<div align="center">

Statement of Renata Miskell
United States Department of the Treasury
Before the Oversight and Government Reform
Subcommittee on Government Operations
United States House of Representatives
January 13, 2026

</div>

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, thank you for the opportunity to discuss how the Department of the Treasury (Treasury) is using innovative tools to detect and prevent fraud and improper payments across the federal government.

Treasury is firmly committed to advancing data-driven strategies that strengthen payment integrity, safeguard taxpayer dollars, and reduce fraud, waste, and abuse government-wide. Each year, Treasury, on behalf of federal agencies, disburses trillions of dollars in payments. Ensuring those payments go to the right people, in the right amounts, and at the right time is both a fiscal responsibility and a matter of public trust.

Federal agencies have had difficulty sufficiently safeguarding taxpayer dollars against fraud and improper payments due to government-wide technology challenges and longstanding issues with accessing data to verify eligibility and authenticity of payment recipients. Through modernized stewardship, Treasury can assist federal agencies and states administering federal funds to better detect and prevent fraud and improper payments – moving away from a reactive "pay and chase" model to a proactive prevention model. At the core of this effort is the principle that access to high-quality, interoperable data – used responsibly and securely – allows agencies to detect and prevent improper payments as early as possible, before funds ever leave Treasury.

Do Not Pay

Under the leadership of Secretary Bessent and OMB Director Vought, Treasury is modernizing stewardship by expanding agencies' use and enhancing the utility of Do Not Pay. Do Not Pay, which is authorized and governed by the Payment Integrity Information Act of 2019 (PIIA), is a government-wide tool provided by Treasury for federal agencies and states operating federally funded programs that provides data to prevent the leading causes of improper payments, including data on deceased individuals, ineligible entities, and invalid bank accounts. It is a one-stop shop designed to help federal programs prevent improper payments before they are made.

Do Not Pay has been underutilized by agencies due to complex legal and administrative barriers and lack of agency engagement. In fiscal year 2024, only four percent of federal programs completed the legal requirements to access all the databases in Do Not Pay.

In addition, Do Not Pay has not had sufficient databases to detect the leading root causes of improper payments. Adding new data sources to Do Not Pay follows a legal process called

"designation," which requires OMB approval. Historically, this process could take a year or more to complete due to limited standardization and the complexity of navigating differing agency legal interpretations and requirements. What previously took a year we are now able to accomplish within a few months. In addition, Treasury has requested additional statutory authority to access federal databases that would be highly effective in reducing financial fraud and improper payments – namely databases that enable federal programs to better verify identity, financial status, and death. Despite often widespread support in Congress for proposals designed to address these challenges, legislation has been slow to advance.

To address these challenges, especially following the significant losses related to fraudulent payments in COVID-19, Treasury created a cross-functional "Tiger Team" to study why fraud and improper payments persist, and to prototype innovative solutions that accelerate the detection and prevention of financial fraud. The team worked with federal, state, and industry stakeholders to strengthen and expand data-sharing partnerships, identify and adopt best practices and tools, and embrace emerging technologies like machine learning and artificial intelligence (AI). As a result, Treasury identified and tested 19 new data sets that could potentially prevent approximately $28 billion in improper payments.

To combat rising check fraud, Treasury tested and implemented AI techniques like machine learning algorithms to mitigate check fraud in near real-time – strengthening and expediting processes to recover potentially fraudulent payments from financial institutions. As a result, Treasury prevented and recovered over $1.9 billion in check fraud in fiscal years 2024 and 2025 combined.

In March 2025, Treasury collaborated with the White House on the development of Executive Order 14249, "Protecting America's Bank Account Against Fraud, Waste, and Abuse," which embedded many of the lessons learned for stopping fraud and improper payments. Since then, Treasury and OMB have made substantial progress in reversing the underutilization of Do Not Pay at a scale and pace not previously possible.

First, Treasury and OMB have worked aggressively to remove administrative barriers that slowed the agency sign-up process for Do Not Pay. OMB issued guidance[1] outlining the new streamlined process, while protecting privacy. Collectively, these actions reduced administrative friction and are on track to expand the full use of Do Not Pay by all large agencies and all federal programs by the end of fiscal year 2026. Building on this progress, Treasury and OMB are improving the effectiveness of Do Not Pay by designating new high-value databases through a streamlined process. In parallel, Treasury is developing enhanced capabilities to help agencies better interpret and take action on screening results through improved risk-based indicators.

---

[1] Office of Management and Budget, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, Memorandum M-25-32 (Washington, DC: Executive Office of the President, August 20, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/08/M-25-32-Preventing-Improper-Payments-and-Protecting-Privacy-Through-Do-Not-Pay.pdf

Finally, Treasury's Do Not Pay system now supports the back-end data and technology for the Department of Health and Human Services' (HHS) Administration for Children and Families Public Assistance Reporting Information System (PARIS), which is used to detect duplicate public benefits in multiple states. In fiscal year 2025, PARIS identified approximately $1.3 billion in improper payments through interstate duplicate beneficiary matching. In November 2025, PARIS expanded beyond duplicate detection to include death matching for 19 states using Do Not Pay data, with an estimated $156 million in additional improper payments expected to be prevented. Treasury is working with PARIS to expand death data access to all states in 2026.

Payment Verification

In addition to expanding and enhancing Do Not Pay, pursuant to Executive Order 14249, Treasury is implementing additional payment verification screening to further safeguard against fraud and improper payments in federal spending by identifying anomalies in individual payment files prior to agency certification. To improve accuracy, Treasury has implemented new validations to confirm that payment vouchers include valid accounting codes (i.e., Business Event Type Code and Treasury Account Symbol) and that sufficient funds are available in the account at the time of payment. In addition, to safeguard against fraud and improper payments, Treasury is in the process of deploying screening to detect payments to deceased individuals, to confirm that the bank account provided is open and belongs to the intended payee, and that a proper and valid identifier (i.e., Social Security number or Taxpayer Identification Number (TIN)) is provided for each payee. By the end of January 2026, Treasury will screen all remaining Treasury-disbursed payments for deceased payees and will continue to implement additional payment verification checks going forward.

Challenges

Treasury is modernizing stewardship by transforming Do Not Pay from an underutilized compliance tool into a sophisticated internal control and implementing payment verification screening on all federal disbursements made by Treasury prior to agency certification.

However, additional statutory authority would help Treasury fully achieve the objectives of PIIA and Executive Order 14249. There are several federal data sources that Treasury has had difficulty accessing that would dramatically improve identity attribute checks, eligibility determination, and fraud prevention.

Treasury has made a targeted set of legislative proposals to address the major root causes of improper payments. Verification of death data is critical, and Treasury's continued access to the complete Death Master File is essential. The Consolidated Appropriations Act of 2021 required Treasury to conduct a three-year pilot, which is currently set to expire at the end of 2026. Treasury's initial 12-month pilot demonstrated significant impact, projecting an estimated $330 million in net benefits (2024–2026). Permanent access through new, explicit statutory authority could reduce improper payments by billions of dollars, and I'm happy to report that yesterday

evening, the House passed legislation by voice vote that would do just that. S. 269, the Ending Improper Payments to Deceased People Act passed the Senate in a similar fashion last year and now goes to the President for his signature. The three-year pilot that Congress authorized is a successful model that should be repeated for other data sources.

Notably, to safeguard against identity theft and to fully implement Executive Order 14249 requirements to screen payments for valid TINs, Treasury proposes additional statutory authority for Do Not Pay to access the IRS's Employer Identification Number data and the Social Security Administration's Social Security number validation service (Numident) for all programs. Additionally, Treasury proposes additional authority for Do Not Pay to access select tax information for payment verification in a privacy-preserving manner, under Internal Revenue Code section 6103 protections, and is limited to responding to specific queries, such as providing a "yes" or "no" response to general questions like: "Is the TIN valid and associated with the payee?" "Was the individual reported to be a victim of identity theft?" and "Was the individual's adjusted gross income less than or equal to $Y in year Z?" Treasury is committed to collaborating with SSA, IRS, and the White House to put forward legislative language around proposals.

In addition, Treasury is continuing to seek legislative authority to eliminate obstacles to access other important data sources, including the National Directory of New Hires data and certain information covered by the Fair Credit Reporting Act[2]. Treasury's analysis shows that these data sources could help agencies prevent tens of billions of dollars in improper payments and fraud while rigorously protecting Americans' privacy.

Importantly, all access to and use of Do Not Pay data is governed by strict privacy, security, and user access controls. All users are trained on the appropriate use of Do Not Pay data, and Treasury diligently monitors the actions of every user accessing Do Not Pay systems. Treasury is unwavering in its commitment to protecting the sensitive data on Americans and works closely with agencies to help ensure compliance with all legal and cybersecurity requirements.

In closing, Treasury's experience is clear: when agencies have timely access to authoritative data and use it before payments are made, fraud and improper payments decline. With continued partnership from Congress, Treasury can further modernize payment integrity, protect the American taxpayer, and ensure that federal programs deliver benefits efficiently and lawfully.

Thank you for the opportunity to testify. I look forward to your questions.

---

[2] This proposal is limited to allowing Do Not Pay to partner with data aggregators such as credit reporting agencies to validate payee attributes against credit header data, not credit score or trade histories.