WRITTEN TESTIMONY OF HAYWOOD TALCOVE

CHIEF EXECUTIVE OFFICER, LEXISNEXIS SPECIAL SERVICES INC.

BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON WORK AND WELFARE

February 6, 2025

## 1. Introduction

Chair LaHood, Ranking Member Davis, and members of the Subcommittee, thank you for inviting me here today to discuss an issue that lies at the heart of our nation's public trust. The widespread fraud that has undermined government assistance programs intended to help millions of Americans during the pandemic continues today. My name is Haywood Talcove, and as the Chief Executive Officer of LexisNexis Risk Solutions for Government, I have spent over sixteen years leading efforts to stop fraud, streamline government services, and protect taxpayer resources. I have witnessed firsthand the transformative power of effective data and identity verification technologies—not just in safeguarding resources, but in ensuring that aid reaches those who genuinely need it. It is my personal mission and that of my team to assist government programs in protecting the benefits they provide, as well as the integrity of our social safety net.

The events of the past few years have shaken that mission to its core. The scale and sophistication of fraud targeting government programs—particularly, but certainly not limited to, unemployment insurance—have reached alarming new heights, exposing vulnerabilities to our systems and demonstrating just how easily malicious actors can exploit them. Post-COVID, these criminals have shifted their focus toward all government assistance programs as a lucrative target, treating public benefits like a low-risk, high-reward business model. Of the nearly $1 trillion estimated to have been stolen across all relief programs, only about $4 billion has been recovered—a sobering reminder of how much remains lost. Additionally, it has come to my attention that the expiration of the statute of limitations for prosecuting CARES Act-related unemployment insurance fraud will occur on March 27, 2025. Congress must act before the deadline to extend the statute to ensure continued prosecution of criminals who continue to defraud our nation's unemployment insurance programs.

The impact of this fraud extends far beyond the numbers. Each case of fraud is a person, a life, someone who needed help and was left without it because criminals exploited a system designed to help them. Fraud doesn't just drain taxpayer dollars; it leaves families, seniors, workers, and countless others waiting for months—or even years—for essential support they were entitled to receive.

## II. Nature and Scope of the Problem

**The pandemic placed an unprecedented burden on our social services and welfare programs, which were designed to help our nation's most vulnerable during times of crisis.** The rapid deployment of relief funds, paired with an abrupt shift to digital processing, inadvertently opened the

door to large-scale fraud. At first glance, this may appear to be a purely technical or financial issue. But the reality is far more troubling. Funds intended to support struggling Americans were instead diverted into the pockets of criminals, including organized crime syndicates, transnational networks, and hostile foreign states. This is not simply a financial oversight—it is a profound threat to our national security and a betrayal of public trust.

**A clear and disturbing pattern emerges when examining the fraud landscape.** These funds have been targeted not only by individual opportunists but by complex, organized entities spanning various levels. **In my estimation, there are four primary groups responsible for exploiting our public assistance programs, each with distinct motivations and methods.**

At the most localized level are **individuals I call "first-person fraudsters,"** who seize upon the system's vulnerabilities for personal gain. These people often overstate their lost income, fail to disclose re-employment, or otherwise misrepresent eligibility details, bending the rules to receive benefits to which they are not entitled. Although this form of fraud has existed within public assistance programs for years, the pandemic's economic strain has dramatically amplified it.

**The second group is perhaps more insidious: the Insider Threat.** These cases involve government employees entrusted with administering these programs who instead exploit their positions to facilitate fraud. Insider threats are particularly dangerous because they exploit the trust and authority granted to public servants, allowing employees to override controls, approve fraudulent claims, or even sell claimants' personal information for profit. We have seen these cases documented across a range of programs, from Unemployment Insurance to Supplemental Nutrition Assistance (SNAP) and Temporary Assistance for Needy Families (TANF). Each instance of insider fraud tarnishes the integrity of these programs, transforming essential safety nets into channels for exploitation and corruption.

A third, highly coordinated group comprises **domestic criminal organizations that have transformed public benefit fraud into a calculated, profitable enterprise.** These groups, ranging from local gangs to larger crime networks, systematically filed thousands of fraudulent claims using stolen Social Security numbers and other personal identifiers. For these organizations, the government's rush to release funds—coupled with temporary relaxations in eligibility verification—was an unprecedented opportunity. In Maryland, one organized ring filed over 47,000 false unemployment claims, extracting hundreds of millions of dollars. Profits from these fraudulent claims did not circulate within the economy or help support those in need; instead, they were reinvested into criminal enterprises, including narcotics, firearms, and other illicit activities. The impact is real and measurable. Just up the road in Baltimore, a significant connection between COVID-19 fraud and violent crime has been identified. Maryland U.S. Attorney Erek Barron reported that approximately 60% of violent criminals were also involved in some form of COVID-19-related fraud. By prosecuting these fraud cases, Baltimore experienced a 20% reduction in homicides and a 10% decrease in nonfatal shootings. This connection between relief fraud and broader criminal activity demonstrates the critical role that fraud prevention and enforcement can play in enhancing public safety.

Finally, **the most alarming element in this structure is the involvement of transnational fraud rings, terrorist organizations, and hostile nation-states.** The necessary pivot to digital, remote applications made it possible for international actors to access and exploit our systems from afar.

Reports indicate that as much as 70% of the fraudulent unemployment insurance claims filed during the pandemic originated overseas. Funds siphoned by these transnational groups were not redirected toward humanitarian or developmental causes; instead, they supported the most destructive elements of global crime. Some of the misappropriated funds have been traced to North Korea's nuclear weapons program, helping finance weapons of mass destruction. Moreover, links have been identified between these stolen funds and organized crime networks operating in countries like China, Nigeria, Iran, and Russia, further emphasizing the global scale of this exploitation.

The reach of these alliances is growing, as we see the increasingly frequent collaborations between Mexican drug cartels and China-based money-laundering operations. When domestic criminal groups align with international money launderers, the danger to both our national security and public safety increases exponentially. Funds meant to aid Americans have instead been used to strengthen and diversify these alliances, creating a more formidable criminal infrastructure that threatens not only our own citizens but also international stability. This is not a matter of minor technical improvements; it is a matter of reinforcing our defenses against adversaries who see our public resources as an easy target and whose motives directly oppose American values and security.

**While the challenges are significant, there are success stories that demonstrate what can be achieved through effective partnerships and targeted action.** In a Mid-Atlantic and a Midwest state for example, we worked closely with state agencies to curb rampant unemployment fraud, employing advanced identity verification, and real-time data analytics. Together, we were able to halt the extraction of fraudulent funds and redirect resources to legitimate claimants. The results were immediate and profound—not only did fraudulent claims decline dramatically, but the agencies were also able to serve their residents more effectively, providing a blueprint for what is possible on a national scale. These collaborations highlight the potential of proactive measures and robust partnerships in restoring integrity to these vital programs.

Each of these four criminal elements—whether individual opportunists, insider threats, domestic crime rings, or international actors—has exploited our systems in unique ways, creating a wake of harm that reverberates from struggling individuals to national security interests. The time to act is now, to protect public resources, rebuild trust, and defend against adversaries whose reach grows more complex and dangerous each day.

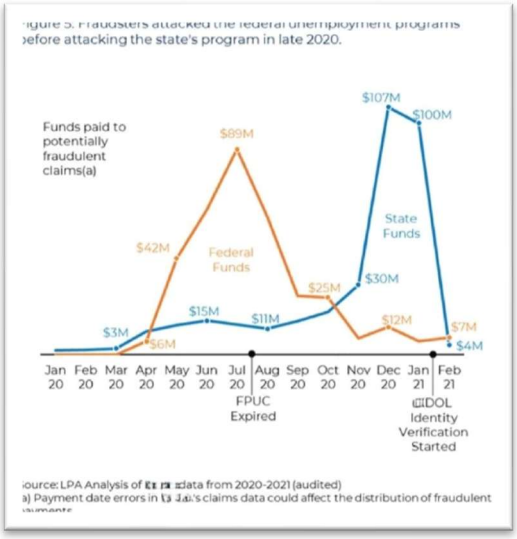


Diagram from a Midwest state audit of UI payments

Imagine for a moment that a single dollar misappropriated from unemployment benefits ends up contributing to the aforementioned dangerous causes. Now multiply that single dollar by hundreds of billions, and we begin to see the weight of this issue—not just as a loss of taxpayer money, but as a matter of national security.

## III. Causal Factors

The COVID-19 pandemic necessitated a rapid shift from traditional, in-person verification methods for unemployment insurance (UI) to online systems and call centers. This transition, while essential for public health, inadvertently created vulnerabilities that were swiftly exploited by criminals. The Government Accountability Office (GAO) estimates that fraudulent UI claims during the pandemic resulted in losses between $100 billion and $135 billion, accounting for approximately 11% to 15% of total UI benefits paid during that period. Some experts, me included, place this figure even higher—at over $250 billion.

Several key factors contributed to this surge in fraudulent activity:

**Stolen Identity and Data Breaches:** Over the past decade, data breaches have compromised the personal identifiable information (PII) of virtually every American. This data is already in the hands of criminal groups and hostile nation-states, waiting to be weaponized. Platforms like Telegram and Discord openly sell stolen financial accounts and personal information, making large-scale fraud accessible even to unsophisticated actors. The question is no longer whether this data will be used—it already has been and continues to be. Fraud rings and hostile nations are exploiting this stolen information to undermine public programs, jeopardizing billions in taxpayer funds and threatening national security.

**Lack of Effective Identity Verification Solutions:** The urgent need to process a massive influx of claims led many states to implement streamlined application processes, often at the expense of robust identity verification. Criminals quickly exploited these weaknesses, sharing successful tactics and strategies to bypass security measures, overwhelming call centers and outdated systems. Many states

and agencies relied on identity verification standards established as far back as 2017—standards that were not designed to address modern threats like AI-generated deep fakes and synthetic identities. Compliance with outdated standards does not equal security, and criminals using advanced tools can easily exploit these vulnerabilities.

This deluge of fraudulent applications siphoned off billions in funds and created significant backlogs, delaying assistance to legitimate claimants who desperately needed help. Even the Department of Labor has acknowledged the urgent need to modernize identity verification measures to combat this type of fraud.

**The Rise of Bot Attacks:** Cybercriminals have increasingly employed automated bots to flood state benefit systems with fraudulent claims. These bot attacks can submit thousands of applications in a short period, overwhelming system infrastructure and hindering the processing of legitimate claims. For instance, one state reported intercepting over 250,000 bot-generated applications in a single day after implementing advanced threat detection solutions. This highlights the scale of the problem and the necessity for robust cybersecurity measures to protect public resources.

**Self-Certification:** In an effort to expedite the distribution of benefits, some programs allowed applicants to self-certify their eligibility without requiring immediate verification, and this practice continues in many programs today. This policy opens the door to widespread fraud, as individuals submit false information with minimal risk of detection. Subsequent audits and investigations have consistently identified self-certification as a significant vulnerability that is persistently exploited.

Once fraudulent payments are disbursed, recovery becomes exceedingly difficult. The "pay and chase" model, where authorities attempt to recoup funds after they have been distributed, is largely ineffective. The rewards for criminals often outweigh the risks, especially when states lack the necessary tools and resources to pursue and prosecute these bad actors. Legislative measures, such as H.R. 1163, aim to encourage states to recover UI funds, but they do not sufficiently address the need for preventive measures prior to disbursement.

The convergence of widespread data breaches, inadequate identity verification processes, sophisticated cyber tactics like bot attacks, and policies permitting self-certification created a perfect storm that facilitated unprecedented levels of UI fraud during the pandemic. Addressing these vulnerabilities is crucial to safeguarding public funds and ensuring that assistance reaches those who truly need it.

## IV. How Criminals Stole Billions from Our Aid Programs

The pandemic era ushered in an unprecedented flow of government relief funds to millions of Americans, but with this influx came a dark undercurrent of exploitation. Opportunistic criminals, organized criminal networks, and even ordinary citizens looking for loopholes quickly discovered how easily these funds could be diverted. From exploiting identity verification flaws to circumventing lax security in digital applications, criminals saw the rapid rollout of these programs not as a safety net for those in need but as a prime opportunity for theft on a staggering scale.

The gaps in our system became both an invitation and a roadmap for fraud, as criminals recognized just how little oversight was being applied in the rush to get benefits to those affected by the pandemic. The scheme was not always sophisticated, nor did it require access to underground networks; even

rudimentary knowledge of stolen personal information could yield substantial financial rewards. And perhaps no case exemplifies the ease with which criminals gamed the system more than that of Eric Michael Jaklitsch, a New Jersey man whose audacious fraud scheme highlights both the vulnerabilities in our benefit programs and the desperate need for stronger safeguards.

Jaklitsch, a career criminal, exploited the most basic forms of identity verification to siphon millions from pandemic-related relief programs. His approach was shockingly simple. Using stolen personal data he obtained online, he crafted applications with real names, birthdates, and Social Security numbers. Jaklitsch did not just rely on others' identities; he went a step further, creating doctored state driver's licenses from New York, South Carolina, and California. In a disturbing yet absurd twist, he placed his own photo on these fake IDs, sometimes wearing an orange clown wig and makeup to avoid detection. To fulfill basic verification requirements, he uploaded selfies wearing the same costume, achieving an astonishing 87% success rate in passing identity checks.

State agencies, burdened by high application volumes and relying on outdated verification processes, accepted these false identities with little scrutiny. They issued prepaid debit cards loaded with benefits, which Jaklitsch then drained at ATMs across the region. What began as an investigation into a few hundred thousand dollars of fraud soon revealed far more extensive theft. Jaklitsch's schemes ultimately amassed known losses of $7.5 million in UI benefits alone, with authorities managing to recover only a fraction of that amount. Moreover, his fraudulent activities extended beyond UI; he also obtained nearly $1.3 million in Small Business Administration (SBA) Economic Injury Disaster Loans (EIDL), illustrating how pervasive these vulnerabilities are across various aid programs.

Jaklitsch's case highlights a profound systemic breakdown. The ease with which he was able to exploit the system exposed multiple points of failure: state agencies failed to validate the authenticity of uploaded driver's licenses; some licenses even lacked essential address details that would have been flagged by basic document authentication tools. In a glaring oversight, the system even processed applications linked to deceased individuals, with no checks in place to verify the applicant's status. This lack of validation extended beyond documents—email addresses associated with multiple claims went unchecked, debit cards were mailed to out-of-state locations without any historical ties to the listed identities, and suspicious IP addresses originating from other states were ignored.

At every step, the system seemed to roll out the red carpet for fraud, allowing Jaklitsch and others like him to manipulate and redirect funds with near impunity. Self-certification policies, designed for expediency, effectively handed criminals a blank check, enabling them to certify eligibility without oversight. Dangerous opportunists like Jaklitsch simply redirected benefits to drop locations and used tumbled email addresses to keep their schemes under the radar.


ID Verification Images (PII Redacted) Submitted for UI Claim in Name of A.R.


ID Verification Images (PII Redacted) Submitted for UI Claim in Name of R.C.

Jaklitsch's case may be a dramatic example, but it is by no means an isolated one. Across the country, criminals were taking advantage of these same vulnerabilities. Whether it was false identities or automated bots flooding systems with hundreds of thousands of claims, the overarching theme was clear: our infrastructure was unprepared for the digital demands of pandemic-era aid distribution, and criminals of all calibers capitalized on this unpreparedness. Without stringent identity verification, without proactive fraud detection, and without adequate inter-agency communication, our safety nets became a target for unprecedented theft.

## V. Empathetic Solutions to Combat Fraud in Public Benefit Programs

Fraud, waste, and abuse are not isolated issues but interconnected elements in a chain of systemic vulnerability. Addressing these challenges collectively is essential to restoring the integrity of our government programs and ensuring that benefits reach those who genuinely need them. One individual who has been at the forefront of this effort is Michael Horowitz, Chair of the Pandemic Response Accountability Committee (PRAC). The PRAC, established as part of the CARES Act, has led the charge in investigating fraud and mismanagement within pandemic relief efforts, highlighting how critical it is to view fraud prevention as part of a larger strategy to address fraud, waste, and abuse across federal programs.

As Horowitz noted in his testimony before Congress, the scale of pandemic-related fraud is unprecedented and demands a renewed focus on program integrity. According to Horowitz, the PRAC has not only exposed weaknesses in our benefits distribution systems but also identified key opportunities to strengthen oversight and prevent fraud before it occurs. At its core, this is a data problem—one that can be solved. We have the tools and technology to identify patterns, detect fraud in real time, and prevent funds from being misused. Despite these capabilities, we continue to rely on outdated practices, such as failing to share critical information between agencies and accepting self-reported data without sufficient verification.

The failure to share data across systems creates blind spots that criminals are eager to exploit. Self-reported information, left unchecked, is an open invitation for crime. This is not a question of whether solutions exist—they do. What is needed is the will to implement them. The PRAC's work serves as a stark reminder that fraud within public benefit programs is not just a budgetary issue but a solvable problem that requires modern solutions.

### Mandate Stronger Identity Verification Across Programs

Fraudulent claims were able to exploit a lack of stringent identity verification, especially as systems shifted online during the pandemic. Implementing multi-factor authentication and requiring both physical and digital identity verification across all benefit programs would set a strong foundation for fraud prevention. Private-sector industries like finance and healthcare have demonstrated how these techniques can protect resources while preserving ease of access. Imagine a benefits system that seamlessly verifies an applicant's identity in real time, cross-referencing personal information against secure databases, and catching anomalies before benefits are disbursed. These measures can prevent fraud at the entry point, supporting legitimate applicants without unnecessary delays.

### Eliminate Self-Certification and Rely on Real-Time Data Verification

Self-certification—allowing applicants to certify their own eligibility—was introduced as a way to streamline benefits distribution, but it created an environment ripe for fraud. Horowitz and the PRAC have repeatedly emphasized that reliance on self-attestation is one of the major weaknesses in pandemic-era relief programs. Agencies must pivot to real-time data verification, cross-checking self-reported information with external data sources to confirm eligibility. Real-time verifications can reduce fraud significantly, and by holding state agencies accountable for their verification processes, we ensure that benefits go to eligible individuals, not to those gaming the system. For those in genuine need, this approach offers both integrity and fairness, ensuring that only verified applicants receive support.

**Eliminate Broad-Based Categorical Eligibility (BBCE) To Address Fraud**

Current policies like Broad-Based Categorical Eligibility (BBCE) have unintentionally created pathways for fraud by using the lowest bar to entry as the standard for multiple programs, allowing eligibility in one program to automatically confer access to benefits across others—often without additional verification. This practice has led to cases where individuals who qualify for one program gain unverified access to multiple other benefits, bypassing crucial eligibility checks and opening the door to billions in fraud. To protect taxpayer resources and ensure program integrity, BBCE should be eliminated entirely.

**Front-End Prevention: Shift from "Pay and Chase" to Proactive Safeguards**

By the time fraud is identified, the funds have often been spent, making recovery difficult or impossible. To date, only a fraction—around $4 billion—of the estimated hundreds of billions stolen during the pandemic has been recovered, underscoring the futility of this approach. Rather than chasing lost dollars, we must focus on preventive measures. The PRAC's creation of the Pandemic Analytics Center of Excellence (PACE) has shown that data analytics can identify fraudulent patterns in real time, allowing agencies to flag suspicious claims before funds are disbursed. A front-end focus would save taxpayers billions and ensure that benefits reach genuine recipients promptly and securely.

**Declare Fraud and Mismanagement in Public Programs a National Emergency**

Over the past two decades, fraud, waste, abuse—across Medicaid, SNAP, Social Security, and various emergency programs—have collectively cost taxpayers more than $2.8 trillion, surpassing even all federal education spending. This is not a simple administrative issue; it is a national emergency that impacts millions of Americans and undermines the purpose of public benefit programs. Fraud and waste in these programs divert funds away from critical services, from education to infrastructure, and dilute the impact of aid intended for vulnerable citizens.

**A Commitment to Efficiency and Fairness for Recipients**

The reforms proposed here are not only about protecting taxpayer dollars; they are also about safeguarding the dignity and rights of honest applicants who depend on these programs. Modern verification and fraud detection systems can work in the background, making the process seamless for legitimate users while catching fraudulent claims. This approach respects the needs of those facing hardship, ensuring that they receive assistance without unnecessary bureaucratic obstacles. By focusing on ease of access and empathetic design, we can build a public benefits system that is both secure and user-friendly.

## VI. Conclusion

### Partnering to Build a Secure and Compassionate Benefits System

Thank you for the opportunity to discuss solutions to protect and strengthen our public assistance programs. Your commitment to addressing the challenges within these programs, safeguarding taxpayer resources, and ensuring that benefits reach those in need is essential. What you do every day is crucial for upholding the trust and wellbeing of your constituents, and it is with deep gratitude that I work alongside you in this mission.

The impact of pandemic-related fraud has reached every corner of our country. Hundreds of  Billions of taxpayer dollars were misappropriated, and legitimate claimants—the single parents, seniors, and unemployed workers—found their claims delayed or overshadowed by fraudulent applications. Criminals exploited overwhelmed systems, leading to backlogs that harmed those who rely on these lifelines most. As Amy Simon, Principal of Simon Advisory, wisely stated in her previous testimony, "suggesting that benefit timeliness and benefit accuracy must be opposing goals is a false dichotomy… all stakeholders have a vested interest in ensuring that fraud detection and prevention is an integral, permanent part of the program's mission." Fraud prevention and efficiency are not competing priorities; they are complementary, essential components of a trustworthy system.

This is about more than reducing fraud. It is about restoring integrity, honoring the American taxpayer, and ensuring that public resources reach the individuals who need them most. Every instance of fraud represents a person—a life disrupted, someone who counted on support and was denied or delayed because of exploitation in the system. By mandating stronger identity verification, enhancing real-time data checks, and adopting modern, user-centered security measures, we can create a system that is not only secure but also compassionate and accessible. These changes are an investment in a better, more dignified experience for those who seek help. They offer a guarantee that taxpayer dollars will serve their intended purpose and a promise that fraud will no longer undermine the vital programs our citizens rely on.

Recent calls from leaders like Senator Mike Crapo and Chairman Jason Smith emphasize the importance of transparency and accountability in this mission. Their unanswered request for clarity from the Department of Labor regarding the allocation of funds earmarked to combat unemployment insurance fraud underscores a broader need for focused, outcome-driven action. The question of how these funds are being spent—whether on robust fraud prevention measures or unrelated pilot programs—affects not only fraud prevention efforts but also public confidence in the government's ability to safeguard taxpayer dollars.

The task before us is clear. We must act decisively to implement common sense reforms. Congress has the power to lead the way, making fraud prevention and program integrity a national priority. By transitioning from a reactive "pay and chase" model to a preventive approach, we can stop fraud at the source, reduce fraud, and free resources to serve those who need them. This is an investment in our country's future, a demonstration of our shared commitment to the stewardship of public resources.

I stand ready to support you in this mission. With the right policies, technology, and collaboration, we can achieve a benefits system that embodies efficiency, security, and compassion—one that respects the

dignity of every honest applicant, safeguards taxpayer funds, and upholds the trust of the American people.

Sources:


- Rolling Stone: The Trillion-Dollar Grift: Inside the Greatest Scam of All Time, https://www.rollingstone.com/politics/politics-features/covid-relief-scam-fraud-money-billions-1234784448/
- California Globe: Exclusive: California EDD Fraud Money Paid for North Korea Nukes?, https://californiaglobe.com/fl/exclusive-california-edd-fraud-money-paid-for-north-korea-nukes/
- World Tribune: Fraud expert: Half of all U.S. Covid relief funds likely went to nations like China and Russia, https://www.worldtribune.com/fraud-expert-half-of-all-u-s-covid-relief-funds-likely-went-to-nations-like-china-and-russia/
- Rolling Stone: Scammers Stole $100 Billion in Pandemic Relief: Secret Service, https://www.rollingstone.com/politics/politics-news/secret-service-pandemic-relief-fraud-100-billion-1274931/
- The Hill: Maryland officials discover $501 million unemployment fraud scheme, Maryland officials discover $501 million unemployment fraud scheme.
- American Enterprise Institute, Amy Simon, Matt Weidinger: Pandemic Unemployment Fraud in Context: Causes, Costs, and Solutions, https://www.aei.org/research-products/report/pandemic-unemployment-fraud-in-context-causes-costs-and-solutions/
- American Enterprise Institute, Amy Simon, Matt Weidinger: Ten Findings from a Congressional Hearing on Pandemic Fraud, https://www.aei.org/center-on-opportunity-and-social-mobility/ten-findings-from-a-congressional-hearing-on-pandemic-fraud/
- American Enterprise Institute, Matt Weidinger: New Report Details Lessons from Massive Pandemic Unemployment Fraud, https://www.aei.org/center-on-opportunity-and-social-mobility/new-report-details-lessons-from-massive-pandemic-unemployment-fraud/
- US House Committee on Oversight and Accountability, 9/10/2024, Where Do We Go From Here? Examining a Path Forward to Assess Agencies' Efforts to Prevent Improper Payments and Fraud, https://oversight.house.gov/hearing/where-do-we-go-from-here-examining-a-path-forward-to-assess-agencies-efforts-to-prevent-improper-payments-and-fraud-2/
- GSA/Arvix Facial Biometrics Study: A large-scale study of performance and equity of commercial remote identity verification technologies across demographics, https://arxiv.org/pdf/2409.12318
- SSA OIG Self-Attestation: Supplemental Security Income Recipients Who Under-report Financial Account Balances, https://oig.ssa.gov/assets/uploads/a-02-21-51028.pdf
- The Register: GSA plows ahead with face matching tech despite its own reliability concerns, https://www.theregister.com/2024/10/10/gsa_plows_ahead_with_face/
- WBALTV: I-Team Exclusive: Drop in Baltimore homicides due to COVID-19 fraud prosecutions, US attorney says, Exclusive: Homicides drop linked to COVID-19 fraud prosecutions
- GAO: Unemployment Insurance: Estimated Amount of Fraud During Pandemic Likely Between $100 Billion and $135 Billion, Government Accountability Office
- Bleeping Computer: Telegram is a hotspot for the sale of stolen financial accounts, Bleeping Computer
- U.S. Department of Justice: New Jersey Man Pleads Guilty to Fraudulent Schemes to Steal California Unemployment Insurance Benefits and to Steal Economic Injury Disaster Loans, Eastern District of

California | New Jersey Man Pleads Guilty to Fraudulent Schemes to Steal California Unemployment Insurance Benefits and to Steal Economic Injury Disaster Loans | United States Department of Justice

- Senator Mike Crapo: Crapo, Smith Seek Basic Information on Labor Department's Fund to Combat Unemployment Insurance Fraud, Crapo, Smith Seek Basic Information on Labor Department's Fund to Combat Unemployment Insurance Fraud | U.S. Senator Mike Crapo.
- GAO: Improper Payments: Agency Reporting of Payment Integrity Information, Improper Payments: Agency Reporting of Payment Integrity Information | U.S. GAO