Testimony of Linda Miller

Co-Founder and Chair, Program Integrity Alliance

Chairman Sessions, Ranking Member Mfume, Members of the Committee, I am grateful to have been invited to speak to you today about ways our government can better detect and deter fraud and improve the efficiency and effectiveness of government in the process.

For decades, politicians, officials, and the media have decried fraud, waste, and abuse in government programs, while Americans have questioned their leaders' ability to safeguard taxpayer dollars. The COVID-19 pandemic exposed just how unprepared our government was for fraud on a massive scale, alarming citizens and lawmakers alike. Yet, fraud isn't limited to crises; it permeates everyday government operations, quietly siphoning resources from programs meant to serve the public. The net result of this trend is a deterioration in trust in government.

My testimony outlines how the government can better prevent fraud and improper payments, ensuring taxpayer money truly serves the people. Two fundamental ideas underpin my testimony. The first is that any long-term solution requires an ambitious focus on strengthening fraud prevention, and in particular, *data-driven* fraud prevention. The second is that fraud is a whole-of-government problem requiring coordinated, whole-of-government solutions. My testimony will focus on three high impact actions the Congress can take: 1) invest in agencies' capacity to modernize their fraud prevention in the digital age 2) establish a centralized, whole-of-government approach to accelerate the use of data for fraud prevention; and 3) pass future-ready legislation that advances the use of data to prevent fraud.

We must invest in agencies' capacity to modernize their fraud prevention in the digital age

Investing in data-driven fraud prevention is investing in better program outcomes for the American people. As the President's FY 2025 Budget states, "There is compelling evidence that investments in administrative resources can significantly decrease the rate of improper payments and recoup many times their initial investment for certain programs." When describing the adjustments to base discretionary funding levels for four programs (Social Security, Unemployment Insurance, Medicare and Medicaid) to invest in antifraud activities, the budget analysis estimates net savings of $40 billion over ten years. For continuing disability reviews (CDR), the budget calculates this return on investment (ROI) at 9:1.

The benefits of investing in data-driven approaches extend beyond the direct financial impact of preventing improper payments and fraud. Increased data use can also significantly reduce administrative burdens on honest Americans who deserve efficient interactions with the government.

For many government agencies, taking data-driven approaches to mitigate risks of improper payments and fraud is in its infancy. To accelerate the modernization of program integrity and fraud prevention, additional resources are critical. Congress should establish a Program Integrity Fund (PIF), administered jointly by the Treasury and Office of

Management and Budget (OMB), that agencies can access to develop more sophisticated, data-driven fraud prevention tools. This fund should come with a requirement to report on measurable outcomes in terms of financial and nonfinancial benefits. Establishing the PIF as mandatory funding, as opposed to discretionary, would help to protect the funding and ensure appropriate use of funds.

To further evaluate "what works" and assess the ROI of data-driven fraud prevention, Congress could also establish pilot programs in select high-risk areas using a sandbox approach. Just as in software development, this approach would give agency leaders a "test environment," coupled with a mandate and resources, to experiment, iterate, and refine solutions.

For example, Congress could revise the limitation on the administrative expenses language proposed in the President's FY 2025 budget to allow funds provided under the first paragraph, $1,903,000,000, to remain available through March 31, 2026, for the costs associated with CDRs under titles II and XVI of the Social Security Act, to include the cost of all anti-fraud programs, projects, and activities of the Social Security Administration (SSA), not just the CDRs.

Congress could hold the SSA Commissioner accountable for demonstrating a return on that three-year investment in fraud prevention technologies and practices, with an obligation to report annually on savings and other impacts from the effort. Such pilots would provide critical insights into the implementation of data-driven preventive measures that are transferable across government, and they would advance governments' ability to measure and understand ROI in this context. And they would more than pay for themselves.

We need a centralized, whole-of-government approach to accelerate the use of data for fraud prevention

Investing in the capacity of agencies to modernize their fraud prevention is necessary but insufficient. Moving from rudimentary systems to a mature, data-driven approach that fully leverages technology requires significant resources and a coordinated, whole-of-government effort. In this context, there is an opportunity for the Congress to have a substantial impact through the creation of an independent agency or office with a sole mandate and budget dedicated to building the foundation for data use across government entities. This entity would centralize many of the data management and consolidation activities that agencies now tackle in siloes, creating duplicative efforts and draining taxpayer resources. The entity could also create methodologies and tools for programs to tailor further in their own contexts, thereby reducing lead times and start-up costs at the agency level.

The PRAC's Pandemic Analytics Center of Excellence (PACE) has been a bright spot precisely because of its focused mission to identify fraud in COVID-19 programs. Imagine the impact and efficiency gains if such an entity was empowered to support *all* government agencies to collect and make sense of data in service of fraud *prevention*. Treasury's Office of Payment Integrity (OPI) could serve as an excellent platform for housing this

independent initiative. It already manages the Do Not Pay (DNP) platform, as well as a host of data-driven tools to promote payment integrity. Staffed with fraud subject matter experts and data scientists and armed with a mandate to find and prevent fraud across government programs, this office could drive meaningful progress in the decades-long fight against fraud.

And collaboration between the inspector general community and the management side of government must be strengthened. Establishing a truly whole of government approach to fraud prevention requires leveraging the data and knowledge the inspectors general possess to assist agencies in preventing fraud from occurring in the first place. If Treasury's OPI were expanded to serve as the unifying office for government fraud prevention, close collaboration with the PRAC/PACE, GAO and the inspectors general to include sharing data and leads, would be a force multiplier without impacting agency independence.

We need future-ready legislation to advance fraud prevention

Creating future-ready legislation for fraud prevention requires mandating the use of existing data and expanding access to new data sources. The Fraud Prevention and Recovery Act—introduced in the Senate earlier this year—is commendable for the steps it takes in this direction. As one example, the bill includes provisions to enhance agencies' use of the DNP platform within Treasury's newly formed OPI, including requirements that agencies leverage data to verify and compare bank account information before certifying vouchers for disbursements.

These requirements alone could prevent, detect, or recover an estimated $37.8 billion in improper payments over 10 years. Notably, by comparing bank accounts during voucher precertification, the government could save an additional $152 million just by eliminating the need to print 200 million checks. Similar savings across other programs would further amplify these benefits. Incentives for agencies to make use of data already available have the potential for a high return on investment for taxpayers.

To ensure readiness for the next emergency, Congress should pursue legislation directing Treasury, agencies, and the PRAC to develop and/or enhance existing guidance, policy, technology platforms, methods, and data systems to address domestic and international fraud and improper payments, including adhering to the guidance set forth in the GAO Fraud Risk Management Framework. Such legislation should make using the DNP system mandatory for all emergency funding programs.

And legislation that addresses critical data sharing and access issues would tackle a persistent problem with improper payment reporting, which has become largely a check-the-box exercise. In FY 2023, over 66 percent of improper payments reported on paymentaccuracy.gov were due to a common issue: "Failure to access data/information needed to validate payment accuracy prior to making payment." Yet agencies are not seriously reckoning with this problem; they just continue to report it, quarter after quarter. This reporting distracts from an agency's core mission, adds to administrative burdens for

civil servants, and offers questionable value in reducing improper payments. It adds waste upon waste.

Treasury, as the central disbursing agency, can support federal programs in detecting new and emerging fraud schemes. Expanding Treasury's statutory authority to access data necessary for the purposes of detecting and preventing fraud and improper payments is critical to enable timely fraud detection and prevention. These expanded authorities should include the following key data sources for purposes of identifying and preventing improper payments:

- permanent access to the Full Death Master File;
- expanded access to the National Directory of New Hires; and
- expanded access (by amending the Fair Credit Reporting Act) to consumer credit data.

Further, amending the Privacy Act to exempt agencies from computer matching agreement requirements for purposes of payment integrity and preventing fraud and improper payments would remove the enormous administrative burden that limits agencies' ability to access data for fraud prevention.

Conclusion

Fraud and improper payments are a whole-of-government problem that require coordinated, whole-of-government solutions, especially to overcome systemic barriers to data sharing for fraud prevention. To build a stronger foundation for fraud prevention, Congress should invest in agencies' capacity to modernize their approaches, establish a Program Integrity Fund, and support pilot programs that test data-driven solutions in high-risk areas. Future-ready legislation is also essential to expand data use and access, ensuring more effective fraud detection and prevention across all programs. Finally, creating a centralized entity, such as an expanded Office of Payment Integrity, dedicated solely to leveraging data for fraud prevention, would enhance coordination and reduce duplication of efforts. By implementing these measures, we can achieve systemic improvements that amplify agency-level actions, and create a government that is truly trustworthy and accountable to the American people. And save billions and billions of taxpayer dollars in the process.