Fighting Fire with Fire
Using Artificial Intelligence to Combat Unemployment Insurance Fraud

By Carol Tannous, Michael Greene, Benjamin Tyler Brede, and Chris Carter
A publication from the Deloitte AI Institute for Government

 Agencies can look beyond known tactics to keep up with new and emerging schemes. Although state unemployment insurance (UI) agencies have decades of experience fighting fraudulent claims, the COVID-19 pandemic increased the level of combat. The surge in unemployment, broadening of eligibility, and influx of funding attracted a new breed of more sophisticated fraudsters. Individual bad actors and organized crime rings are aggressively targeting UI agencies with large-scale, technology-enabled fraud schemes.

These agencies are not alone: the threat extends to all benefits systems that have high-volume funding distribution, across the country and at every government level.

The money at stake is significant. The Labor Department’s Office of the Inspector General (OIG) estimates that the rate of improper payments, including
fraudulent payments, for the UI program under the 2020 Coronavirus Aid, Relief, and Economic Security (CARES) Act and subsequent legislation may be higher than 10%, or more than $89 billion. The OIG identified just $5.4 billion in potential fraudulent payments from March through October 2020, indicating that much of the suspected fraud has yet to be uncovered.1

While economic recovery and the termination of pandemic unemployment assistance (PUA) have led to a decline in unemployment claims, the threat of sophisticated fraud remains. Fraudsters that have taken advantage of these agencies since the onset of the pandemic are unlikely to move on.

To meet this challenge, UI agencies should fight fire with fire by deploying large-scale, sophisticated, artificial intelligence (AI)-powered detection systems to support their workforces. Two scenarios—account takeovers and insider threats—illustrate these systems' potential.

Expansion of unemployment benefits
COVID-19 transformed the funding and delivery of unemployment benefits. To address the pandemic-induced unemployment surge—which hit a record monthly increase of 15.9 million new jobless workers in April 2020—Congress used the CARES Act and the American Rescue Plan Act to broaden unemployment eligibility.2 With self-employed and gig workers becoming newly eligible for federally-funded benefits and both state and federal payments supplemented by an additional $300-$600 per week, states’ claims volumes reached unprecedented levels. New unemployment claims averaged just over 200,000 a week in January and February 2020, but then surged to a weekly average of 2.4 million initial claims from March through July 2020.3

The surge in claims presented state agencies with a wide range of challenges. They were in uncharted territory with new eligibility requirements, non-traditional applicants, and shifting guidance on program rules. At the same time, they faced critical staffing and workload issues. Finally, data from the National Association of State Workforce Agencies indicates that when the pandemic began, only about 40% of UI programs had completed their current technology modernization efforts.4 Updating technology takes time, but economic shocks and surges in claims often happen rapidly and unexpectedly.

A long-term, large-scale threat
Although the pandemic provided fraudsters with new opportunities to illegally collect unemployment benefits, the threat of fraud is not new. Bad actors have long targeted state and federal agencies to commit fraud and misdirect payments. They use a variety of techniques, often increasingly sophisticated and broad in scope:

- **Identity appropriation.** Bad actors use the names of those in nursing homes or prisons or the recently deceased to submit claims.
- **Bot-driven automation.** To perpetrate large-scale fraud, bad actors leverage automated processes to rapidly generate email addresses and submit and certify claims.
- **Wage and verification falsification.** To evade detection mechanisms, fraudsters fabricate wage verification documentation and alter ID cards.
- **Cyberattacks.** Bad actors can hack into systems to gain access and perpetrate fraud. Some can also pass through the identity verification because they have access to people’s security questions from earlier cyberattacks.
- **Social engineering.** Bad actors pose as legitimate program employees to gain access to real accounts.

---


The most impactful fraud schemes applying these techniques are not driven by individuals misfiling or misrepresenting a single claim. The threat arises from coordinated groups of fraudsters perpetrating large-scale schemes, including, rarely, bad actors working for state agencies.

**Detecting signals to address the threat**

Despite being technologically sophisticated and highly motivated, the bad actors perpetrating fraud at scale create “signals” or “digital fingerprinting” that agencies can detect if they have the tools to effectively evaluate the data. Agencies must also look beyond known tactics so they can keep up with fraudsters in adapting to new and emerging schemes. Bad actors learn quickly and will switch methods as soon as agencies identify one signal and stop associated fraudulent claims.

To create tailored fraud detection solutions, agencies should consider applying advanced analytics tools and AI techniques, in combination with a deep understanding of unemployment data, processes, and program rules. Two fraud scenarios provide an overview of the tools and techniques, and how UI agencies can apply them to identify fraud:

**Account takeover.** Multiple states and UI agencies have seen bad actors hijack the accounts of real claimants. Fraudsters use many sinister methods to obtain personal information, including purchasing it on the dark web, acquiring it through cyberattacks, and social engineering. Once they gain access to a claimant’s account, they immediately change bank account information and steal payments before victims become aware of what is happening.

But all is not lost. Fraudsters leave behind digital fingerprints in the form of anomalous patterns and behaviors. An agency can use anomaly detection and AI models to understand normal behavior, as well as frequency and order of account activities.

---

**NETWORK GRAPH**

- **CLAIM**
- **ADDRESS**
- **PHONE**
- **IP ADDRESS**
- **BANK ACCOUNT**
- **USER**

**User enabling payment on suspicious claims**

**Shared bank account**

**Claims sharing an IP address**

**Shared address**

---

**Source:** Compiled by authors using simulated data.
Some suspicious indicators include:

- The use of new IP addresses or devices to edit a claim
- Changes to payment methods or accounts
- Changes to account or login information
- Deviations from normal account activity patterns, such as the timing of updates or sequencing of activities

**Insider threats.** With the influx in federal unemployment funding, some UI agencies have seen patterns of nefarious activity by insiders, including rogue employees and contractors. To thwart insider threats, agencies can use AI models to identify anomalies, analyze networks, and apply a risk-based approach. Techniques include:

- Statistical methods to identify unique activities that are anomalous to specific user groups—that is, activities that do not align with a user’s typical interaction with a claim or claim attributes. Examples include home addresses, bank account information, etc.
- Machine learning techniques to label users who share patterns that resemble known insider threats.
- Anomaly detection to analyze suspicious internal activities—for example, actions taken on dormant claims and the frequency of these actions.
- Network analytics to determine the connectivity between internal users and claimants. Network graphs (as shown on the previous page) can help identify common attributes and hidden connections between claimants and users.

By fighting back with AI tools and techniques, UI agencies can reduce the amount of data exfiltrated and fraud committed.

However, even with the most sophisticated detection approaches, UI agencies cannot eliminate fraud entirely. Claims volume will likely surge again in response to future recessions, economic shocks, and the continued evolution of fraud techniques.

To prepare for these known threats, agencies should consider acting now to deploy and rapidly scale AI and machine learning that keeps up with the evolution of fraud techniques. They should also consider coordinating with other state and federal agencies who have faced fraud in the past and will continue to encounter it in the future. By being proactive with advanced fraud detection measures, agencies can make progress in preventing the proliferation of these crimes and help ensure that eligible candidates receive vital unemployment benefits.

**Contact us:**

Scott Malm, Principal
Deloitte Consulting LLP
smalm@deloitte.com

Carol Tannous, Managing Director
Deloitte Transactions and Business Analytics LLP
cタンノス@deloitte.com

**About Deloitte AI Institute for Government**

The Deloitte AI Institute for Government is a hub of innovative perspectives, groundbreaking research, and immersive experiences focused on artificial intelligence (AI) and its related technologies for the government audience. Through publications, events, and workshops, our goal is to help government use AI ethically to deliver better services, improve operations, and facilitate economic growth.

Contact the Institute at usgpsartificialintelligence@deloitte.com

---

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2021 Deloitte Development LLC. All rights reserved.