Testimony of Linda Miller
Government Operations Subcommittee

House Committee on Oversight and Government Reform
March 31, 2022

Committee Chairman Connolly, Ranking Member Hice, and esteemed members of the Committee, my name is Linda Miller, and I am pleased to be here today to share my perspectives on enhancing the government's efforts to prevent, detect and respond to fraud and improper payments. I am currently a Principal at Grant Thornton, LLP, where I lead the firm's Fraud & Financial Crimes Practice. I also bring to bear my former experience both as an Assistant Director in the Forensic Audits and Investigative Service group at The Government Accountability Office (GAO), as well as my former role as the Deputy Executive Director of the Pandemic Response Accountability Committee, or PRAC.

My testimony today focuses on three key areas that must be addressed to better prevent, detect and respond to fraud and improper payments: 1) the collection, use, and sharing of data across and within agencies; 2) the lack of commitment from senior level executives to prevent and detect fraud and improper payments; and 3) technology gaps that hinder government from more effectively preventing and detecting fraud and improper payments.

Bottom line: I believe that a dedicated antifraud office with requisite authority is needed to devote the necessary attention to this enormous and growing problem.

Pandemic Spending and Increasingly Sophisticated Fraud Techniques Created the Perfect Storm for Fraud

Today, fraud actors have at their disposal massive amounts of personal information on nearly every American. Coupled with sophisticated tools, this makes committing fraud far easier than it's ever been. In this environment, the injection of nearly $5 trillion in relief spending—most of which were direct payments to citizens—created the perfect storm for fraud.

A combination of inadequate oversight and internal controls, large scale and organized fraud rings, and antiquated data and information systems contributed to the massive and widespread fraud we saw during the pandemic.

As of January 31, 2022, the federal government had obligated $4.2 trillion and expended $3.6 trillion, of the $4.6 trillion in funds from six COVID-19 relief laws. GAO recently reported that agencies had significant shortcomings in their application of fundamental internal controls and financial and fraud risk management practices in administering COVID-19 relief funds.

The program that suffered the largest fraud losses was the Pandemic Unemployment Assistance (PUA) program. The federal government cannot say for sure how much of the roughly $900 billion in pandemic-related unemployment relief has been stolen, but credible estimates range from $87 billion to $400 billion — *at least half of which went to foreign crime syndicates*, law enforcement officials say.[1] The most organized fraud actors are made

[1] https://www.nbcnews.com/news/us-news/easy-money-how-international-scam-artists-pulled-epic-theft-covid-n1276789

up of international organized crime rings, including actors from Russia, China, Nigeria and Ghana, as well as U.S. street gangs.

The investigative journalism site ProPublica calculated that from March to December 2020, the number of jobless claims added up to about two-thirds of the country's labor force, when the actual unemployment rate was 23 percent.

As the Department of Labor (DOL) Office of Inspector General (OIG) has reported, many states were not prepared to process the volume of new claims under completely new UI programs. As a result, many internal fraud controls that had been traditionally used or recommended for the processing of UI claims were not initially implemented by the states. This created a situation where fraudsters had a high-reward target— an individual could make a fraudulent claim with relatively low risk of being caught, at least initially.

One illustrative example: The California State Auditor reported in January 2021 that the state's Employment Development Department (EDD) was slow to take action to address rampant fraud. This resulted in payments of about $10.4 billion for claims that it has since determined to be fraudulent. Among its findings:

- The auditors identified 26,000 addresses that were associated with more than 555,000 claims – an average of 21 different claims per address for that batch of applications.
- The state paid $810 million in benefits in the names of 45,000 prison inmates because it had not developed the capacity to regularly match data from its claims system with data from state and local correctional facilities.
- California state law requires the EDD to review its anti-fraud policies to make sure they are effective, but the auditors found the agency did this once in 2015 and hasn't done it since then. The EDD also has no specific division responsible for stopping fraud.

While fraud perpetrated against PUA was the most egregious, many other programs also experienced unprecedented fraud. The PRAC reported in August 2021 that a key lesson learned was the need to certify or validate self-reported information prior to making a payment. The Small Business Administration (SBA) and the DOL both allowed applicants to self-certify that they were eligible for pandemic related financial relief. Not validating self-reported information has been a long-standing and widespread contributor to fraud and improper payments across virtually all benefits programs.

Better Use of Data, Senior Level Commitment and Enhanced Technology are Needed to Effectively Address Fraud and Improper Payments

Data Collection, Sharing, and Analysis Must all be Strengthened

Despite efforts across different agencies to collect, share and analyze data, most are struggling to effectively use data to identify and prevent fraud and improper payments. Reliability concerns hamper data collection through data reporting mechanisms like USAspending, as GAO has reported. Data sharing is significantly hampered by privacy limitations and many agencies lack the data analytics maturity and skillsets needed to conduct meaningful analyses.

Data matching (comparing two or more sets of data to look for matches that would indicate duplicates) is key to identifying ineligible beneficiaries, yet agencies are doing limited data matching, often because they don't have access to data to match against. Agencies cannot easily access Social Security death data, IRS data is totally off limits due to strict confidentiality laws, and other valuable data sets and information that could be used to verify the eligibility of an applicant is exceptionally challenging to access and share due to federal privacy laws.

Treasury's Do Not Pay (DNP) initiative was intended to provide up-front verification of applicant eligibility through data sharing and matching across federal programs and agencies. However, the system has significant weaknesses. In 2017, GAO reported the DNP working system offers full access to only three of six databases required by improper payments laws and only partial or no access to the remaining three.

GAO further reported that OMB had not formally evaluated user agencies' suggestions for additional databases or designated any additional databases to be included in the DNP working system. OMB staff acknowledged to GAO that some user agencies made suggestions for additional databases through their annual agency financial reports (AFRs) but stated the suggestions were not communicated through "formal requests."

Still more troubling, GAO reported while the law requires agencies to use DNP to review databases prior to award or payment, and while matching is conducted at the time of payment, agencies generally receive the results after payments have been made. GAO also found because the DNP functionality is part of Treasury's payment issuance process, payments made through other means—such as non-Treasury disbursing offices or contractors—are not automatically matched in DNP. Examples include Department of Defense payments disbursed through the Defense Finance and Accounting Service, and Medicare Fee-for-Service payments, both of which are programs with outlays in excess of $300 billion.[2]

A dedicated antifraud office could devote the needed time and resources to enhance data collection, address DNP weaknesses and provide guidance for establishing more robust data analytics capabilities. DNP could be significantly enriched with the addition of third party datasets that would allow more insight into beneficiaries. Further, agencies need help establishing analytics programs and the antifraud office would be well positioned to offer guidance and tools. In the age of the data breach, with so much personally identifiable information available to fraud actors, addressing the urgent need to access and share data to root out fraud and improper payments is paramount.

Agency Senior Leadership Must Demonstrate Commitment to Preventing and Detecting Fraud and Improper Payments

In general, agencies that operate benefits programs see their mission as primarily focused on distributing those benefits, but not as much attention is focused on ensuring those payments are directed only to the recipients who are eligible to receive them. When I was at GAO, agency officials directed us to OIG when we asked about fraud risk management. They simply did not see the prevention of fraud as their responsibility. It makes sense. Agency leaders have few if any real incentives to prioritize program integrity over delivery of

[2] https://www.gao.gov/assets/gao-17-15.pdf

benefits as agency leaders only get angry calls from citizens who did not receive a benefit. Similarly, congressional representatives only get calls from angry constituents when benefits are delayed or not received. No one calls to say fraud is a problem.

A more robust commitment and enhanced accountability from and for agencies' senior management is critical to efforts geared at preventing fraud and improper payments. Senior leaders need to prioritize mechanisms that support and promote program integrity. Government-wide initiatives to curb improper payments have turned into a "check the box" compliance exercise, given the current lack of management priority. And these efforts are all largely after the fact for many programs rather than being on equal footing with distributing benefits.

GAO issued its *Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework)* in 2015, which includes four key areas agencies should focus on in developing robust fraud risk management programs. The first area—Commit—directs agencies to establish a dedicated antifraud entity. However few, if any, agencies have established this entity. Just as the Fraud Risk Framework calls for top-level commitment within the agencies, a federal antifraud entity would demonstrate a governmentwide commitment to proactively managing risks to fraud and improper payments.

Government Must Overcome Technology Limitations that Hinder Agencies' Ability to Prevent and Detect Fraud

The government severely lags the private sector in the use of technology to identify and prevent fraud. During the pandemic, fraud actors saw an enormous opportunity to exploit this weakness. Many state unemployment programs were operating on legacy IT systems dating back to the 1970s. In 2020, the Labor IG reported states that do not have modernized unemployment systems may need alternative controls to compensate for the limitations imposed by outdated systems, including hiring additional staff.

State and federal agencies were and are vulnerable to fraud because they lack the tools necessary to detect fraud patterns. An example: Fraud actors have stolen millions by taking advantage of a Gmail feature in which Google ignores periods when interpreting Gmail addresses, known as the "dots don't matter" feature. If your email is johnsmith@gmail.com, all dotted versions of your address (i.e., john.smith@gmail.com, johnsmith.@gmail.com, etc.) are automatically delivered to your email account.

Fraud actors have exploited this feature by establishing Gmail accounts with long names and then applying for benefits with each iteration of that email address that includes a dot placed after each letter in the name. To the government system, this looks like many different email accounts—and different applicants—and they process each claim separately.

A cyber intelligence research firm identified 259 variations of a single email address used by the crime ring known as Scattered Canary[3] to create accounts on state and federal websites with the intent to carry out fraud.

Another fraud event exploited the website the IRS set up to process claims from people who aren't required to file tax returns. The website was vulnerable because existing tax data on these individuals did not exist, making it relatively easy for fraud actors to use stolen information and receive a benefit. Fraud actors filed at least 82 fraudulent benefit

[3] https://www.agari.com/cyber-intelligence-research/whitepapers/scattered-canary.pdf

applications using basic personally identifiable information that's regularly stolen in identity theft and available on dark web forums: an individual's name, address, date of birth, and social security number. One can buy this level of information for less a dollar on the dark web.

Government agencies must begin to catch up with the technology used by sophisticated fraud actors. The antifraud office can serve as the focal point for identifying emerging technology, establishing guidance and providing technical assistance to help agencies adopt new technology. For example, the office might help agencies adopt things like Identity Proofing tools, device fingerprinting, and intelligence tools that can monitor the deep and dark web activity for new fraud schemes.

It is important to note that when discussing antifraud technology, concerns about access and equity must be considered. Government must strive to prevent fraud and improper payments while ensuring legitimate beneficiaries are not hampered in accessing much-needed benefits. In this area, the government can look to the private sector which considers the reduction of so-called *friction* when implementing new antifraud technology. Today there are many automated, behind-the-scenes, data-driven tools that can authenticate a user and verify eligibility in near real time with little to no impact on the user. Government agencies need to consider user experience and balance antifraud tools with access whenever considering new technology.

A New Framework is Needed for Addressing Risks to Fraud and Improper Payments

The current approach to the prevention of fraud and improper payments is simply not working. There have been five iterations of legislation focused on improper payments over the last 20 years, while the improper payment rate and total improper payments have nonetheless steadily risen. Since fiscal year 2003, cumulative improper payment estimates have totaled about $2.2 trillion. For fiscal year 2021, improper payments were estimated to be about $281 billion, which represents a $75 billion increase from the prior fiscal year and approximately double the amount reported in fiscal year 2017. However, as GAO has noted, this estimate does not reflect all government-wide improper payments, as large as it is. Several agencies with large programs that have been identified as susceptible to significant improper payments are not reporting estimates, and some reported estimates are not comprehensive.

While there is a lot to do to fix agencies' ability to estimate and reduce improper payments, it is vital to take a more targeted, risk-based approach to fraud and improper payment prevention. As currently written, the Payment Integrity and Information Act (PIIA) creates burdensome compliance requirements on low-risk agencies and programs. The Congressional Research Service analyzed 2017 data and found that 85 to 98 percent of all improper payments were centered on the 20 programs identified as high priority following a 2009 Executive Order that established criteria for such programs. Yet all agencies with programs of at least $10 million are currently required to comply with improper payments risk assessment requirements, which they undertake with a check-the-box approach, wasting valuable time and resources that could be better spent on data- and outcome-oriented efforts.

Its time for Congress to pivot from the well-intentioned but marginally effective and burdensome improper payment framework created over the last twenty years and towards a more pragmatic approach that emphasizes data and outcomes.

Real progress in areas of fraud and improper payments can only be made by transitioning to a risk-based, data- and outcome-focused approach and establishing a more robust accountability system to compel leadership attention. Holding those agencies with high-risk programs accountable for implementing proactive, intelligence- and analytics-driven initiatives to prevent, detect, and respond to fraud threats and to demonstrate meaningful progress in measuring and reducing improper payments is vital. Further, rather than ineffectual across-the-board compliance activities, all agencies, regardless of risk level, must instead create outcome-focused data analytics initiatives aimed at proactively detecting patterns indicative of fraud.

These are complex problems and there are no easy solutions. Therefore, a dedicated antifraud office must be created to work solely on addressing the data, accountability, and technology challenges facing agencies at every level of government. The United Kingdom established such an office in 2018 and has seen enhanced focus on program integrity as a result. Among other things, such an office can work to:

- enhance and expand DNP, which is currently underutilized;
- help agencies negotiate data sharing agreements more expeditiously;
- provide technical assistance and oversight to ensure robust fraud risk assessments and the implementation of preventative controls aimed at fraud and improper payments are in place; and
- assist in the use of deep and dark web threat intelligence, and identity proofing tools to prevent identity theft-based fraud.

The erosion of citizen trust in government is warranted when leadership places so little priority on safeguarding the integrity of taxpayer dollars. It is time to rewrite the playbook for how to manage the risk of fraud and improper payments. The pandemic created a window into agencies' preparedness to prevent, detect and respond to fraud and improper payments. But fraud is not going away with the end of the pandemic; indeed these fraud actors are likely going to feel emboldened by their success and continue to target ill-prepared agencies. The time for action is now.

I look forward to any questions you may have.