WRITTEN TESTIMONY OF HAYWOOD TALCOVE CHIEF EXECUTIVE OFFICER, LEXISNEXIS SPECIAL SERVICES INC. BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM SUBCOMMITTEE ON DELIVERING ON GOVERNMENT EFFICIENCY

February 12, 2025

1. Introduction

Chairwoman Greene, Ranking Member Stansbury, and members of the Subcommittee, thank you for the opportunity to testify before you today on the urgent need to combat **fraud**, **waste**, **and abuse** (**FWA**) in government programs. Over the past two decades, improper payments have reached crisis levels, eroding public trust, siphoning billions away from those who truly need assistance, and burdening taxpayers with systemic inefficiencies.

I am Haywood Talcove, CEO of LexisNexis Risk Solutions for Government. My team and I work with federal and state agencies to stop fraud before it happens, streamline government operations, and protect taxpayer resources. Today, I will outline the scale of fraud and improper payments across multiple programs, highlight proven solutions, and emphasize the urgency of bold, decisive action to eliminate inefficiencies in federal programs.

Since 2003, federal agencies have reported approximately \$2.7 trillion in cumulative improper payments, a staggering figure that underscores the persistent vulnerabilities across government programs. In fiscal year 2023 alone, improper payments totaled \$236 billion, spanning over 71 federal programs. The scope of this problem is not limited to any single agency or initiative—Medicaid, Medicare, Unemployment Insurance, and SNAP continue to be plagued by fraud, mismanagement, and outdated verification systems that allow ineligible recipients and criminal networks to exploit loopholes.

The Paycheck Protection Program and expanded Unemployment Insurance programs during the COVID-19 pandemic further exposed deep weaknesses in oversight and allowed foreign and domestic fraud rings to siphon away billions of taxpayer dollars. Yet, pandemic-era fraud was only a symptom of a broader, long-standing issue. Even before the pandemic, programs like the Earned Income Tax Credit (EITC) had improper payment rates exceeding 25%, while Medicaid and Medicare consistently accounted for tens of billions in misallocated funds annually.

To truly address this crisis, we must move beyond the failed "pay and chase" model, where agencies attempt to recover funds long after they have been stolen. Instead, we must leverage identity verification AND authentication, public-private partnerships, and investments in fraud detection. The private sector has already demonstrated the effectiveness of these tools in stopping fraud before it occurs, and it is imperative that government agencies adopt them at scale.

Without decisive action and strategic investment, we will continue to see systemic fraud drain resources from vital programs, delay assistance for those in need, and erode public trust in government

institutions. The **War on Waste** must begin with data-driven, front-end solutions that modernize fraud prevention efforts. The time to act is now.

II. The Pandemic Exposed—But Did Not Create Systemic Fraud

While the COVID-19 pandemic placed an unprecedented burden on social services, it did not create the fraud crisis—it merely revealed the full scale of it. The vulnerabilities exploited during pandemic-era relief programs were not new; they existed for decades across Medicaid, Medicare, Unemployment Insurance, SNAP, and other federal assistance programs. The rapid disbursement of pandemic funds simply magnified these weaknesses, turning government programs into a high-value target for criminals.

The numbers prove this fraud extends well beyond emergency relief efforts. Since 2003, the federal government has reported over \$2.7 trillion in improper payments, with \$236 billion lost in 2023 alone. Medicaid remains one of the worst offenders, with over \$50 billion in improper payments in 2023, while Unemployment Insurance saw \$44 billion in losses last year alone. These figures dwarf even the worst fraud estimates from pandemic programs and demonstrate that the federal government remains one of the largest, easiest financial targets in the world.

Transnational fraud rings, terrorist organizations, and domestic criminal enterprises have turned public benefit fraud into a permanent, highly profitable business model. These groups have moved beyond pandemic relief and now target core social programs with the same tactics—leveraging stolen identities, synthetic identities, and insider collusion to siphon off billions from American taxpayers.

A clear example of the systemic nature of this fraud is the **National Accuracy Clearinghouse** (NAC). The NAC pilot program has already identified **over 14 million cases of duplicate participation** in Medicaid, SNAP, and TANF, preventing billions in improper payments. Yet, <u>despite congressional mandates for nationwide implementation</u>, the USDA continues to delay full adoption, allowing fraud to persist unchecked.

The pandemic did not cause this crisis—it merely exposed what criminals already knew: The U.S. government's outdated, disconnected fraud prevention systems make it the largest financial target in the world. Until agencies move beyond their reactive "pay and chase" model and implement real-time fraud detection and identity verification, the theft of taxpayer funds will continue at an unprecedented scale.

This is not simply a financial oversight—it is a profound threat to our national security and a betrayal of public trust.

The Most Dangerous Exploiters of Public Assistance: Organized Crime, Insider Threats, and Nation-State Actors

Public assistance programs have become a **primary target for fraud**, exploited by a wide array of bad actors. While individual opportunists have always taken advantage of loopholes to misrepresent income or claim unearned benefits, they are not the biggest threat to the integrity of these programs. The most insidious fraud comes from highly **organized**, **systemic exploitation**—perpetrated by **insider threats**, criminal organizations, and transnational fraud networks, including hostile nation-state actors.

The **insider threat** is particularly alarming because it operates from within the system itself. These cases involve government employees—individuals entrusted with administering benefits—who instead use their positions to approve fraudulent claims, override security controls, or even sell sensitive claimant information for profit. Insider fraud is not a hypothetical risk; we have already seen it deeply embedded in federal and state programs, including Unemployment Insurance, SNAP, and TANF. Each instance of

insider corruption does more than steal funds—it undermines public trust and creates a roadmap for criminals to exploit gaps in the system further.

More alarming still is the role of domestic and transnational criminal organizations. These are not small-scale fraudsters filing a handful of false claims—they are highly structured operations that treat government benefits as a business model. Organized crime groups, from street gangs to large-scale financial crime networks, systematically submit tens of thousands of fraudulent claims using stolen or synthetic identities. These schemes generate hundreds of millions in illicit profits, which are then reinvested in drug trafficking, human smuggling, weapons distribution, and violent crime.

The connection between public assistance fraud and violent crime is undeniable. In Baltimore, investigators found that 60% of violent criminals had also committed COVID-19 relief fraud. By aggressively prosecuting these cases, the city saw a 20% drop in homicides and a 10% decrease in nonfatal shootings—proving that fraud enforcement is a public safety issue as much as a financial one.

However, the most dangerous exploiters of government benefits are **transnational fraud rings**, **terrorist organizations**, and hostile nation-states. The shift to digital application processes has made it easier than ever for international actors to penetrate U.S. assistance programs from abroad, stealing billions with minimal risk. Reports indicate that as much as 70% of fraudulent unemployment claims filed during the pandemic originated overseas. These stolen funds did not simply line the pockets of criminals—they have been linked to North Korea's nuclear weapons program, funding weapons of mass destruction. Similar fraud pipelines have been traced to China, Nigeria, Iran, Romania, and Russia, where state-backed and organized crime networks collaborate to launder stolen U.S. government funds.

The scale of these international operations is growing, with criminal organizations working hand-in-hand with money-laundering networks to siphon funds from U.S. assistance programs. The U.S. government is not just losing money—it is inadvertently funding global instability and empowering adversaries.

Without aggressive enforcement, real-time fraud detection, and stronger identity verification measures, these organized networks will continue exploiting taxpayer-funded programs at an unprecedented scale. Fraud prevention is no longer just a financial necessity—it is a national security imperative.

III. Causal Factors

The COVID-19 pandemic accelerated the longstanding shift away from traditional, in-person verification methods for unemployment insurance (UI) toward digital systems and remote processing. While this transition was necessary for public health and efficiency, it exposed and amplified vulnerabilities that had existed for years. Criminals quickly capitalized on outdated identity verification protocols, weak fraud detection measures, and a lack of real-time data-sharing between state agencies, turning UI into one of the largest financial targets in modern history.

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. However, many experts—including myself—place this figure significantly higher, exceeding \$250 billion when factoring in organized transnational fraud, identity theft, and widespread exploitation of temporary program waivers.

These staggering losses were **not merely a pandemic-era phenomenon**. The same systemic flaws that enabled UI fraud—weak identity verification, reliance on self-certification, and a failure to detect cross-state duplicate claims—continue to exist in other major benefit programs today, including Medicaid,

SNAP, and disaster assistance funds. Criminals have simply redirected their efforts to exploit the same weaknesses in different agencies. Until government fraud prevention efforts match the sophistication of today's financial crime networks, taxpayer dollars will continue to be funneled away from legitimate recipients and into the hands of fraudsters.

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 Steal Billions from Our Aid Programs

The pandemic-era flood of relief funds was meant to provide urgent assistance, but it also opened the flood gates for fraud. Criminals—from career fraudsters to organized crime networks—exploited identity verification gaps and lax security in digital applications, treating these programs not as a safety net, but as a jackpot.

No case illustrates this systemic failure better than Eric Michael Jaklitsch, a New Jersey criminal who exploited the weakest links in identity verification to steal millions from pandemic relief programs. His scheme was brazen yet simple: using stolen identities, he applied for benefits under multiple names, fabricating state driver's licenses and even submitting selfies in disguise—at times donning an orange clown wig and makeup—to evade detection. Shockingly, he passed identity checks 87% of the time.

State agencies, overwhelmed and relying on outdated verification systems, issued prepaid debit cards with little scrutiny, allowing Jaklitsch to withdraw millions from UI benefits and \$1.3 million in SBA loans before authorities caught on. The system failed at every level—from approving fraudulent documents with missing details to ignoring duplicate email addresses, suspicious IP addresses, and out-of-state debit card shipments. Even applications tied to deceased individuals sailed through with no verification.

This was not an isolated case—it was a roadmap for fraud. Jaklitsch's success was made possible by self-certification policies, weak identity controls, and an overall lack of oversight that enabled criminals to siphon billions with ease. His case is a stark warning: without modern fraud prevention tools, real-time data verification, and stricter oversight, our government assistance programs will remain prime targets for exploitation.









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 dramatic, but it is far from unique. Across the country, criminals exploit these same systemic weaknesses across longstanding federal and state benefit systems. They use false identities, synthetic profiles, and automated bots to flood agencies with hundreds of thousands of fraudulent claims, overwhelming outdated verification processes. But this was not just a failure of pandemic-era aid distribution—it was a **broader indictment of how unprepared our public assistance infrastructure has been for the digital age**. The same vulnerabilities that allowed pandemic fraud to flourish have persisted for decades in Medicaid, Unemployment Insurance, and nutrition assistance programs, costing taxpayers hundreds of billions annually. Without stringent identity verification, proactive fraud detection, and real-time interagency data sharing, these safety nets have not just been exploited during crises—they remain an ongoing and lucrative target for criminals at every level.

V. Expanding State-Level Efforts to Combat Fraud and Strengthen Oversight

Fraud prevention and financial accountability are not just federal responsibilities—states play a central role in administering federal funds and must take proactive steps to modernize oversight, close eligibility loopholes, and prevent improper payments before they occur. While the federal DOGE model has demonstrated the effectiveness of data-driven fraud prevention, many states still lack the technological infrastructure and coordination needed to detect fraudulent claims in real time. Without robust state-level action, improper payments will continue to drain public resources and weaken public trust in government programs.

To address these challenges, states must prioritize fraud prevention as a fundamental component of financial management, integrating real-time data sharing, predictive analytics, and automated verification systems across all state-administered federal programs. Establishing independent state commissions on government efficiency, improving interagency collaboration, and adopting private-sector best practices can drastically reduce fraud and ensure taxpayer dollars are directed to their intended purpose.

Recognizing the urgent need for reform, New Hampshire Governor Kelly Ayotte issued Executive Order #1, establishing a Commission on Government Efficiency to eliminate waste, modernize government operations, and strengthen financial oversight.

"I am proud to bring together business leaders and state government officials to make our state government more efficient and effective for all of New Hampshire," Governor Ayotte stated.

By implementing state-level DOGE strategies, New Hampshire is taking a proactive approach to financial accountability, ensuring taxpayer funds are used efficiently and effectively. The challenges New Hampshire faces are not unique—every state must adopt similar measures to safeguard public resources and restore fiscal discipline.

States that fail to act will continue to experience rising improper payments, strained budgets, and weakened public confidence in government administration. The federal government cannot fight fraud alone—states must step up, implement modern oversight measures, and work in partnership with federal agencies to protect taxpayer dollars at every level of government.

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-World 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 pandemicera relief programs. Agencies must pivot to real-time data verification, cross-checking self-reported information with external data sources to confirm eligibility. Real-world 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.

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: Investing in Integrity, Saving Billions

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 public trust and ensuring the well-being of millions of Americans, and it is with deep gratitude that I collaborate with you in this mission.

The impact of fraud has reached every corner of our country—not just during the pandemic, but over decades. Systemic failures in program integrity have resulted in trillions of dollars in improper payments, siphoning resources away from those who need them most. The pandemic simply exposed the scale of this crisis, proving that government agencies, lacking modern fraud prevention tools, have become the biggest financial targets in the world.

As criminals evolve their methods, so must we. We must abandon the false choice between SPEED and SECURITY in program administration. 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 essential to each other.

The **return on investment** is undeniable. A modest investment in fraud prevention technology can save billions by preventing improper payments before they occur. The private sector has already demonstrated these best practices, using real-time identity verification, advanced analytics, and cross-sector collaboration to stop fraud before it happens. Government agencies must follow suit and adopt data-driven strategies that ensure funds go only to eligible recipients. Public-private partnerships will be key to this transformation. The private sector has invested in fraud detection for decades, continuously refining technology to outpace bad actors. By working alongside industry leaders, government agencies can rapidly deploy solutions that eliminate systemic inefficiencies, strengthen program integrity, and protect taxpayer dollars at scale.

This is not just an opportunity for reform—it is an obligation. Congress must act now to modernize program oversight, mandate real-time fraud prevention measures, and demand agency accountability. These actions are not merely cost-saving measures—they are essential investments in the long-term sustainability and trustworthiness of government programs. By mandating stronger identity verification, enhancing real-time data checks, and fostering collaboration between public and private sectors, we can create a system that is not only secure, but also compassionate, accessible, and resilient. These changes offer a guarantee that taxpayer dollars will serve their intended purpose and a promise that fraud will no longer undermine the vital programs that millions rely on.

The time for reform is now. 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 while protecting the most vulnerable among us.

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, <u>Bleeping Computer</u>
- 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