterns and signals.
- Use scorecards to weigh analytical "scores" to prioritize investigative work.

Identity proofing and bot detection

- Centralize development efforts—including validation skills.
- Deploy global operating model using lower-cost resources to achieve scale.
- Standardize and streamline development, validation and governance procedures.

Integrated, real-time fraud detection

- Embed event-driven fraud assessments into business processes to deliver real-time insights and results.
- Direct workflow to the right groups or individuals in the organization using business rules.
- Inform and protect the organization as new threats emerge, using cybersecurity scans.

If this list seems daunting, consider that states don't need to have all of these capabilities in place at once to improve their ability to curb UI fraud. In fact, the above list goes approximately in order from least to most advanced, with fraud vulnerability analysis and a rapid detection platform being first-stage targets for many. Those capabilities can serve as the foundation for the other, more advanced capabilities.

What's most important is getting started—expanding, improving and deepening existing UI fraud remediation capabilities. Because not only are fraudsters becoming more sophisticated, state governments are buckling down even further in the face of a revenue crunch. They are looking even more closely at massive programs such as UI to make sure they're being run as efficiently as possible. And that begins with smarter approaches to fraud, waste and abuse.

About the Authors

Luther Klein is a managing director at Accenture responsible for North American Finance and Risk Analytics.

Carl Hammersburg is manager of government and healthcare risk and fraud at SAS.

Alta Photo / Shutterstock

Reaction and overreaction: The unemployment insurance disaster

BY CARL HAMMERSBURG

Criminals follow money, and the impacts of the COVID pandemic led them straight to unemployment insurance (UI) programs.

Coming off historically low unemployment rates and staffing, UI agencies were hit with a double whammy of a massive explosion in claims and changes to the system by the CARES Act. How did they respond? By shoveling money out the door with both hands. What was the result? Billions—most likely, tens of billions—of dollars, in fraud went to organized criminal networks.

I've testified in states across the country and at the federal level about the scourge of UI fraud. Most recently I was in Pennsylvania, where the state's Department of Labor and Industry was overwhelmed by claims and, despite herculean efforts, is receiving thousands of calls per day from citizens in need. Lawmakers were concerned about threats to its Pandemic Unemployment Assistance Program—and they are right to be concerned: UI fraud is rampant.

Some examples are stark. My home state of Washington was hit badly by Scattered Canary, a fraud operation conducted by a ring out of Nigeria. Losses quickly grew from $1 million to $300 million to $576 million. At the peak, the state admitted over 56% of all money going out the door was lost to fraud. The same ring hit numerous states, including Massachusetts, Wyoming, Oklahoma, Rhode Island and Florida.

Florida hackers who hijacked computers using malware tried to file $500 million in claims in Maryland. A state contractor hired to process claims for Michigan's UI agency stole $2 million.

But that's the tip of the iceberg. The Identity Theft Resource Center has seen 28 times the number of UI fraud cases reported year-to-date in 2020, compared to 2019. The Secret Service reports that UI fraud is now the bulk of its work.

Overreaction hurts people in need

In response to the waves of fraud, states clamped down in the most manual way possible. Agency employees, contractors and in some cases the National Guard were called up to manually process documents. State after state saw backlogs in claims—tens of thousands in some cases, and more than 1 million in California.

> "IT'S TIME TO THINK DIFFERENTLY. LET'S STOP FUNDING IDENTITY THIEVES AND BRING TOGETHER MULTIPLE DATASETS WITHIN EACH STATE TO HELP VALIDATE IDENTITIES AND ENSURE THAT CLAIMS ARE PAID TO REAL AMERICANS WHO ARE HURTING."

Real people with legitimate claims haven't received a single UI payment after waiting for two or three months. Or they received assistance for just one or two weeks, then were shut down and caught in an administrative nightmare. For those whose identities were stolen to file claims, it could be even worse as they fight that damaging impact and try to reclaim payments made to criminals.

Legislatures all over the country are making inquiries to find out exactly what happened, and how to set matters straight.

The balancing act

It's time to think differently. Let's stop funding identity thieves and bring together multiple datasets within each state to help validate identities and ensure that claims are paid to real Americans who are hurting.

One of the best approaches that could be quickly implemented is to run all the existing claims through analytics software to not only detect fraud and stop future payments, but see who looks like a real person and approve payment immediately.

What does that look like in the data? Here are a couple of examples taken from real-world experience:

- One person laid off from a restaurant in Massachusetts might bank at a small out-of-state bank in Indiana. But if 20 people from that restaurant are all at that same small bank, it's a huge warning light for identity theft.
- An independent hairdresser shut down during the pandemic can file for Pandemic Unemployment Assistance. The UI agency doesn't have much information on that person, as they were exempt from previous withholding. But they will have a business license from the state, a cosmetology license and state tax filings. If none of those exist, it's identity theft.

Even for citizens with legitimate needs, payment speed is inhibited by fears that people will get money they "don't deserve." The risks of overpayments of a few hundred dollars that can be collected once people go back to work is small compared to an explosion of fraud.

UI agencies need people to staff the inundated phone lines and to process payments. However, analytics technology can be used as a force multiplier, poring through thousands of claims filed across many different accounts, providing a thorough view of risk, reducing fraud and adding speed and confidence to the payment process.

It's time to stop rewarding criminals. It's time to help Americans in need. Let's get off the seesaw.

About the Author

Carl Hammersburg is manager of government and healthcare risk and fraud at SAS.

Route Fifty and GCN are both GovExec publications

sas For more information, visit: sas.com