McKinsey
& Company

Public & Social Sector Practice

Fighting identity theft in benefit claims and payments

US government agencies are using analytics to mitigate fraud at scale and ensure benefits get into the hands of citizens who need them most.

by Matt Higginson, Sahil Jain, Ajit Sawant, and Eric Schweikert

© Golubovy/Getty Images

October 2020

Paying benefits to US citizens experiencing economic hardship amid the COVID-19 pandemic is a process that has been fraught with challenges. Claimant volumes have spiked, often by more than an order of magnitude. Worse, many of these claims are submitted by fraudsters committing identity theft (IDT), netting as much as $10,000 per application. Fraud costs federal, state, and local governments billions of dollars each year and generates a vicious cycle of extra work and payment delays.

But now, authorities are fighting back. State agencies are employing a whole-system approach that applies analytics to identify, test, and approve or deny applicants at scale. Successfully preventing and resolving IDT requires coordination across financial operations, using, for example, tiered triage rules, better prioritization of cases for further investigation, and new, digital self-service solutions. By rapidly adopting such approaches, agencies can erect effective defenses, attempt to stay ahead of new waves of fraudulent claims, and better serve their citizens in need of assistance from the devastating effects of the pandemic.

The attack of the swarming fraudsters

Public-sector agencies often underinvest in fraud defenses, in part because the savings in prevented fraud usually can't be used to fund the cost of detecting and remediating it. And since most citizens are honest, this approach, while not ideal, has allowed agencies to muddle through.

However, IDT, in which a fraudster uses a stolen identity to apply for benefits to which someone else is entitled, can be problematic for lightly defended agencies. For an agency to lose lots of benefits to first-party fraud, many citizens need to decide to cheat. A single fraudster using different stolen identities, however, can create large fraud losses quickly. Fraudsters talk to each other, so when a good opportunity for IDT presents itself, fraudsters using many identities can swarm.

IDT swarming occurred at the US Internal Revenue Service in the early 2010s,[1] as well as at state unemployment insurance (UI) agencies recently. The inspector general of the US Department of Labor estimates that UI systems will lose $26 billion[2] to fraud and improper payments in 2020, and the state of Washington has paid as much as $650 million to fraudsters (although it recovered about half of that amount).[3]

Many factors make UI benefits a ripe target for fraud. UI agency staffing is cyclical, and the long economic expansion before the COVID-19 pandemic has run down staffing and experience at most state agencies. The number of unemployed workers in early 2020 was at historically low levels, matched by the limited resources and scale of the agencies that served them.

Once COVID-19 hit, however, unemployment increased at unprecedented rates, and agencies were flooded with up to 6 million[4] applications a week—more than five times the prior peak—stretching staff and resources. At the same time, staff had to implement multiple new federal UI benefit programs with additional reporting requirements. One of those benefits included eliminating the traditional waiting week that agencies had used to perform due diligence. Other benefits allowed for an increased payout, which, combined with Department of Labor guidance that backdating be allowed, meant an initial payment on a UI claim in some states could be more than $10,000.

These changes stretched UI agency resources and taxed their sometimes-antiquated systems. After unemployment levels spiked in mid-March 2020 and federal benefits came online about a

[1] Lizette Alvarez, "With personal data in hand, thieves file early and often," *New York Times*, May 26, 2012, nytimes.com.
[2] *Member briefing before the US House of Representatives Committee on Oversight and Reform Subcommittee on Government Operations*, Office of Inspector General, US Department of Labor, June 1, 2020, oig.dol.gov.
[3] Paul Roberts, "Washington's unemployment fraud may have hit $650 million; state recovers $333 million," *Seattle Times*, June 4, 2020, seattletimes.com.
[4] *Unemployment insurance weekly claims*, US Department of Labor, October 8, 2020, dol.gov.

month later (depending on state implementation), fraudsters began submitting more and more IDT applications. Favoring speedier disbursements, states reduced standard procedural checks and processed and paid many of these initial applications. Around mid-May 2020, the volume of IDT applications skyrocketed. Agencies tightened their systems for detecting IDT, and some even halted processing all applications for a period, thereby creating a new backlog problem that persists today in some places.

These detection efforts prevented more payments to many potential fraudsters. But the flood of IDT detections created unmanageable queues of hundreds of thousands of accounts awaiting verification. In one state, over a quarter of all applicants were told they needed to verify their identities. Typically, applicants send identification documents for verification and then trained investigators manually determine whether they match and are genuine. Record application volume combined with historically high IDT rates caused many states to generate as much as a year's worth of investigative work in the first few weeks of May 2020.

How agencies can fight fraud

Preventing and treating fraud requires coordination across all elements of operations. Agencies need to appreciate the power of analytics for prioritization and automation in bulk approval of low-risk claims, while focusing scarce, skilled human resources on those claims that need them. Agencies should think creatively about fraud detection, auto-adjudication, and smart investigation. And while fighting fraudsters on the one hand, they must ensure a better claimant experience on the other (see sidebar, "How a state UI agency devised a holistic plan to address IDT").

How a state UI agency devised a holistic plan to address IDT

One state UI addressed IDT with a whole-system approach. Facing a backlog of several hundred thousand claims requiring adjudication, the agency cleared about two-thirds of its queues in four weeks by applying an analytics-based approach to identify, test, and then bulk-approve low-risk populations. The agency employed technological solutions to improve document-processing productivity and prioritized the workload to identify tasks that newer, less-trained staff could complete effectively. A focus on measuring and actively managing workforce performance has improved productivity and helped the agency incorporate the many new hires and temporary staff that have been added to augment capacity. And the agency continues to focus on managing its work queues equitably to ensure that any remaining delays have the minimum customer impact possible.

Between volume in general and the fallout of IDT remediation, the agency's call center has been swamped. To minimize errors, confusion, and progress-chasing (that is, people calling in to find out the status of their applications), it is revamping its customer experience. This includes ensuring that all communications are clearly written, that online FAQs and inbound call-center interactive-voice-response (IVR) messaging address the most common issues being raised, that account and application status are available online, and that self-service options are offered when possible.

Successfully preventing and resolving identity theft requires coordination across financial operations.

Five actions can help agencies create a virtuous cycle of light-touch, but effective, fraud monitoring and detection:

Fraud detection rules need creative thinking and rigorous evaluation

Typically, IDT detection rules are either outsourced to specialist vendors or built from the insights of individual fraud investigators, but rarely updated. Fraudsters have learned to change their tactics rapidly to avoid fraud detection rules as they are implemented, so it is important for agencies to continue to evolve their detection rules. State UI agencies can connect with one another, either directly or through the National Association of State Workforce Agencies,[5] to share their ideas. They should crowdsource additional ideas from nationwide investigators who are working cases. Also, there are third-party vendors that can provide services such as address or bank account verification.

These fraud-detection rules then need a rigorous system to evaluate their accuracy. In general, a rule should maximize the absolute number of true positives (fraudsters caught) while minimizing the false detection rate (the percentage of legitimate applications snagged by the rule that eventually end up being adjudicated "good" and released). An evaluation system can start by back-testing the rule, meaning looking at historical adjudications to see what would have happened if the rule had been in place. The next step is testing the rule live on a sample of new applications. If results of the live test are positive, then the rule can be promoted to full production.

Many agencies have IDT detection rules already in production that are not systematically evaluated for efficacy and may carry legacy bias (for example, focused on detecting only certain types of counterfeit information). It is important to measure and report the number of true positives and the false detection rate for every IDT rule that stops applications and sends them for verification.

Innovative fraud treatments can reduce the need for manual investigations

Historically, most agencies received only a limited number of IDT cases and treated them as exceptional investigations, often requesting the claimant send in identification documents for manual review. Not only is this time-consuming, but also in the recent flood of IDT, fraudsters are submitting convincing fake documents.

Alternate approaches can provide high-confidence verifications with limited effort. For instance, through the US Postal Service, several states have mailed letters containing a personal identification number for applicants with verified addresses.[6] The applicant can then input the number into a secure website, thus verifying that the applicant does, in fact, reside at this known address. This may be sufficient for an agency to rule out identity theft. Third-party vendors offer document verification and,

[5] National Association of State Workforce Agencies, naswa.org.

[6] Relying on postal instead of electronic notifications avoids alerting fraudsters who may have access to the purported claimant's online unemployment-insurance account.

in some instances, states can trigger escalation during the application process. And some states use cyber behavioral patterns to block fraudsters from even applying.

Auto-adjudication and prioritization can help manage investigation queues

Given the swarm of IDT attempts, many agencies have faced unmanageable queues of investigations. Simply adding staff may not be the right answer, as it takes training and experience to adjudicate potentially fraudulent applications properly. In rare instances, fraudsters have even infiltrated state UI agencies' temporary adjudicating workforces.

One option when working with less experienced adjudicators is to divide the queue into easier- and harder-to-adjudicate groups. For instance, applications that were stopped by detection rules with a high false-positive rate are more likely to be good and may be candidates for review by lower-tenure adjudicators who have less training.

Another option is to look for positive attributes among those applications awaiting adjudication. Examples include applicants who did not request any backdating of their claim, or who had previously contacted customer service. A sample of applications meeting positive criteria can be prioritized for adjudication. If the bad rate in the sample is low enough, the agency may choose to remove them from the adjudication queue and bulk-approve all of them, accepting some low rate of fraud to prioritize payments to the vast majority of legitimate claimants.

A clean-sheet view of customer experience can reduce confusion and burden on call centers

Customer confusion can lead to claimant errors that land legitimate requests in IDT queues. These can prevent legitimate claimants from successfully completing their weekly certifications, leading to non-IDT adjudication and payment holds.

Taking a customer-experience lens can lessen confusion. Reviewing all communications—for example, letters, websites, online account notices, and interactive voice responses (IVR)—and revising the language to remove jargon and feature consistent, clear explanations, starting with the highest-volume communications, can begin to shrink the inflow of new claims for adjudication.

Additional potential fallout from long IDT adjudication queues has overwhelmed customer service centers. Setting clear expectations at the outset in the documentation request—and reinforcing those expectations—while providing as much account-level information as possible through the call center's IVR or online, can both reduce the number of phone calls and improve the claimant experience.

Spotting and defying the fraudsters enables agencies to speed up essential payments to those citizens who need them the most.

Digitization and self-service can make the entire process more scalable

Given the dramatic swings in volume seen by UI agencies, their entire operations, from application to recertification to IDT detection and treatment, would benefit from automation and digitization. By using more standardized applications, many irregularities requiring investigation could be eliminated at the outset. And once an application has been submitted, digital channels offer claimants the opportunity to track progress in real time. Some states have employed smart chatbots to inform and better prepare first-time applicants for the complexities of the UI process. Not only do digital channels reduce the need for slow, manual processing, but they may also offer a better, more familiar, and more convenient user experience.

The COVID-19 pandemic has generated unprecedented demand on unemployment insurance and other government benefit agencies. Few have coped well. Exacerbating the problem has been the voracious appetite of fraudsters to commit IDT. Faced with evident payment trade-offs, many agencies chose speed over diligence, leading to vast fraudulent overpayments. Agencies are fighting back to break this vicious cycle. Spotting and defying the fraudsters enables agencies to speed up essential payments to those citizens who need them the most.

Matt Higginson is a partner in McKinsey's Boston office, where **Ajit Sawant** is an associate partner. **Sahil Jain** is an associate partner in the Chicago office. **Eric Schweikert** is a senior expert in the Washington, DC, office.

Designed by McKinsey Global Publishing