Government Business Council

Safeguarding Unemployment Insurance Benefits from Fraud

Fraud mitigation techniques for individuals, employers, and state agencies

SPONSORED BY: okta

THE BIG ISSUE

As a result of the COVID-19 pandemic, government agencies are under great pressure to provide prompt services to appropriate constituents, however, technological limitations and an unprecedented surge in demand have exposed gaps in fraud mitigation.

WHY IT MATTERS

Fraudulent unemployment insurance (UI) claims have multiplied existing hurdles to receiving benefits, resulting in an estimated $26 billion in lost benefits funding intended for those who need it[1].

States Overwhelmed by Mass Unemployment

The national unemployment rate in April 2020 increased to 14.7%, up from just 4.4% the previous month. This is the highest rate and the largest month-to-month increase since data was first collected in January 1948[2]. The unprecedented influx of unemployment claims in 2020 has overwhelmed state employment services.

Understanding Unemployment Insurance Fraud

INCREASED DEMAND FOR UNEMPLOYMENT BENEFITS

Signed into law in March 2020, the Coronavirus Aid, Relief, and Economic Security (CARES) Act expanded unemployment benefits for those affected by the COVID-19 pandemic in several ways, including increasing the weekly benefit amount by $600 through July 31, 2020. Unemployment benefits were also made available to self-employed and gig workers through the Pandemic Unemployment Assistance (PUA) program. With millions out of work as a consequence of the economic slowdown, state unemployment agencies have been overwhelmed by claims for unemployment benefits and are struggling to quickly provide payments to those in need. An average of 5 million people filed for unemployment claims in one week in April 2020[3], which is nearly eight times more than those made in a week during the Great Depression. Criminals are taking advantage of the surge in job losses to steal unemployment benefits from Americans nationwide, complicating an already tough situation for millions of impoverished Americans and overwhelmed state unemployment offices.

WHAT IS UI FRAUD?

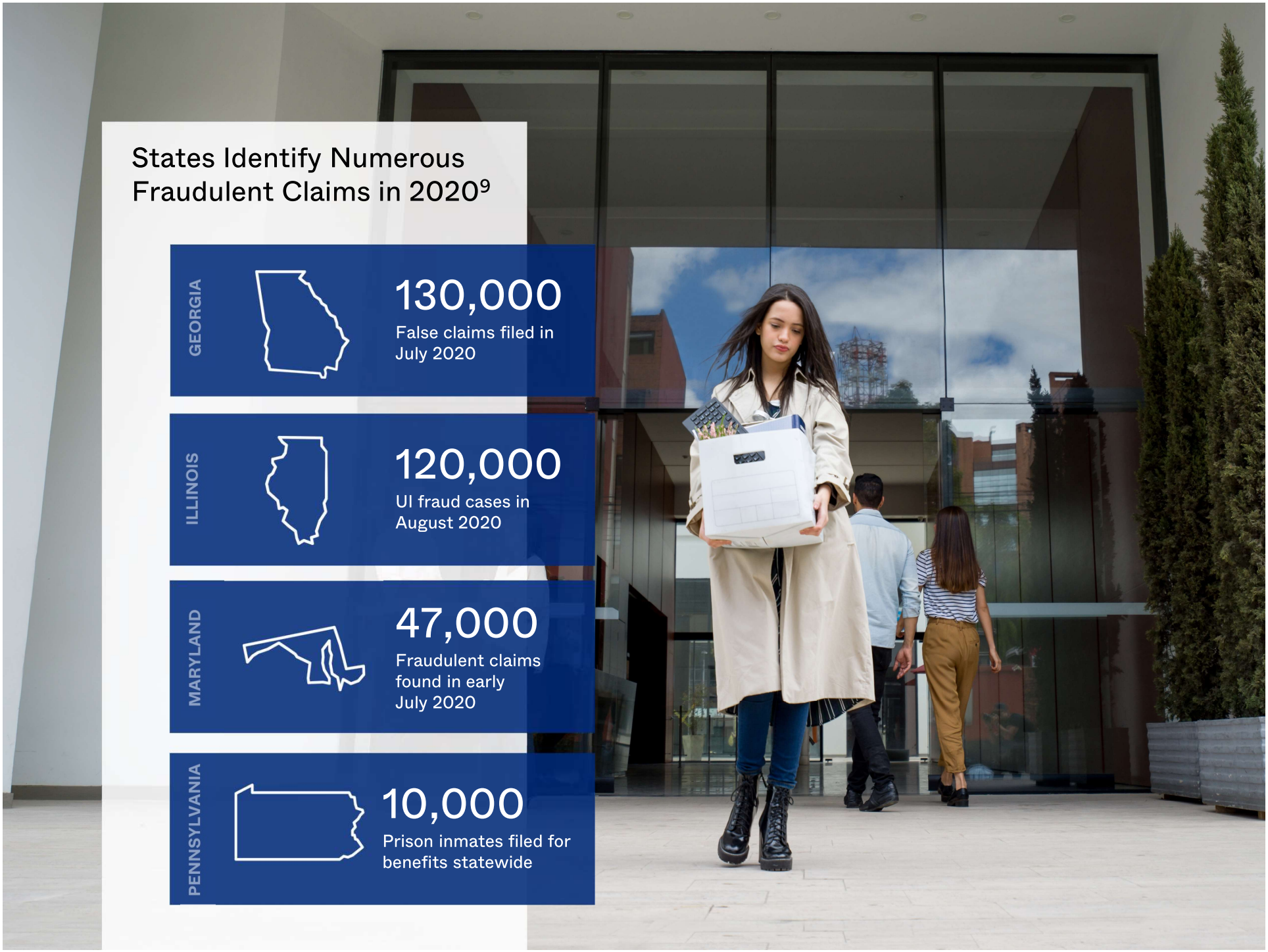
According to the U.S. Department of Labor (DoL), knowingly collecting benefits based on false or inaccurate information that was intentionally provided when filling a claim is considered fraud[4]. UI fraud can result from identity theft that is not the fault of the victim or the victim's employer.

CRIMINAL ACTIVITY

The Federal Bureau of Investigation (FBI) has reported a spike in fraudulent unemployment insurance claims involving the use of stolen personally identifiable information (PII)[5]. Cyber fraud scammers can use techniques like phishing, deepfake voice spoofing, and malware to con innocent victims into providing confidential information and exploit vulnerable IT systems[6]. Criminals have also taken advantage of the PUA which lacks the wage-verification measures that a traditional unemployment application has. Security experts say the bulk of the fraud appears to be committed by criminal actors impersonating victims and using the victims' stolen identities to submit fraudulent unemployment insurance claims online[7]. Many victims of fraudulent unemployment claims are still employed and have no idea that a claim has been filed in their name.

Criminal Networks Committing Fraud

Organized fraud rings, like the Nigerian-based Scattered Canary, have access to technology and data necessary to pull off digital heists from state employment agencies[8]. This group and others like it purchase breached data off the dark web and seize legitimate email addresses through a variety of techniques. With enough data to build a convincing application, they use the stolen identities to apply for unemployment insurance and route the payments through money mules to overseas accounts. However, not every example of UI fraud is done by a criminal network. These cases vary in sophistication but have occurred in nearly every U.S. state.


States Identify Numerous Fraudulent Claims in 2020[9]
GEORGIA
130,000
False claims filed in July 2020
ILLINOIS
120,000
UI fraud cases in August 2020
MARYLAND
47,000
Fraudulent claims found in early July 2020
PENNSYLVANIA
10,000
Prison inmates filed for benefits statewide

The Challenges to Fraud Mitigation

ONE

STRAINED APPLICATION SYSTEMS

The dramatic spike in unemployment claims to 14.7% in April 2020 left state unemployment agencies and their online application systems overladen and unable to keep up. The state of Nevada alone saw unemployment rise to 25.3% in May of 2020, a sharp contrast to an unemployment rate of just 4% one year before[10]. Increased demand for services, limited staff, new processes, and outdated systems have all made it more difficult to provide necessary aid and have made it easier for criminals to take advantage of strained systems[11]. Pressed for time, state unemployment offices have struggled to properly vet applicants and separate fraudulent from legitimate claims. States must strike a delicate balance between speed and accuracy in order to get benefits to the people who need them while also stopping those who try to defraud the system.

TWO

INSUFFICIENT IT INFRASTRUCTURE

The technology and processes at many state unemployment agencies were ill-equipped to handle the millions of applications for unemployment benefits[12]. This created an opportunity for criminal networks and impostors. In California, investigators found over 21,000 fraudulent unemployment claims that were filed in the names of prison inmates[13]. IT systems will need to be better prepared to accommodate changes to unemployment insurance programs, including a surge in claims or attempts to fraudulently claim benefits.

A Wide-spread Issue

As states scrambled to avoid financial losses from fraud, many halted payments. Michigan ceased payments for 340,000 claims, roughly 20% of its total, and Pennsylvania stopped 58,000 claims for its Pandemic Unemployment Assistance[14]. Nearly every state has suffered from fraudulent claims and lost benefits.

Preventing Fraudulent Claims

PROTECT PERSONALLY IDENTIFIABLE INFORMATION

On a personal level, one of the simplest ways to prevent identity theft and subsequent UI fraud is to protect personally identifiable information (PII). By safeguarding personal information, changing passwords regularly, and enabling two-factor authentication whenever possible, individuals and employers can play an important role in preventing fraud. Employers should regularly consult with their IT department to confirm that databases containing employee information have not been compromised[15]. In addition, IT administrators can update firewalls, install current software patches, train staff on known phishing techniques, or monitor for new scamming tactics. The Cybersecurity and Infrastructure Security Agency (CISA), FBI, and the DoL are warning individuals and businesses to stay vigilant against scams that seek to steal PII[16].

IMPROVE IDENTITY AUTHENTICATION PRACTICES

By improving their capability of identifying a fraudulent claim from a legitimate one, state employment agencies can ensure funds are distributed more appropriately. Existing IT systems have shown limited capability of keeping up with submitted claims and are in need of modernization. To rectify this issue, algorithms can be used to verify an individual's identity by checking their publicly available digital footprint. Individuals leave behind a digital footprint when using social media, paying bills, and shopping online among many other things. Cutting edge techniques in machine learning and artificial intelligence now make it possible to build an incredibly rich identity graph and ensure that the person behind the keyboard is who they say they are[17].

New Techniques in Preventing UI Fraud

According to state officials, the Colorado Department of Labor and Employment was able to prevent over 50,000 fraudulent claims from being approved by using a tech-based method that is referred to as the "18th measure." State officials declined to elaborate on the approach for fear of tipping off criminals[18]. The state is also working with the FBI, Secret Service, and local and state law enforcement agencies to try to recover $40 million already paid out to fraudsters.

US Department of Labor Aids in Fraud Mitigation

The Unemployment Insurance Information Technology Support Center (UI-ITSC) provides information, software tools, and advisory services to states to support IT systems for the UI program[19]. The UI-ITSC also disseminates best practices, supports state adoption of modernized technologies, and provides training related to IT functions. States are also encouraged to use the newly developed Unemployment Insurance Interstate Connection Network (UI-ICON) to cross-reference and match applicant data[20].

> “These [UI-ITSC and UI-ICON] projects address weaknesses within the UI system exposed due to the coronavirus pandemic. By strengthening the integrity of the UI system, increasing the cohesion between the states via a data exchange network, and developing better information technology practices, we are improving unemployment and reemployment services and outcomes for American workers[21].”
>
> - John Pallasch, Assistant Secretary for Employment and Training.

Preventing Fraudulent Claims

IDENTIFY FRAUDULENT CLAIMS EARLY ON

When a criminal network is flagged for committing fraud, states are obliged to flag all users with characteristics matching the scam artists until they can re-verify their identity with the agency. This is a time-consuming process that can result in cutting off claimants' earned compensation for weeks[22]. Instead, state unemployment agencies should implement industry-tested tools to verify identities upon the date of application[23]. Flagging potential impostors using tools and datasets during the application process is key to preventing substantial financial losses. Using insights from multi-dimensional data sources, these tools can execute several verifications of a claimant's identity and validate the legitimacy of information on the application for benefits[24]. Additionally, state officials should integrate with ID theft protection firms to quickly notify potential victims if their information has been used to file an unemployment claim[25].

DEVELOP A REPORTING SYSTEM

Unfortunately, not all UI fraud can be stopped at the application process. Therefore, systems must be put in place to report fraudulent claims once they are discovered by individuals or employers. In Kansas, officials have established reportfraud.ks.gov for potential victims and employers to report suspected fraud. It is unknown how many claims by fraudsters have been approved, but the Kansas DoL has said they have blocked at least 45,000 fraudulent payments since the beginning of the year[26]. Individuals and employees in all states should be made aware of reporting systems available to them.

U.S. Department of Labor Provides $100 Million to Combat UI Fraud

On September 1, 2020, the U.S. DoL announced that $100 million in funding will be provided to support states' efforts to combat fraud and recover improper payments in the Unemployment Insurance program, including those programs created under the CARES Act. The U.S. DoL also encourages states to work with the Employment and Training Administration and the Unemployment Insurance Integrity Center in order to proactively address UI fraud[27].

Sources

1. https://apnews.com/article/f8e34c8436b52e6df38f974a44403b55
2. https://www.bls.gov/opub/ted/2020/unemployment-rate-rises-to-record-high-14-point-7-percent-in-april-2020.htm#:~:text=The%20unemployment%20rate%20in%20April,to%2023.1%20million%20in%20April.
3. https://www.cnbc.com/2020/04/08/five-million-more-unemployment-claims-expected-but-now-layoffs-could-be-more-permanent.html
4. https://www.dol.gov/general/maps/fraud
5. https://www.fbi.gov/news/pressrel/press-releases/fbi-sees-spike-in-fraudulent-unemployment-insurance-claims-filed-using-stolen-identities
6. https://www.nextgov.com/ideas/2020/04/intersection-cyber-crime-and-coronavirus-stimulus-perfect-storm-fraud/164552/
7. https://apnews.com/article/f8e34c8436b52e6df38f974a44403b55
8. https://abc7news.com/millions-lost-in-edd-scam-by-scatter-canary-crime-ring/6201928/
9. https://www.shrm.org/hr-today/news/hr-news/pages/unemployment-fraud-on-the-rise.aspx
10. https://www.forbes.com/sites/mikepatton/2020/06/28/pre-and-post-coronavirus-unemployment-rates-by-state-industry-age-group-and-race/?sh=641354f7555e
11. https://apnews.com/article/f8e34c8436b52e6df38f974a44403b55
12. https://insight.equifax.com/record-unemployment-fraud-demanded-a-solution/
13. https://www.ktvu.com/news/california-lawmakers-urge-hearings-over-fraudulent-unemployment-claims
14. https://www.socure.com/blog/how-to-combat-the-spike-in-unemployment-fraud
15. https://www.shrm.org/hr-today/news/hr-news/pages/unemployment-fraud-on-the-rise.aspx
16. https://www.dhs.gov/news/2020/04/24/fact-sheet-dhs-taking-covid-19-related-fraud
17. https://www.socure.com/blog/how-to-combat-the-spike-in-unemployment-fraud
18. https://coloradosun.com/2020/09/10/colorado-unemployment-fraud-scammers-pua-pandemic/
19. https://www.dol.gov/newsroom/releases/eta/eta20200928
20. https://www.dol.gov/newsroom/releases/eta/eta20200928
21. https://www.dol.gov/newsroom/releases/eta/eta20200928
22. https://www.nelp.org/publication/from-disrepair-to-transformation-how-to-revive-unemployment-insurance-information-technology-infrastructure/
23. https://www.socure.com/blog/how-to-combat-the-spike-in-unemployment-fraud
24. https://insight.equifax.com/record-unemployment-fraud-demanded-a-solution/
25. https://www.socure.com/blog/how-to-combat-the-spike-in-unemployment-fraud
26. https://www.ncsl.org/research/labor-and-employment/state-strategies-for-stopping-unemployment-fraud-amid-the-pandemic-magazine2020.aspx
27. https://www.dol.gov/newsroom/releases/eta/eta20200901

ABOUT GBC

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and a commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at www.govexec.com/insights

ABOUT OKTA

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to both secure and manage their extended enterprise and transform their customers' experiences. With over 5,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely adopt the technologies they need to fulfill their missions. Over 5,600 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to securely connect their people and technology.

Learn more at www.okta.com