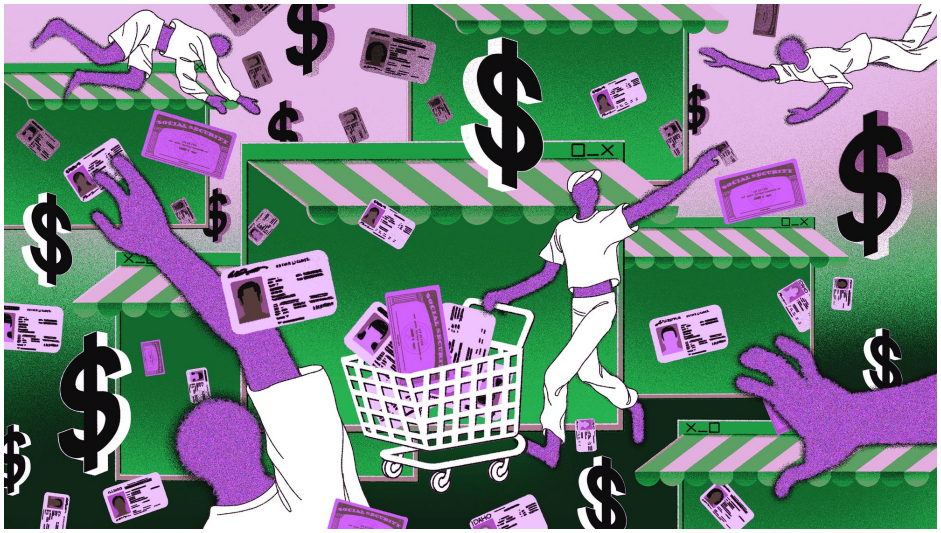
PROPUBLICA

Labor

How Unemployment Insurance Fraud Exploded During the Pandemic

Bots filing bogus applications in bulk, teams of fraudsters in foreign countries making phony claims, online forums peddling how-to advice on identity theft: Inside the infrastructure of perhaps the largest fraud wave in history.



Cath Virginia, special to ProPublica

by Cezary Podkul

July 26, 2021, 5 a.m. EDT

ProPublica is a nonprofit newsroom that investigates abuses of power. Sign up to receive our biggest stories as soon as they're published.

A Bronx man allegedly received $1.5 million in just ten months. A California real estate broker raked in more than $500,000 within half a year. A Nigerian government official is accused of pocketing over $350,000 in less than six weeks.

What they all had in common, according to federal prosecutors, was participation in what may turn out to be the biggest fraud wave in U.S. history: filing bogus claims for unemployment insurance benefits during the COVID-19 pandemic. (The broker has pleaded guilty, while the Bronx man and Nigerian official have pleaded not guilty.)

Fraudsters have filed in high volumes, sometimes obtaining payments from multiple states, despite the fact that a jobless person is barred from getting assistance in more than one state. One person, according to the U.S. Department of Labor, used a single Social Security number to file

unemployment insurance claims in 40 states. Twenty-nine states paid up, sending $222,532.

But the problem extends far beyond a plague of solo scammers. A ProPublica investigation reveals that much of the fraud has been organized — both in the U.S. and abroad. Fraudsters have used bots to file online claims in bulk. And others, located as far away as China and West Africa, have organized low-wage teams to file phony claims.

In addition, the fraud has been enabled by a burgeoning online infrastructure, whose existence has not previously been reported in the mainstream press. Much of it is geared toward exploiting aging or obsolete state unemployment systems whose weaknesses have drawn warnings for decades. Communities have sprouted on messaging apps such as Telegram, where fraudsters trade tips on how to cash in. Hustlers advertise their techniques — or "sauces" (apparently short for "secret sauce") — for filing bogus claims, along with state-specific instructions on how to get around security checks, according to a ProPublica review of messages on more than 25 such chat forums.

Some of the forums have thousands of participants and regularly offer stolen identities for sale, alongside tech tips, screenshots that ostensibly prove the methods work and advice on which states are easiest to game and which are "lit" — that is, still paying out fake claims. Users have created two Telegram channels in which they trade tips for filing claims in Maryland, whose labor department recently said it detected some 508,000 potentially fraudulent jobless claims between the start of May and mid-June. Participants in those forums have been talking about turning their efforts to Pennsylvania, where officials recently said they have "noticed an uptick" in fraudulent claims.

Telegram did not respond to requests for comment. But after ProPublica's inquiry, 10 of the channels we asked about suddenly went dark, marked with this notice: "This channel can't be displayed because it violated Telegram's Terms of Service."

Nobody has yet come close to putting a definitive number on the dollar value of fraud relating to pandemic-era unemployment benefits. But ProPublica performed a data analysis that hints at the massive scope. In state after state, the volume of initial jobless claims has far exceeded the number of estimated job losses. Across the U.S. from March to December 2020, the number of initial claims equated to 68% of the country's labor force, which stood at around 164 million before the pandemic. In five states — Arizona, Georgia, Hawaii, Nevada and Rhode Island — the initial claims outnumbered the entire pool of civilian workers. By contrast, about 23% of American workers were out of a job or underemployed at the peak of the pandemic, according to the Bureau of Labor Statistics; in the most recent report that figure is just under 10%. (There are innocent explanations for at least some of the disparity: If a person loses a job more than once during a given year, they can legitimately file for benefits more than once during that time.)

The fraud estimates provided by states so far range from high to jaw-dropping. In Vermont, as many as 90% of claims in some months were

determined to be fraudulent, state officials said in June. Rhode Island's labor agency said in March that it suspected fraud in 43% of the claims it had received. The equivalent agency in California has confirmed fraud in about 10% of its payments and said it's investigating a further 17%. The numbers have tailed off in Texas, whose agency says it now suspects fraud in about 14% of its claims.

"The system was the victim of what is one of the largest internet crimes in history, perpetrated against all 50 states at extraordinary levels," said James Bernsen, a spokesperson for the Texas Workforce Commission. (Bernsen and officials for other states say the damage could've been even worse: They say they've been able to stop billions of dollars' worth of bogus claims before they got paid.)

The U.S. Department of Labor's inspector general estimates that at least $87 billion in fraudulent and improper payments will have made their way through the system by the time pandemic-linked jobless aid programs expire in September. That estimate is based on a historic assumption that fraud and waste eat up about 10% of unemployment insurance aid. The inspector general acknowledges that figure is likely too conservative in an environment where unemployment insurance fraud has "exploded" to "unprecedented" levels.

Other experts anticipate a dramatically higher tally. "From my experience, when this is all said and done, we are going to be counting in the hundreds of billions of dollars, not the tens of billions," said Jon Coss, who heads a unit within Thomson Reuters that is helping states detect fake unemployment insurance claims.

Coss bases that assessment on the widespread fraudulent activity he's seen. He said one U.S. state, which he declined to name, received fake claims — all purportedly from state residents — that originated from IP addresses in nearly 170 countries. They included countries historically linked to fraud, such as China, Nigeria and Russia, as well as more surprising ones, such as Cuba, Eritrea, Fiji and Monaco. Overall, Coss said, between 40% and 50% of the claims his group has analyzed seem highly suspect. He added, "It's mind-boggling the level of fraud that we're seeing."

Defrauding unemployment insurance, or UI, programs, which pay out weekly benefits to workers who've lost jobs through no fault of their own, is likely as old as the programs themselves. But the rise of internet-based crime over the past 25 years or so, particularly the use of stolen identities to file fake claims on someone else's behalf, opened the way to fraud on an epic scale.

The problem was already described as ongoing as early as 1998, when the Labor Department's inspector general warned about the "continued proliferation of UI fraud schemes." Four years later, a report by the inspector general said, "We are particularly concerned with identity theft or imposter schemes, which occur when individual identities are stolen and then used to apply for UI benefits." The report noted that "individuals have the opportunity to defraud multiple states from a single location."

In 2015, the agency detailed the "systemic weaknesses" that make UI programs vulnerable to fraud. (More on those later.) At least twice during the Obama administration, the Labor Department proposed reforms to Congress to address some of these inadequacies, primarily by boosting information sharing among states and federal agencies. Both times these efforts went nowhere. President Donald Trump included similar reforms in each of his four budget proposals to Congress. They, too, were never enacted.

Meanwhile, states' funding for unemployment insurance administration was falling, largely because the economy strengthened and unemployment fell. At the start of the pandemic, funding for states' unemployment insurance administration stood at a 30-year low, according to the National Association of State Workforce Agencies.

The funding squeeze led to some predictable results. California, which had hired Coss's firm to help detect fraud, canceled that contract in 2016 to save money. Budget cuts also trimmed the ranks of the federal Labor Department's inspector general's office, which lost 28% of its criminal investigators between 2012 and 2020, according to figures provided in response to a Freedom of Information Act request.

At the same time, online criminals were expanding their targets. Years ago, Agari Data, a cybersecurity firm that helps catch email scams, began tracking a Nigerian cybercrime group it dubbed "Scattered Canary." Agari produced a timeline of the group's evolution that looks like an ever-branching tree: It grew out of Craigslist scams (2009) into phishing (2015) and then tax return fraud and credit card fraud (2016). Scattered Canary started targeting unemployment aid, too. "Similar to how the group pivoted from individual victims to business targets during the previous three-year period," Agari wrote in a 2019 report, "Scattered Canary again set their sights on a new type of target in 2017 — government agencies."

A steady procession of large-scale hacks of corporations and governments over the past decade provided the raw material needed to defraud government benefit programs. What scammers call "fullz" — a suite of data ranging from a person's name and address to their Social Security number, date of birth and more — was increasingly easy to obtain. The Privacy Rights Clearinghouse, which tracks data breaches, tallied 2,229 hacks from 2010 to 2019, according to a database of such incidents. Those hacks exposed nearly 6.9 billion records.

When the pandemic seemed to threaten the foundations of the economy in March 2020, Congress responded quickly, launching the biggest expansion of unemployment insurance since the system was created amid the Great Depression. Lawmakers created three massive programs that workers could tap as states shut down to halt the spread of the deadly virus.

One program provided workers 13 additional weeks of aid once they exhausted their regular unemployment benefits. Another gave laid-off workers an extra $600 per week on top of existing benefits. A third, known as Pandemic Unemployment Assistance, funded 39 weeks of jobless

benefits for workers traditionally excluded from unemployment insurance, such as self-employed "gig economy" contractors.

As of July 17, 2021, the three programs have collectively paid out about $604 billion, a total projected to reach up to $873 billion by the time the programs expire in September. That's on top of states' regular unemployment insurance plans, which paid out another $166 billion in jobless benefits between March 2020 and June 2021. That means total payments to the jobless could add up to about $1 trillion over 18 months.

Augmenting UI payments was not an unusual move for Congress — but the scale and speed were vastly different. For example, in the aftermath of the 2008 financial crisis, Congress funded an extra $25 a week on top of regular state unemployment benefits, then averaging around $300 a week. This time, Congress authorized a weekly $600 payment that was automatically added to regular UI payments, which require verification of prior income and employment.

But in its urgency to get cash to people with no work, Congress chose not to require such verification in the PUA program. It requested only self-certification of eligibility and no proof of income or identity. And successful applicants could get the extra $600 weekly payment, too.

With its loose application requirements, PUA instantly drew throngs of scammers. California state authorities have said that 95% of its confirmed fraudulent UI payments originated in PUA claims. Pennsylvania's agency estimated that nearly 84% of its PUA claims were phony.

A scroll through the thousands of messages exchanged in Telegram chat forums provides a vivid illustration of what state unemployment agencies have been up against. The forums are easy to find: Simply searching for the acronym "PUA" can lead any Telegram user to a bunch of them (even after Telegram shut 10 of them in the wake of our questions). They have proliferated since the start of the pandemic, providing bustling marketplaces for criminals looking to obtain stolen IDs, methods for filing fake jobless claims or other advice. The most common products sold on the forums — state-specific sauces for filing claims — are hawked with daily frequency.

A Telegram user who posts under the handle "VerifiedFraud" recently offered his 1,300 chat room participants a new sauce for Pennsylvania's system that he said would pay $700 a week. (VerifiedFraud also posted an earnest "new month prayer" on July 1, asking God to help his customers: "My prayer is all your sleepless night & day coming to this forum working & praying to God shall come through and Success will locate u.")

ProPublica screengrab from Telegram

Pennsylvania said it's unable to speak to the validity of the guide. When ProPublica asked about the guide, VerifiedFraud responded with two emojis: 🙄🙄. Fifteen minutes later, he posted a message in his channel that seemed to rationalize fraud: "Virtually all these wealthy entrepreneurs you see around 90% of them started with something illegal to make enough money to run their business."

The guides available on Telegram include lengthy step-by-step directions and screenshots detailing where to input stolen information. They offer advice on how to avoid triggering anti-fraud software, such as not to fill out part of the application on one device or from one IP address, then switch to another. One guide for filing claims in New York state warns users, "Don't Copy and Paste in the text box. Type in the details while filling the text boxes. A script monitors activities like Copy&Paste to raise red flags."

When such guides outlive their usefulness, new ones quickly pop up. "New CALI SAUCE WAVE," read one of several messages posted in late June alongside a screenshot of what purported to be a successful unemployment aid application for California. The ad, offered by someone who calls himself the "King of Cali," touted a video guide and a PDF walk-through. California's Employment Development Department declined to comment.

ProPublica screengrab from Telegram

Many of the pitches are blunt. One ad features the 2021 edition of a “Fraud Bible” for sale alongside 19 other sauces, including a guide for obtaining loans under the government’s Paycheck Protection Program, another frequent fraud target. The PPP loan program ended on May 31, underscoring the risk that the people selling the Fraud Bible may not be on the up and up. (When ProPublica requested comment, the seller or sellers of the Fraud Bible responded with variations of “fuck you.” The “King of Cali” responded by asking, “Are you ready to pay? I’ll give you everything you need.” Hours later, his profile was deleted and replaced with a warning: “Many users reported this account as a scam or a fake account. Please be careful, especially if it asks you for money.”)

Concerns about fraud are rampant inside the forums — but only insofar as the users fear they could become victims of it rather than perpetrators, say, by paying for a fraud strategy that no longer works. One Telegram forum called "$CAM C3NT£R" promises a "trusted" escrow service that clears sales of sauces, stolen identities and other services to make sure participants don't rip each other off while preparing to rip the government off. (The administrator of $CAM C3NT£R told ProPublica he's just trying to stop fraud inside his channel: "lot of fake people around and I'm doing escrow to protect my people.")

To convey the success of their methods, sellers frequently post photos of wads of cash or screenshots of unemployment payments seemingly landing in their bank accounts or mobile payment apps. One user who recently advertised a Michigan sauce elegantly arranged $20 bills in the shape of the words "tap in" to encourage users to pay $200 via Bitcoin for his method, along with a screenshot of Michigan's jobless aid website and the claim that "Michigan still hittin and is payin good money." (A spokesperson for Michigan's Unemployment Insurance Agency said the state is having success stopping fraudulent payments before they're made and that "these type of messages amount to false advertising in order to elicit money from those who would steal identities.")

ProPublica screengrab from Telegram

Social Security numbers, names and dates of birth are frequently exposed in the forums by sellers wishing to give buyers a taste of what they've got. Sometimes users post links to files of data purportedly stolen via corporate hacks. In another dark web forum called White House Market, some participants offer to create identity profiles tailored to specific states where buyers want to file jobless claims. "No guarantee in success, but all pros would be made just for you," read one such ad. The asking price was $70 per profile.

Such forums have attracted users from around the world, but user messages suggest that one country in particular appears to provide a significant set of followers: Nigeria.

That's where Abidemi Rufai was bound on the evening of May 14 when he was getting ready to board the first-class cabin of a flight at John F. Kennedy International Airport after visiting his brother in New York. Instead, he was arrested by FBI agents and charged with stealing more than $350,000 in unemployment benefits from Washington state.

Details of that indictment shed light on how federal prosecutors believe such schemes are carried out, and the sheer variety of participants they have attracted: Rufai serves as a senior special assistant to the governor of a Nigerian state.

He allegedly used stolen identities to file fake unemployment benefits in 11 states, including over 100 applications in Washington, where state auditors have tallied a total of $1.1 billion in possible imposter fraud from nearly 250,000 potentially bogus claims.

Prosecutors say Rufai filed his claims using variations on the same email, sandytangy58@gmail.com, which he modified by inserting periods in different places, like san.dyta.ngy58@gmail.com or sa.ndyt.a.ngy58@gmail.com. Servers for state unemployment agencies treat those as different email addresses, but Google disregards periods when routing messages to a gmail account. That allowed Rufai and his co-conspirators the convenience of filing in multiple states while handling all of their correspondence from one email account. It's a popular strategy: Another Nigerian national allegedly used it to claim more than $489,000 of unemployment payouts from 15 states, according to an affidavit filed in a similar case.

When completing unemployment benefit applications, Rufai and his co-conspirators directed states to pay benefits into Green Dot online banking accounts, one of several fintech platforms favored by criminals for their ability to quickly link debit cards with checking accounts that can be used to receive government benefit payments. In other cases, they directed payments into bank accounts controlled by "money mules," people who would receive funds and then transfer them to Rufai and his co-conspirators in exchange for a fee. (Green Dot Chief Risk Officer Philip Lerma said the company has been working with state agencies to combat fraudulent activity. "This is an ongoing process of learning and refinement across the industry," he said in a statement.)

Prosecutors said Rufai's email account contained a "staggering" amount of stolen information, including passwords to people's email accounts, security questions and answers, driver's license numbers, and bank account and routing numbers, as well as more than 1,000 stolen tax returns.

Rufai had also used his gmail account to submit claims for Federal Emergency Management Agency disaster relief in 2017, according to prosecutors, followed by fraudulent submissions to the Small Business Administration and the Internal Revenue Service. After Rufai was charged, investigators at the IRS disclosed they had been investigating the sandytangy58@gmail.com account for several years. They told prosecutors that the agency had received 652 applications for fraudulent tax refunds from "dot variants" of that email, totaling $1.6 million. Of that, about $900,000 was approved for payment.

Rufai has pleaded not guilty. His lawyer, Michael Barrows, did not respond to repeated requests for comment. Barrows wrote in a bail filing in late June that Rufai has no criminal record and that prosecutors are offering "intentionally false and/or misleading information in an effort to exaggerate the crimes alleged while tarnishing the reputation of a well-respected Nigerian government official."

Some scammers employ similar techniques on a mass scale by writing computer scripts, or bots, to automatically populate stolen identities into states' application portals. New York suffered an attack from one such bot, which was able to repeatedly navigate and complete its application process, according to a person familiar with the episode. New York's labor commissioner has said that the state is "aggressively deploying advanced resources" to fight fraud, including computer algorithms of its own.

Other fraudsters outsource such activity to human labor farms in low-wage countries, according to cybersecurity firm F5. Patterns of UI applications indicate workers in China, Brazil, Bolivia, Mexico and West African nations have been hired to input data into U.S. unemployment portals, according to Carlos Asuncion, F5's director of solutions engineering. Asuncion said job ads to do that kind of work often pop up on websites catering to "microworkers" — people who earn pennies per task for such actions as creating gmail accounts, inputting email addresses or zip codes and solving captchas (the latter for as little as five hundredths of a cent per captcha). The labor can be even cheaper, according to Asuncion, than developing and updating a computer algorithm. As he put it, "It's kind of an arms race."

State unemployment agencies, burdened by aging technologies and siloed databases that don't effectively communicate with each other, have been unable to keep up with any sort of arms race.

Federal rules require states to cross-check applicants' information against a handful of databases when determining eligibility for jobless benefits. These include a national directory of new hires, quarterly wage records submitted by employers, and an immigration database that allows states to verify applicants' citizenship status. The Labor Department also recommends that states check a database aimed at preventing claims in

multiple states, as well as the Social Security Administration, prisoner records and an interstate data hub meant to help flag foreign IP addresses, suspicious email domains and applicants, according to a May 2020 compliance bulletin.

But performing all those checks requires modern technology. Many states are running their UI systems on software so obsolete that it's hard to even find anyone able to service it. North Dakota had to recruit programmers from Latvia to prop up its systems last year, since the tiny Eastern European nation is one of the few places that still teaches the software used by the state's unemployment insurance system. The clunky mainframe was "miraculously patched together, at considerable cost, to get us through the pandemic surge," the state's governor said in his December 2020 budget proposal, which sought to replace the system.

Amid the surge in claims, databases frequently froze up or slowed to a crawl, according to the Labor Department's inspector general. States also reported not having the mainframe capacity to perform cross-matches for the large volumes of claims they were getting.

The result was that many cross-checks simply didn't happen. Twenty states did not perform all the required database cross-matches, and 44 states did not perform all recommended ones, the inspector general found.

Even when states perform the checks, they can still be fooled. After all, the extent of identity theft means that criminals often input the information of a real person. Validating that the data is accurate doesn't necessarily verify whether the claim was filed by the person whose data was used. "Verification and validation are two different things," said John Pallasch, an assistant secretary of labor during the Trump administration. "That was the inherent flaw in all of this."

Violinist Philip Payton got caught on the wrong end of this after he lost his job playing in Disney's "Frozen" musical. When the pandemic shut down all Broadway performances in March 2020, word got around the orchestra that musicians could apply for unemployment insurance. By early April, Payton was receiving $504 a week plus the extra $600 authorized by Congress, his account shows. "This just helped me stay normal," he said. "I could pay my bills and pay my half of the rent."

But things changed in mid-September when the weekly payments suddenly stopped. He called New York's Department of Labor and was told, he said, that he had a claim in another state. The agent didn't tell him which state. A follow-up conversation in October ended the same way.

Many have shared Payton's plight. In 2020, consumers filed nearly 400,000 complaints claiming their identities were stolen and used to claim government benefits. That was up more than 2,900% from about 13,000 such complaints in 2019, according to Federal Trade Commission data.

Unsure what to do, Payton kept calling until he finally got through to someone who told him the other claim was in Texas. Payton called the

Texas Workforce Commission's fraud line, but couldn't get through to anyone.

By then, it was January and Payton was beginning to run low on cash. He kept calling and leaving messages but couldn't get a call back. Eventually, through a chain of contacts, Payton reached an agent at the Texas commission, who told him he was listed as having filed claims in multiple states. The agent told him to call New York's labor department to get his benefits restarted.

That prompted yet another round of phone calls. It was now early April. Payton had drained his savings and was falling behind on rent. Sometimes he'd spend three to four hours a day on hold while practicing violin or browsing job ads on the internet. He also started contacting organizations he thought might be able to help. Eventually, he connected with a paralegal at the Legal Aid Society, who sent an email to two New York labor department officials asking to expedite his case.

A day later, after eight months of missed payments and little work, Payton's unemployment benefits finally restarted (and covered the earlier missed payments). But the experience shook his faith in the program. "There just has to be a better system," Payton said.

The state unemployment agencies in New York and Texas both declined to comment on Payton's situation, citing privacy restrictions. But Bernsen, the spokesperson for the Texas Workforce Commission, said in a statement that the state generally blocks suspicious claims by placing a "fraud block" on them. "This becomes a problem when the legitimate person needs to access those funds." He added, "Fundamentally, the system is trying to do two things simultaneously that are at odds with one another: ensure quick payments to individuals and prevent fraud."

Of the two issues, fraud prevention is now much more on the minds of officials in Washington. Gene Sperling, President Biden's top official in charge of the pandemic response, said the issue goes beyond just unemployment insurance. The deluge of fraudulent claims has slowed as the surge in federal aid draws to a close, but he sees the proliferation of identity theft for government benefits as the larger threat. "It's always a bad thing when somebody cheats and gets a few thousand dollars by doing this or that," Sperling told ProPublica. "But we seem to be seeing something much larger and systemic."

Sperling said the White House asked federal agencies to provide preliminary recommendations by mid-July on what the government can do to prevent criminal syndicates from using stolen identities to access government aid, whether unemployment benefits, small business loans or disaster aid given out by FEMA.

One idea that's already being implemented is improving the Labor Department inspector general's access to states' unemployment compensation data, so that federal watchdogs can analyze claims for fraud in real time instead of individually subpoenaing states for the data.

The administration is also planning to spend $2 billion to modernize states' unemployment insurance programs and strengthen them against

fraud. The Labor Department is still figuring out how to allocate the funds, which were appropriated under the $1.9 trillion coronavirus stimulus bill enacted in March. One approach under consideration involves having the federal government develop centralized technology to help the 53 states and territories manage their jobless aid programs, instead of having them all fend for themselves and scramble to implement changes during crises.

Recent increases in funding to bolster fraud detection have also been a boon for ID.me, a company that has been hired by 27 states since mid-2020 and recently won a $1 billion federal contract to provide its services to more states. ID.me verifies that claimants are who they say they are by having them take selfies or asking them to appear on video and checking to make sure their faces match the photos on identity documents used to apply for benefits.

ID.me's chief executive, Blake Hall, made headlines last month when he told Axios that he thinks taxpayers' losses from UI fraud will top $400 billion. Hall defends that estimate, which some commentators criticized as wildly inflated. Hall based the figure on the precipitous drop-offs in new claim applications that states have experienced after implementing ID.me verification. In New York, for instance, state data confirms that new claims for PUA fell by 89% after ID.me went live in late March. And more than 50% of people who have already filed for UI benefits don't even try to confirm their identities when asked to do so, according to Hall, who cited data from five states the company has worked with.

Fraudsters are trying to adapt. Telegram forums have lit up with offers of sauces and software that sellers claim can bypass ID.me. Hall said his firm monitors such ads and maintained that he has yet to find any that work. "There is no bypass," he asserted.

That may be true today. But, as one recent post on a dark web marketplace noted, "The fraud business is an ever-changing type of business, meaning methods are constantly being updated because of new security implementations on the market."

Do you have any information about unemployment insurance fraud that you'd like to share with us? Email cezary.podkul@propublica.org.

Filed under —
Labor