‘A magnet for rip-off artists’: Fraud siphoned billions from pandemic unemployment benefits

The Covid Money Trail

Identity theft and other sophisticated criminal schemes contributed to potentially $163 billion in waste, while inflicting harm on unwitting victims.

By Tony Romm
and
Yeganeh Torbati

May 15, 2022 at 6:30 a.m. EDT
Listen to article
21 min

Sareena Brown-Thomas, a victim of identity theft that caused her to be unable to collect unemployment benefits. The number of fraud cases in unemployment insurance benefits has increased significantly. (Carolyn Van Houten/The Washington Post)

Sareena Brown-Thomas had just arrived home from her shift as a custodian when she noticed an envelope in the mail from the D.C. government. Bearing her name, address and the last four digits of her Social Security number, the letter inside said she had been awarded unemployment benefits — a problem, she later recalled, since she had never applied for them.

The 32-year-old soon notified her bosses, believing last summer that she had put the matter to rest. But the real trouble wouldn’t start until September: When Brown-Thomas did actually find herself out of a job, she couldn’t get the financial support she needed. Mired in bureaucratic battles, she said she faced a months-long struggle just to prove her identity to the city.

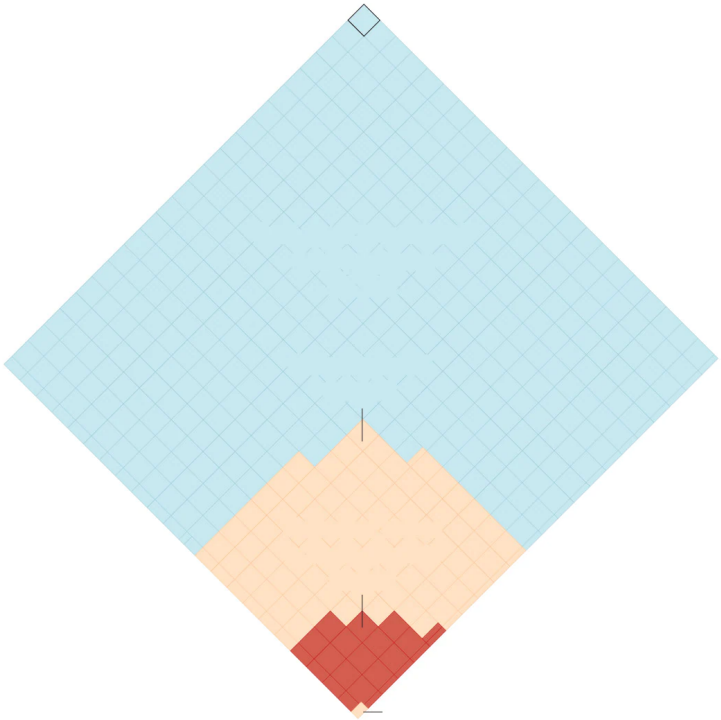
“I’m still trying to figure out how to get a lot of stuff paid,” Brown-Thomas, who warred at one point with D.C. over her eligibility, said in an interview this spring. “It was so easy for them to use my Social Security number to get unemployment.”

Brown-Thomas is part of a sprawling community of victims caught up in a massive series of attacks targeting the nation’s generous coronavirus aid programs. The more than $5 trillion approved since the start of the pandemic has become a wellspring for criminal activity, allowing fraudsters to siphon money away from hard-hit American workers and businesses who needed the help most.

The exact scope of the fraud targeting federal aid initiatives is unknown, even two years later. With unemployment benefits, however, the theft could be significant. Testifying at a little-noticed congressional hearing this spring, a top watchdog for the Labor Department estimated there could have been “at least” $163 billion in unemployment-related “overpayments,” a projection that includes wrongly paid sums as well as “significant” benefits obtained by malicious actors.

So far, the United States has recaptured just over $4 billion of that, according to state workforce data furnished by the Labor Department this March. That amounts to roughly 2.4 percent of the wrongful

payments, if the government's best estimate is accurate, raising the specter that Washington may never get most of the money back.



$10B

Total spent in pandemic

relief programs

$5.23T

Unemployment

$1.03T

Estimated losses

to overpayments

$163B

Recovered at least $4.1B

In many cases, the criminals stole the unemployment funds using real Americans' personal information. They bombarded states with applications filed in the names of actual workers or people in prison — sometimes to such a degree that, in the case of Maryland, fraudulent claims came to outnumber real requests for help, according to state correspondence reviewed by The Washington Post.

Criminals employed tools known as botnets to fire off thousands of applications, federal officials say, often with a single computer click. And they openly swapped tips for defrauding the government on popular websites and apps, including the messaging service Telegram. That has continued this year, as

research showed at least two dozen groups with nearly 200,000 members openly discussed ways to avert states' defenses and siphon funds just over an eight-week period in March and April.

The tactics are laid bare in a wide array of federal documents, congressional testimonies, technical reports and court filings, as well as interviews with roughly two dozen government officials and outside experts. Some of the malicious actors potentially even avoided detection, at least for a time, after the Labor Department refused to supply information needed to assist federal fraud investigations — a hurdle the White House intervened to resolve last year.

The troubles date to the earliest days of the pandemic, when roughly a million Americans were being thrust out of work daily. Congress responded with a series of massive rescue packages, which greatly augmented the jobless aid available nationally. Totaling nearly $900 billion, according to the Labor Department, the federal funds helped blunt the toll of the worst economic crisis since the Great Depression, allowing families to keep their homes and pay their bills.

But the aid quickly emerged as a ripe target for fraudsters, who found novel ways to exploit the nation's under-resourced state unemployment agencies. In recent months, a wide array of state and federal law-enforcement agencies have sprung into action, training their sights on domestic criminals and gangs, as well as sophisticated networks based in Nigeria, Russia and Eastern Europe. The White House, meanwhile, has embarked on a broader effort to close the gaps in the nation's unemployment program — and ensure that other federal aid can't be targeted in the same way again.

"The unprecedented explosion of unemployment claims, combined with years of disinvestment in our unemployment system, lack of state-by-state data sharing and weak identity controls, created a perfect storm for the fraud and identity theft in 2020 that we inherited," Gene Sperling, a top adviser to President Biden who oversees pandemic spending, acknowledged in a statement.

'Large-scale fraud'

The troubles plaguing the nation's unemployment insurance program are part of a familiar pattern: In the face of an unprecedented crisis, federal officials consistently chose haste over precision, dispatching aid with uncharacteristic speed to save the economy — even at the risk of costly mistakes.

Beginning in March 2020, Democrats and Republicans aimed to provide historic economic support for the torrent of workers unexpectedly thrust from their jobs. Lawmakers expanded the size of the benefits — at one point providing an extra $600 per week — while extending the amount of time that out-of-work Americans could receive the aid. Congress also created a program to provide financial help to those who drive for Uber, deliver for DoorDash or otherwise participate in the "gig economy" — a category of self-employed laborers who traditionally are not eligible for unemployment insurance.

Americans rushed to take advantage of the financial lifeline, overwhelming the state workforce agencies that administer unemployment insurance programs, typically with minimal involvement from Washington. Massive delays soon left millions without pay, even as states relaxed some paperwork requirements. Amid that chaos, fraudsters soon gained a toehold.

The first signs of widespread trouble came in May 2020, when the Secret Service issued an alert about "large-scale fraud" targeting North Carolina, Massachusetts, Rhode Island, Oklahoma, Wyoming and likely other states. The bulletin said the suspects, based in Nigeria, had harnessed personal information stolen from government officials, school employees and others to obtain benefits under their names. Law enforcement would eventually trace the operation to a syndicate called Scattered Canary, a notorious Nigerian crime ring associated with romance scams and other nefarious online activity.

In the months to come, the fraud would metastasize.

In California, state officials acknowledged in October 2021 that they may have paid out more than $20 billion in undeserved unemployment payments to criminals. That included at least $810 million that had been wrongly paid to applicants whose information matched the names of people in prison, a population ineligible for unemployment aid, according to a separate report from the state's auditor. Officials at California's top labor agency declined to comment.

In Michigan, a team of state-hired consultants in December projected that they had paid out as much as $8.5 billion in benefits to malicious actors. Arizona said it may have sent $4 billion in checks to criminals. And Pennsylvania conceded this year that fraud appeared to have resulted in the theft of nearly $8 billion. (Those figures are each local estimates, which in some case include state funds and are computed differently than the federal government's projections.)

The harm extended beyond state coffers. In Philadelphia, Natalis Perez first filed for unemployment insurance in July 2020, after her concerns about infection forced her to leave a job at a local food processing plant. But the 27-year-old soon learned that someone else had already filed a claim in her name — a likely sign of fraud that she soon reported to authorities.

The discovery set off 18 months of unreturned calls and bureaucratic haggles, Perez said, as she labored to prove her identity and collect the money she was owed. She ultimately contacted Philadelphia Legal Assistance, a legal aid group, at the end of last year. The unemployment support finally arrived in January — far too late for Perez to put the money to use to address the financial crunch posed by the pandemic.

"It affected me a lot because I stopped paying my bills," she said in a recent interview. "I have a lot of debts now … I had to move because I couldn't pay my rent."

Alex Peterson, a spokesman for the Pennsylvania Department for Labor and Industry, acknowledged the state initially lacked the staff to process a historic surge in applications for benefits. He added in a statement that resource constraints also affected the office's work to solve complex issues around claims in a timely matter, though he noted that Pennsylvania had sought to ramp up its work to better verify workers' identities.

Citing the "record demand" for aid, Peterson added that "it's no surprise there were also unprecedented levels of fraud."

The Labor Department's top watchdog initially feared about $87 billion in wrongful unemployment payments nationally, with much of it concentrated in fraud. But some of the government's tallies suffer from severe gaps, since states report only the investigations they have completed, often on a significant delay. More recently, the agency has said the number could be twice as high: The inspector general has estimated $163 billion in unemployment-related waste, after surveying a sample of federal spending data and applying it to the total pot of money that the government doled out during the pandemic. Unveiling its staggering findings earlier this year, the agency watchdog warned it's likely to be an undercount, too.

"It's obviously substantial," Roy Dotson, the national pandemic fraud recovery coordinator at the U.S. Secret Service, said in a recent interview. "I can't really get into the number … we're all trying to figure that out."

The extent of the caper is laid bare in states including Maryland, where a top official warned Congress this spring that the state had "received more fraudulent claims than honest and deserving ones," according to a letter sent by the state's secretary of labor, Tiffany Robinson, to federal lawmakers.

Maryland Gov. Larry Hogan (R) first revealed in July 2020 that a criminal scheme had siphoned more than $500 million from the state's unemployment program. Since then, the attacks have only intensified. In March, for example, an unknown entity impersonating the Maryland Department of Labor sent emails asking existing unemployment beneficiaries to verify their identities. This time, the scam preyed on the state's work to combat fraud — just to perpetuate more of it.

"What's astonishing is we continue to see these attacks on our customers every single day," Robinson said.

'It's a symptom'

The tsunami of fraud came as little surprise to labor experts, who had been warning about neglect and mismanagement for years.

Many states "started the pandemic with a 50-year low in administrative funding," recalled Michele Evermore, a deputy director at the Office of Unemployment Modernization at the Labor Department. That meant the governments "weren't well resourced in the first place," even before they were tasked to implement major new, high-demand stimulus programs.

Once those mandates arrived, it took only a few short weeks before a top federal watchdog agency saw reason for urgent action. In its April 2020 report, the inspector general for the Labor Department warned that the "substantial increase" in federal benefits could place immense strain on the underfunded state operations, opening the door for expansive criminal activity.

"Those outdated systems are just a magnet for rip-off artists and the fraudsters," said Sen. Ron Wyden (D-Ore.), a longtime advocate for tech fixes, recalling the early red flags.

The agency watchdog also cited "longstanding concerns" about poor staffing and low budgets in the state workforce agencies, and raised the alarm about computer systems running on decades-old technologies. And the inspector general further called attention to the special new program to aid gig-economy workers: Unlike traditional unemployment insurance, which vets applicants' work histories, the new initiative crafted by Congress did not require applicants to provide similar documentation. The approach helped states distribute checks quickly — yet opened the door for waves of abuse.

"We've seen states where literally as many as 3 out of 4 claims into [the program] were highly suspicious and likely fraudulent," said Jon Coss, the vice president of risk, fraud and compliance at Thomson Reuters, which helps states verify applicants. He declined to specify the states.

The inspector general declined to comment.

Beyond the mere design of the programs, the government faced the further challenge of identity theft. Years of major cyber breaches — including the 2017 theft of data from the credit monitoring agency Equifax — offered fertile ground for criminals to mine Americans' personal lives and put it to use to pursue federal benefits.

"It's scary that someone knows your address and Social Security number, and all this stuff, and it makes you wonder what else they might be doing with it," said Rebecca Dixon, the leader of the National Employment Law Project, which advocates for the expansion of unemployment benefits.

Dixon wasn't speaking hypothetically: She herself had been the victim of identity theft, as scammers used her information to apply for benefits in the nation's capital. The longtime labor expert only discovered the issue once a debit card was sent unexpectedly to her house last year.

“It’s a symptom of a bigger and more global problem of private companies not keeping our data safe,” Dixon said.

A spokesman for the D.C. Department of Employment Services did not respond to a request for comment.

With valuable personal data in hand, some fraudsters plotted openly on apps, including Telegram. They swapped their credentials and tips for defrauding the federal government in a wide array of channels, including one dedicated to targeting the Utah unemployment system that alone attracted 16,000 subscribers. The hub offered to “teach” users how make money and “sell all tools” needed for the heist — and contained a slew of photos that purported to depict real Americans’ full checking and routing numbers. They spoke in code about “sauce,” a sort of digital tradecraft for deceiving states and stealing their funds.

A spokesman for Telegram declined an interview request, noting in a statement it is “working to expand both our Terms of Service and moderation efforts to explicitly restrict and more effectively combat other misuses.” Before The Post could highlight the specific channels, or reach out to their owners for comment, the company appeared to remove some of them, including one focused on Maryland.

“They’re advertising on Telegram as of this morning how they’re stealing benefits from the state of California,” said Haywood Talcove, the chief executive officer of government at LexisNexis Risk Solutions, during an interview in late March. Talcove, whose company works with nearly two dozen states to verify applicants, shared screenshots of one such channel called “UI LOAN SAUCE HUB,” which since has been removed.

“They’re showing the money from the bank into their account,” he said.

Yet roughly two dozen other, similar channels remain active and popular on the service, according to data furnished in early April by Gary Warner, the director of threat intelligence at the cybersecurity firm DarkTower. Over a 60-day period in March and April, more than 200,000 users in an assortment of groups openly exchanged intelligence for the best states to target for unemployment-related fraud, the analysis shows.

Some criminals submitted the same fraudulent applications to multiple states, seizing on the lack of a single, central and mandatory repository for national employment data. Dotson, who oversees pandemic fraud work for the Secret Service, said criminals also purchased or created bots to do the work for them — relying on automated technology to fire off “literally thousands or hundreds of thousands of applications at one time.” He declined to name states.

Caught flat footed, states including Pennsylvania and Washington ultimately took drastic steps at the height of the pandemic, even pausing the delivery of much-needed benefits to ferret out fraudsters. California at one point shut down even legitimate applicants’ accounts to investigate the claims, denying aid to thousands caught up in its enforcement efforts. Others implemented tougher technology checks, requiring millions of recipients to verify their identities by submitting photos or using facial recognition software.

But the combination of old technology and newer, flawed digital remedies often carried consequences, too.

Few states struggled as much as Florida: Years of failed technology upgrades and political neglect left millions of out-of-work residents waiting weeks just to obtain their first payments. A year into the crisis, the Sunshine State faced further setbacks after hackers broke into its unemployment program, potentially stealing names, addresses and Social Security numbers from more than 57,000 accounts.

The well-documented woes of the system created headaches for Terri Yearby, a single mom from Port Orange who had collected benefits until she returned to work in January. In April, though, she learned someone may have been receiving benefits in her name for weeks.

In a bid to understand the problem, Yearby tried at the time to log on to the state's unemployment portal but discovered she had been locked out. Florida informed her that she had to verify her identity through ID.me, a firm that provides facial recognition tools and other digital checks to help states vet benefit applicants. But it took 11 days of failed attempts, emails and phone calls before Yearby could prove she was actually herself — at which point she saw someone had been collecting checks and routing them to a bank account other than her own.

Yearby filed a police report, spoke with bank representatives and froze her credit in response, according to correspondence with the state and ID.me as well as other documents she later shared with The Post. Yet she still received a federal form this year that counted the roughly $3,700 in fraudulent benefits as her own income — potentially subjecting her to taxes for aid she never actually received. She said it took roughly a year for her just to get Florida to review her case file formally, which came several weeks after The Post inquired about Yearby's case. She is still awaiting revised documents that would allow her to file her taxes properly.

"I don't want this hanging over my head," Yearby said in an interview. "I tried to resolve this issue. I tried to give them the necessary tools in order for them to resolve it."

A spokeswoman for Florida's unemployment agency declined to provide details on a specific case. But she said last month that the state is communicating with Yearby and otherwise has stopped $23 billion in fraudulent unemployment claims.

ID.me is now under a separate investigation on Capitol Hill, where federal lawmakers in April demanded the company turn over detailed records about its contracts with state and federal agencies, including the IRS. Congressional Democrats raised "serious concerns" about the accuracy of the firm's facial recognition technology, arguing that the mistakes nationwide threaten to deny much-needed financial support to Americans in greatest need.

Blake Hall, the chief executive of ID.me, responded more broadly, pointing out the "underfunded" nature of unemployment agencies across the country.

"As a result, they entered into a perfect storm — facing historic demand and fraud — woefully unprepared to provide the needed levels of access and security," he said in a statement.

'The federal government has not kept up'

In the meantime, the U.S. government faces another daunting task — trying to recover what it has lost.

In early May, a 45-year old man from Lekki, Nigeria, pleaded guilty to using stolen identities to obtain hundreds of thousands of dollars in pandemic benefits, including a massive, 18-state scheme that siphoned more than $350,000 from Washington state. He admitted he had engaged in similar fraud targeting the government for years, dating back to 2017, when he targeted relief programs for hurricane victims.

In late March, in Boston, a 30-year-old man pleaded guilty to stealing identities to obtain about $150,000 unemployment benefits in Massachusetts and other states. The man filed some of the

applications from the same computer, according to the unsealed complaint, eventually drawing investigators' interest.

And a federal court in February sentenced a former employee at California's own unemployment agency to five years in prison, after she was convicted of stealing $4.3 million in benefits. She filed the flurry of claims using Social Security numbers culled from her past work as a tax preparer, prosecutors said.

Despite the recent array of cases, the work to bring these fraudsters to justice hasn't always been easy. Behind the scenes, a battle raged at the end of the Trump administration into the first year of Biden's term over access to the very data that might have helped the federal government catch more criminals sooner.

The trouble stemmed from a dispute between the Labor Department and its own watchdog. Essentially, the Labor Department had erected barriers making it hard for states to turn over troves of information about unemployment claims so that federal officials, including the inspector general, could review the data for fraud. That forced the inspector general to seek separate subpoenas in all 54 states and territories every time it had hoped to query local records, delaying its work considerably, according to three people familiar with the matter, who spoke on the condition of anonymity to describe the dispute.

The dispute saddled not only the inspector general but also the Justice Department, which relies on the watchdog for criminal leads, according to an agency official who spoke on the condition of anonymity to describe the private discussions. By last June, the stalemate bubbled to the surface, prompting Carolyn R. Hantz, the assistant inspector general for audit, to issue a stark warning.

"Billions of dollars in potentially fraudulent claims are at risk of not being detected and improper payments stopped at the earliest opportunity," she said at the time.

Ultimately, the White House intervened: Sperling, who oversees stimulus spending, helped secure access to the data and conditioned some future federal funding on its continued availability. That opened the door for federal officials to augment their efforts to scan unemployment claims for fraud, the sources said.

The Biden administration has since trained its sights on upgrading the country's unemployment system — improving the technology that allows states to verify claims in the first place. Tech teams overseen by Evermore, a top official at the Labor Department, have plugged into states including Arizona, Michigan, Pennsylvania, Washington and Virginia, backed by a $2 billion initiative.

The White House also has explored a potential new executive order that aims to improve the government's ability to combat identity theft and protect federal funds from misuse. The president commissioned a task force to review the issue last year amid a wave of reports about pandemic-related fraud in unemployment and other programs, said Sperling, adding the administration had "taken steps to address the harm to those who have already been victims."

The scramble in Washington may be too late for those Americans who scrounged for aid while criminals feasted on generous federal benefits. But lawmakers, labor advocates, tech experts and law enforcement officials agreed that the government still needs to act swiftly, and aggressively, to stem the tide of a fraud that has left few untouched in its wake.

"The ability to engage in identity theft has grown exponentially and the federal government has not kept up," warned Michael Horowitz, the inspector general for the Justice Department and leader of the Pandemic Response Accountability Committee, which coordinates oversight of the country's more than $5 trillion in spending.

Horowitz said the unfortunate reality is that Americans “don’t realize sometimes” the real victim of such immense fraud targeting the government in the first place: “It’s the individual.”

Request for Reader Submission

Tell The Post: Have you been defrauded in connection with a pandemic aid program?

Scammers have managed to steal billions of dollars in unemployment benefits during the pandemic. A lot of this fraud involves identity theft: Thieves pose as someone else and claim benefits in their name. Similar schemes may be involved in fraudulent attempts to get other payments, too.

The Washington Post is working on a project about how trillions of dollars in covid relief money has been spent and how government officials are scrambling to track it. We’d like to hear from you if you’ve run into scams in connection with the aid.

Tell the Post

Read our full submission guidelines here