WRITTEN TESTIMONY OF HAYWOOD TALCOVE

CHIEF EXECUTIVE OFFICER, LEXISNEXIS SPECIAL SERVICES INC.

BEFORE THE U.S. SENATE

COMMITTEE ON HOMELAND SECURITY & GOVERNMENT AFFAIRS

SUBCOMMITTEE ON DISASTER MANAGEMENT, DISTRICT OF COLUMBIA, AND CENSUS

February 10, 2026

Protecting the Safety Net:
Combating Systemic Fraud to Defend Americans, Restore Trust, and Strengthen National Security

Chairman Hawley, Ranking Member Kim, and Members of the Subcommittee, thank you for the opportunity to testify on an issue that strikes at the heart of public trust, disaster readiness, national security, and the future of America's most essential government programs.

The United States has built one of the most expansive and compassionate social safety nets in the world. These programs exist to help families weather hardship, support workers in transition, protect children, and ensure dignity for the elderly and vulnerable. They are not partisan creations. They are American commitments.

Today, those commitments are under sustained and escalating attack.

Across the country, and most recently brought into sharp focus by events in Minnesota, government benefit programs have become prime targets for large-scale fraud. This is not a localized failure, a single program breakdown, or a reflection of individual wrongdoing by the people these programs are designed to serve. It is a systemic vulnerability and one that organized criminal networks and transnational fraud rings have learned to exploit with alarming speed and sophistication. In some cases, fraud is enabled not only by external actors, but by insider threats by employees, contractors, or trusted intermediaries who exploit access, weak controls, and outdated oversight mechanisms within these programs.

Fraud in government programs is no longer just a matter of waste or administrative mismanagement. It has become a strategic, national vulnerability, one that is magnified during disasters and emergencies, when speed is essential, oversight is strained, and billions of dollars must move quickly to help communities recover.

Criminal organizations now treat public benefit systems as low-risk, high-reward financial targets. Funds stolen from programs intended to help Americans have been traced to organized crime, drug trafficking, human exploitation, and, in some cases, terrorist-affiliated or hostile foreign actors seeking to undermine U.S. interests. At the same time, legitimate beneficiaries such as single parents, displaced workers, seniors, and people with disabilities are left waiting longer, facing increased scrutiny, or losing confidence in programs they depend on.

This is the quiet crisis behind the headlines:

Fraud steals twice: Once from taxpayers and once from the people these programs are meant to protect.

The scale of the problem is sobering. Federal agencies report hundreds of billions of dollars in improper payments each year across major programs. Once fraudulent payments are made, recovery is rare. The current "pay and

chase" model has proven incapable of keeping pace with modern, technology-enabled crime. Meanwhile, criminals adapt faster than government systems, exploiting outdated identity verification, siloed data, and policies designed for a different era.

The environment in which fraud is discovered has also fundamentally changed. In the age of social media, open data, and artificial intelligence, fraud is no longer uncovered only through audits and investigations. Citizen journalists, independent researchers, and data analysts can now surface systemic failures in real time and often faster than government processes designed for a slower, less transparent era. This new visibility is not a threat to public institutions; it is a reality of modern accountability. At the same time, the speed and reach of today's information ecosystem benefits criminals and opportunists as much as it informs the public, allowing fraud tactics to spread rapidly while incomplete or misleading narratives can distort public understanding before facts are fully established.

Recent legislation, including President Trump's One Big Beautiful Bill, reflects a clear recognition that program integrity must keep pace with the scale of generosity. By tying expanded benefits to stronger accountability and imposing real costs on states that fail to reduce fraud and improper payments Congress has made clear that generosity and integrity are not competing goals. These reforms elevate, rather than relax, the need for strong identity verification, continuous monitoring, and modern fraud controls to protect beneficiaries, taxpayers, and the long-term viability of these programs.

Yet this challenge is neither inevitable nor unsolvable.

Every day, the private sector moves trillions of dollars quickly and securely using risk-based identity verification, real-time analytics, and continuous monitoring to protect consumers while minimizing friction for legitimate users. These tools are not experimental. They are proven, widely deployed, and already used by financial institutions, healthcare systems, and critical infrastructure providers.

The central question before Congress is not whether we can protect benefit programs while ensuring access and dignity. We already know the answer is yes. The question is whether we will act with the urgency and coordination that this moment demands.

This testimony will outline:

- How systemic fraud evolved into a disaster-readiness and national security concern,
- Why existing approaches have failed to keep pace with modern threats, and
- How practical, bipartisan reforms grounded in proven technology and public–private cooperation can restore integrity, protect beneficiaries, and preserve these programs for future generations.

These programs are too important to fail, and too essential to the American people to remain easy targets for fraud. Integrity is not the opposite of compassion. It is what makes compassion sustainable.

When Disasters Reveal Systemic Weakness

The scale and persistence of fraud in government benefit programs did not emerge suddenly. What changed was visibility. Disasters and emergency responses forced federal and state systems to operate at speed, revealing weaknesses that had accumulated over many years.

During Hurricane Katrina, Superstorm Sandy, the COVID-19 pandemic, and subsequent disaster responses, agencies were required to deliver aid rapidly, often at unprecedented scale. Speed was essential, and flexibility was often prioritized to ensure assistance reached people in need. In many cases, those tradeoffs were justified. But they also exposed long-standing structural deficiencies in identity verification, eligibility validation, data sharing, and oversight.

Emergency conditions did not create fraud. They exposed systems that were not designed to distinguish legitimate applicants from sophisticated criminal actors operating from around the world.

Programs that relied heavily on self-attestation, infrequent verification, and fragmented data proved particularly vulnerable. As funding expanded and timelines compressed, those weaknesses became repeatable points of exploitation. Criminal activity that might previously have appeared as isolated improper payments began to exhibit consistent patterns across programs and jurisdictions.

Criminal networks adapted faster than government systems. Automated tools, stolen and synthetic identities, and coordinated application campaigns allowed fraud to scale rapidly across multiple benefit programs at once. These were not opportunistic acts by individuals reacting to crisis conditions. They reflected organized, professionalized activity that exploited predictable system behaviors.

The experience in Minnesota illustrates how fraud propagates when common controls fail under pressure. Fraud there was not confined to a single agency or program. It moved across multiple benefit systems, exploiting shared weaknesses in identity verification, oversight, and cross-program coordination. Minnesota's experience is instructive because the conditions that enabled fraud were not unique to that state. Similar structures and pressures exist elsewhere, particularly during periods of emergency response.

Federal oversight has consistently documented these vulnerabilities. For more than a decade, the Government Accountability Office has identified emergency spending and large entitlement programs as especially susceptible to fraud and improper payments when controls do not keep pace with scale. Recent GAO work, including undercover testing, has confirmed that known weaknesses remain exploitable. Fictitious identities, invalid documentation, and unauthorized intermediaries were able to gain access to benefits despite prior recommendations and corrective efforts.

Disasters also intensify the risk of insider abuse. While the vast majority of public servants act in good faith, complex programs create opportunities for a small number of employees, contractors, or intermediaries with privileged access to exploit weak controls. Limited real-time monitoring and delayed detection allow such misconduct to persist longer and cause greater harm. In the rush to get benefits out during a crisis, such as Hurricane Katrina, Irma, Helene, and even COVID – we loosen the limited oversight controls. This puts real needy families in the same line as fraudsters flocking to steal from unguarded programs, often to the frustration of the dedicated public servants at the county, state, and federal level who show up every day trying to help make someone's lives betters. Meanwhile, fraud flourishes and grows, putting families farther and farther back in line.

At the same time, the environment in which fraud is identified has changed. Fraud is no longer uncovered only through audits or investigations conducted months or years after the fact. Citizen journalists, independent analysts, and researchers increasingly identify anomalies using public records, open data, and digital tools. This has shortened the gap between system failure and public exposure.

That same information environment accelerates exploitation. Fraud tactics spread quickly, tools are reused across jurisdictions, and incomplete or misleading narratives can take hold before facts are fully established. Speed now benefits both accountability and criminal adaptation.

The lesson from recent disasters is not that government should slow aid or retreat from generosity. It is that integrity must be treated as a core component of disaster readiness. Systems that cannot verify identity, monitor risk continuously, and adapt to evolving threats will fail. When that happens, aid is delayed, trust erodes, and taxpayer dollars intended for recovery are diverted elsewhere.

These failures are not inevitable. But they will persist unless program integrity is treated as infrastructure rather than an after-the-fact correction.

How Fraud Operates at Scale Today

Modern fraud in government benefit programs is not accidental, sporadic, or opportunistic. It is organized, repeatable, and increasingly professionalized. Understanding how it operates is essential to understanding why traditional controls have failed.

At the core of most large-scale fraud schemes is identity compromise. Criminal actors use stolen, synthetic, or manipulated identities to access programs designed to rely on trust and speed. Synthetic identities, which combine real and fabricated information, are particularly difficult to detect using single-point verification methods. Once an identity is accepted into a system, it can be reused, modified, or scaled across multiple programs.

These schemes are rarely limited to a single application or benefit. Criminal networks test systems to identify weaknesses, then replicate successful methods across jurisdictions and programs. Automated tools allow thousands of applications to be submitted in minutes, often from outside the United States. What appears to administrators as a surge in demand can, in reality, be coordinated fraud activity exploiting predictable system behavior.

Insider access can significantly amplify this risk. Employees, contractors, or intermediaries with legitimate credentials may intentionally or negligently bypass controls, suppress alerts, or facilitate unauthorized access. In complex systems administered at scale, even a small number of compromised insiders can enable disproportionate losses before detection occurs.

Fraud is further enabled by fragmented data and limited cross-program visibility. Eligibility determinations are often made in isolation, without real-time checks against other programs, agencies, or jurisdictions. Requiring matches against deficient federal databases only checks a box, with criminals using those blind spots and program vulnerabilities to enrich themselves. This allows the same identity to receive benefits simultaneously from multiple sources, even when eligibility rules prohibit it. Delayed data matching and post-payment audits frequently identify problems only after funds have been disbursed and recovered rarely. In fact, according to HHS Administration for Children & Families, last February they found over 3.2 million unique individuals receiving Medicaid benefits in other states… over 6.6 million times. And that didn't even include all states, but that's billions of dollars in easily preventable dual participation – much of it fraud, all of it waste.

Technology has accelerated every stage of this process. Artificial intelligence and automation now allow criminals to generate realistic documentation, adapt application narratives, and respond dynamically to system changes. Fraud tactics evolve quickly, often faster than policy updates or procurement cycles can respond. Once a method proves effective, it is shared, reused, and refined.

Intermediaries can also play a role. In some programs, third parties assist applicants with enrollment or claims. While many serve legitimate purposes, weak oversight can allow unauthorized or abusive practices, including enrollment without consent, manipulation of applicant information, or submission of fraudulent claims.

The cumulative effect of these mechanisms is systemic exposure. Fraud losses are not simply the result of individual bad actors slipping through the cracks. They reflect structural conditions that reward speed without verification, scale without coordination, and trust without continuous validation.

Importantly, these same weaknesses do not only enable fraud. They also increase friction for legitimate applicants. As losses grow, agencies respond by adding paperwork, delays, and manual reviews that disproportionately burden those who rely on these programs most. In this way, ineffective fraud controls harm both program integrity and program access. Putting safeguards in place will identify and stop fraud, while expediting the delivery of services to real eligible recipients with increased speed and reduced errors and improper payments.

This operating environment explains why after-the-fact enforcement has proven insufficient. Once funds are disbursed, recovery is rare. Investigations are costly, time-consuming, and often limited by jurisdictional boundaries. The result is a system that absorbs losses rather than preventing them.

Understanding how fraud operates clarifies what reform must address. The issue is not a lack of rules or good intentions. It is a mismatch between modern threats and outdated controls. Until that mismatch is resolved, fraud will continue to adapt faster than the systems designed to stop it.

The Human and Institutional Cost of Systemic Fraud

The consequences of large-scale fraud extend well beyond financial loss. When fraud becomes systemic, it reshapes how programs operate, how agencies behave, and how the public experiences government assistance.

For legitimate beneficiaries, the cost is often delay, confusion, and diminished access. As fraud increases, agencies respond by tightening procedures, adding documentation requirements, and slowing approvals. These measures are typically applied broadly, rather than surgically, because systems lack the ability to distinguish risk in real time. The result is that individuals who are eligible and in need face longer wait times, repeated requests for information, and greater uncertainty at moments of crisis.

In disaster settings, these delays are not inconveniences. They can mean the difference between stability and displacement, between recovery and prolonged hardship. When assistance arrives late or inconsistently, trust erodes quickly, particularly among communities that rely most heavily on timely support.

Systemic fraud also distorts program administration. Resources that should be dedicated to service delivery are diverted to manual reviews, retroactive audits, and recovery efforts that rarely succeed. Staff are asked to manage growing backlogs while responding to public scrutiny and political pressure. Over time, this environment contributes to burnout, turnover, and risk aversion, further degrading program performance.

At the state level, the impact is compounded. States administer many federal programs under tight timelines and with limited flexibility. When fraud levels rise, states face increased oversight, financial penalties, or retroactive disallowances, even when underlying vulnerabilities stem from shared federal and state systems. This dynamic strains federal-state relationships and discourages innovation, as administrators prioritize compliance over effectiveness.

Fraud also undermines public confidence. Taxpayers who see repeated reports of abuse question whether programs are professionally managed or sustainable. Beneficiaries who encounter delays or denials question whether the system is responsive or fair. Over time, this erosion of trust fuels polarization around programs that depend on broad public support to survive.

These outcomes are not inevitable results of generosity. They are the predictable consequences of systems that lack effective front-end controls, real-time monitoring, and adaptive risk management. When integrity mechanisms fail, the burden shifts downstream to beneficiaries, administrators, and taxpayers alike.

In this sense, fraud prevention is not merely a financial safeguard. It is a prerequisite for equitable access, operational stability, and long-term program viability. Systems that cannot manage risk effectively ultimately harm the people they are intended to help.

Understanding these human and institutional costs is essential to evaluating reform options. The question before policymakers is not whether to choose between access and integrity. It is whether to design systems capable of delivering both.

What the Evidence Shows and Why “Pay and Chase” Fails

Evidence from federal oversight bodies consistently shows that large-scale fraud and improper payments are not isolated anomalies. They are predictable outcomes when program controls do not keep pace with scale, speed, and complexity.

The Government Accountability Office has identified improper payments as a high-risk issue across federal programs for more than two decades. Year after year, GAO has reported hundreds of billions of dollars in improper payments across major benefit programs, particularly those that are means-tested, rapidly scaled, or administered through complex federal–state partnerships. These findings are not limited to accounting errors. They include payments made to ineligible recipients, payments made using invalid or fictitious identities, and payments made without sufficient documentation to verify eligibility.

Recent GAO work has reinforced these conclusions through direct testing. Undercover and investigative efforts have demonstrated that fictitious identities, invalid Social Security numbers, and unauthorized intermediaries can still gain access to benefits, even after years of corrective recommendations. These findings confirm that known weaknesses in identity verification, eligibility checks, and oversight mechanisms remain exploitable.

Despite this evidence, the dominant response to fraud has remained reactive. Funds are disbursed first, and attempts at recovery follow later through audits, investigations, and enforcement actions. This "pay and chase" model assumes that losses can be recovered after the fact and that deterrence will limit future abuse. In practice, it has proven ineffective.

Once fraudulent payments are made, recovery rates are low. Funds are often transferred quickly, moved across jurisdictions, or sent overseas. Investigations are time-consuming and resource-intensive, and they frequently occur long after the initial payment. Even when fraud is identified, the cost of recovery can exceed the amount recovered, particularly in cases involving sophisticated networks or synthetic identities.

The limitations of this approach are most visible during emergencies. Disasters require rapid disbursement of funds at scale, often under relaxed verification standards. These conditions create an environment in which fraudulent claims can be submitted and paid faster than oversight mechanisms can respond. By the time irregularities are detected, funds have already been absorbed into criminal operations, and recovery is unlikely.

Evidence also shows that increased enforcement after the fact does not meaningfully reduce future fraud when underlying vulnerabilities remain unaddressed. Criminal actors adapt quickly, modifying tactics to evade detection while continuing to exploit the same structural weaknesses. As a result, agencies find themselves repeating the same cycle: surge spending, post-payment review, limited recovery, and renewed exposure during the next crisis.

This reactive model also imposes costs on legitimate participants. Post-payment audits, retroactive eligibility reviews, and benefit clawbacks can affect individuals who acted in good faith, creating confusion and hardship long after assistance was received. These processes further erode trust and increase administrative burden without addressing the root causes of fraud.

The evidence is clear. Fraud prevention strategies that rely primarily on after-the-fact detection and recovery cannot succeed at scale. Effective oversight must occur before and during payment, not months or years later. Until program integrity is integrated into the front end of benefit delivery, losses will continue to accumulate, particularly during periods of emergency response.

Understanding why "pay and chase" fails is essential to understanding what must replace it. The next section outlines approaches that have proven effective in other high-risk environments and explains how those lessons can be applied to government benefit programs without sacrificing access or speed.

What Works and Why Prevention Outperforms Recovery

The failure of reactive enforcement does not mean that fraud at scale is unavoidable. In other sectors that manage high-volume, high-risk transactions, prevention rather than recovery has long been the dominant approach.

Financial institutions, healthcare systems, and critical infrastructure providers operate in environments where speed, scale, and security are all essential. These sectors move trillions of dollars each day while maintaining relatively low fraud rates by integrating risk-based controls at the point of transaction rather than relying on post hoc review. The lesson is not that government should emulate private industry wholesale, but that certain principles are transferable.

Effective prevention begins with identity integrity. Programs that verify identity at the front end are far better positioned to distinguish legitimate applicants from fraudulent ones before funds are disbursed. Modern identity verification does not rely on a single data point or document. It uses layered signals, cross-referenced data, and risk-based assessment to establish confidence while minimizing friction for low-risk users.

This distinction matters because many government programs still treat submitted documentation as proof. Fraud actors have adapted by fabricating the proof itself. Pay stubs, invoices, tax filings, and business records that appear complete may have no connection to real activity. In an era of AI-assisted document creation, reliance on paperwork alone has become a structural vulnerability rather than a safeguard.

Prevention also requires continuous monitoring. Eligibility is not static, and risk does not end once an application is approved. Systems that reassess risk over time are better able to detect anomalies, identify emerging fraud patterns, and intervene before losses escalate. This approach reflects the reality that fraud adapts and that controls must adapt with it.

Importantly, prevention improves access when implemented correctly. Risk-based systems allow agencies to streamline processing for the majority of applicants who present low risk, while directing additional scrutiny only where indicators warrant it. This targeted approach reduces delays, minimizes unnecessary documentation requests, and improves the experience for legitimate beneficiaries, particularly during emergencies.

Evidence shows that front-end controls also reduce downstream enforcement burdens. When fewer fraudulent payments are made, agencies spend less time on audits, investigations, and recovery efforts that rarely succeed. Resources can be redirected toward service delivery, oversight of high-risk cases, and program improvement.

Public–private collaboration can support this shift when structured appropriately. Government programs already rely on private entities for payment processing, data management, and service delivery. Applying proven fraud prevention capabilities through competitive, transparent, and auditable arrangements can accelerate modernization without locking agencies into rigid or proprietary solutions. Federal standards combined with state flexibility can further ensure that prevention efforts respect local conditions and program requirements.

Safeguards remain essential. Any prevention strategy must include clear limitations on data use, strong privacy protections, and accountability for vendors, intermediaries, and insiders. Risk-based systems should be regularly evaluated for accuracy, bias, and unintended consequences. Oversight must be continuous, not assumed.

The contrast between prevention and recovery is not philosophical. It is operational. Systems designed to verify identity and activity before payment are more resilient during disasters and less dependent on paperwork that can be manufactured at scale. Systems that rely on recovery accept losses as inevitable and shift the burden onto taxpayers, administrators, and beneficiaries alike.

The evidence from other high-risk environments is clear. Prevention works when it is treated as core infrastructure rather than an optional enhancement. The challenge for government programs is not inventing new tools. It is integrating proven approaches into systems designed for a different era.

Preserving the Safety Net Through Integrity and Accountability

The evidence presented in this testimony leads to a clear conclusion. Fraud in government programs is not a marginal problem, nor is it confined to periods of crisis. It is a persistent vulnerability that becomes most visible during disasters, when systems are stressed, funds move quickly, and weaknesses are exploited. Left unaddressed, it erodes public trust, harms legitimate beneficiaries, and diverts taxpayer dollars away from their intended purpose.

The challenge now is execution.

Laws alone do not prevent fraud. Programs succeed or fail based on how they verify identity, validate eligibility, monitor risk, and adapt to evolving threats. When systems rely on static rules, paper documentation, and after-the-fact recovery, losses become predictable. When integrity is treated as core infrastructure, programs are more resilient, more equitable, and better able to deliver aid quickly when it is needed most.

Responsibility for this outcome is shared. Federal agencies must set clear standards and provide the tools necessary to meet them. States must be empowered and expected to administer programs with effective controls

and measurable results. Private-sector capabilities can support modernization when used transparently and with appropriate safeguards. Oversight must remain continuous, not episodic.

None of these steps require abandoning access or slowing assistance. On the contrary, systems that distinguish risk effectively can reduce friction for legitimate participants while focusing scrutiny where it is warranted. Integrity, when designed correctly, strengthens rather than constrains the safety net. It's time we make stewardship and integrity of these programs a priority with funds to move these efforts to the front-end.

The cost of inaction is not abstract. Fraud losses compound over time, confidence declines, and the burden shifts to taxpayers, administrators, and the people these programs exist to serve. In the most serious cases, stolen funds fuel organized crime and hostile activity that directly undermines American interests. Preventing those outcomes is a matter of governance, fiscal responsibility, and national security.

The United States has built programs that millions of Americans depend on in moments of hardship and disaster. Preserving them requires more than continued funding. It requires systems worthy of the trust placed in them.

Integrity is not the opposite of compassion. It is what makes compassion sustainable.

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.
- Office of the Governor of New Hampshire - Governor's Commission on Government Efficiency (COGE) Governor's Commission on Government Efficiency (COGE) | Governor Kelly Ayotte
- GAO: Improper Payments: Agency Reporting of Payment Integrity Information, Improper Payments: Agency Reporting of Payment Integrity Information | U.S. GAO
- GAO: Fraud Risk Management:2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments, Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments | U.S. GAO
- GAO: Improper Payments: Information on Agencies' Fiscal Year 2024 Estimates: Improper Payments: Information on Agencies' Fiscal Year 2024 Estimates | U.S. GAO
- Paragon Health Institute: GAO Probe Finds ACA at High Risk for Fraud: 96% of Fake Applications Approved: GAO Probe Finds ACA at High Risk for Fraud: 96% of Fake Applications Approved - Paragon Health Institute
- US House of Representatives: House Committee on Ways and Means, Subcommittee on Work and Welfare hearing entitled, "Time's Running Out: Prosecuting Fraudsters for Stealing Billions in Unemployment Benefits from American Workers." House Hearing on Prosecuting Unemployment Benefit Fraud
- US House of Representatives: House Committee on Oversight and Government Reform, Subcommittee on Delivering on Government Efficiency hearing entitled, "The War on Waste: Stamping Out the Scourge of Improper Payments and Fraud.": House Hearing on Stamping Out Improper Payments and Fraud
- The National Desk: In the trenches fighting fraud against the government: In the trenches fighting fraud against the government
- CBS News: Go behind the scenes to see how VISA thwarts scams as fraud increases: Go behind the scenes to see how VISA thwarts scams as fraud increases - CBS News
- National Review: Newsom Has His Own Massive State Fraud Problem: California Governor Gavin Newsom Faces Massive State Fraud Problem | National Review