Program Integrity Alliance

For the Record
United States House Committee on Oversight and Government Reform
Subcommittee on Government Operations
Hearing: *Curbing Federal Fraud: Examining Innovative Tools to Detect and Prevent Fraud in Federal Programs*
January 13, 2026

Chairman, Ranking Member, and Members of the Subcommittee:

Thank you for the opportunity to submit this statement for the record in connection with the Subcommittee's hearing on innovative tools to detect and prevent fraud in federal programs.

I am the President and Co-Founder of the Program Integrity Alliance, an independent 501(c)(3) nonprofit, nonpartisan organization focused exclusively on strengthening government integrity through data, evidence, and public-sector innovation. I served as Deputy Executive Director of the Pandemic Response Accountability Committee (PRAC). Before that, I spent a decade at the Government Accountability Office (GAO), where I led the development of GAO's *Framework for Managing Fraud Risks in Federal Programs*.

The central message that I hope the subcommittee will takeaway is that the federal government can and should do far more to prevent fraud before payments go out. While advanced fraud detection methods are available, government agencies do not consistently adopt or embed them into payment operations. In most cases, agencies lack clear statutory authority to act quickly in response to high-confidence fraud indicators, including to stop payments. This is often out of concern for due process protections, which, in Minnesota, meant protecting the fraudsters, to the understandable shock of many Americans.

I draw on lessons from the Minnesota fraud scandal as well as broader limitations the federal government faces to prevent and detect fraud. My suggested reforms are framed through the lens of the GAO Fraud Risk Framework, which provides the federal government's foundational model for committing to fraud risk management, assessing risk, designing and implementing controls, and evaluating and adapting over time.

Background

Minnesota's fraud story is predominantly about what happens after fraud is found. Public reporting and oversight reviews of the Minnesota fraud cases show that fraud risk was identified early and repeatedly. Program administrators flagged implausible growth, anomalous billing volumes, and documentation patterns inconsistent with real-world

service delivery. These warnings were documented, escalated, and, in some cases, acted upon through attempted corrective measures and referrals.

The slow-motion trainwreck that followed was not a failure of fraud analytics or awareness; it was rather a collision with an oversight architecture built for documentation-based trust, emergency speed, and fragmented authority. When agencies attempted to intervene, they quickly faced due process litigation from fraudsters. Courts compelled continued payment because existing statutes provided procedural standards for payment but no fraud-risk standard for non-payment. Funds continued to flow even as the obvious risks were well understood. Minnesota therefore illustrates a broader federal challenge: modern fraud operates at network speed, while oversight authority and payment controls remain rooted in legacy designs.

> Oversight bodies have repeatedly shown that government programs continue to rely heavily on post-payment detection, fragmented data, and documentation-based controls that are poorly matched to modern, networked fraud, including organized crime groups.

Beyond Minnesota, fraud prevention across the federal government reveals the same structural vulnerabilities at scale. GAO has estimated that the federal government loses up to $521 billion to fraud annually, much of it undetected or identified only after funds have been disbursed. Major enforcement actions further demonstrate that sophisticated fraud networks are exploiting systemic weaknesses in identity verification, provider enrollment, and pre-payment controls across programs. As an example, Operation Gold Rush uncovered a multibillion-dollar, transnational Medicare fraud scheme involving durable medical equipment claims and hundreds of providers. In many cases, these schemes persisted for years, not because warning signs were absent, but because detection tools were not consistently deployed at scale and, even when risk was identified, investigators and prosecutors lacked the authority or integration to interrupt payments quickly.

Minnesota should therefore be understood not as an anomaly, but as a concentrated case study of broader federal challenges in translating fraud awareness into real-time prevention.

Problem Statement Through the GAO Fraud Risk Framework Lens

The GAO Fraud Risk Framework emphasizes that effective fraud risk management requires not only identifying and assessing risk but also designing and implementing controls that allow timely response. Minnesota demonstrated a systemic weakness in this latter phase. Agencies and oversight bodies increasingly succeed at surfacing fraud risk through data

integration, anomaly detection, and network analysis. Yet those insights often cannot be translated into action because agencies lack clear authority to pause, segment, or condition payments without triggering legal challenges that focus narrowly on procedural compliance.

As a result, data-driven tools function as retrospective diagnostics rather than proactive, operational controls. This disconnect undermines the framework's design-and-implement and evaluate-and-adapt components and leaves the federal government structurally unable to prevent losses, even when fraud risk is known.

Reforms Needed to Operationalize Detection into Prevention

To align federal programs with the GAO Fraud Risk Framework and the purpose of this hearing, Congress should pass a comprehensive package of reforms that allow innovative detection tools to drive lawful, real-time prevention.

1. **Agencies administering federal funds should have explicit, court-defensible authority to temporarily pause or segment payments when documented fraud risk is present.** This authority should be risk-based, time-limited, and subject to expedited review, but it must exist if detection is to lead to prevention.

2. **Courts evaluating injunctions or payment disputes should be required or allowed to consider the reasonableness of an agency's fraud-risk determination, not solely whether every procedural step was followed.** Courts currently lack a statutory fraud-risk standard, and without one they are forced to privilege process over substance.

3. **Federal payment systems should be required to separate routine payments from unusually large or high-risk claims and temporarily hold the latter pending review.** Payment segmentation and escrow mechanisms can constrain fraud growth and reduce the legal leverage that arises when agencies are forced into all-or-nothing payment decisions.

4. **Continuity of service delivery to beneficiaries must be legally, explicitly separated from provider entitlement to payment.** Protecting access to services does not require guaranteeing immediate payment to a specific provider under investigation. Programs should be designed with contingency mechanisms that protect beneficiaries while allowing provider-level controls when risk is elevated.

5. **Real-time data-driven payment monitoring techniques—including anomaly detection, volume plausibility checks, and network analysis—should be mandated as operational controls rather than treated as advisory tools.** When these systems identify elevated risk, statutes should require defined administrative responses.

6. **Congress should authorize limited, privacy-protective cross-program data sharing so that fraud networks operating across multiple programs can be identified and addressed.** Modern fraud exploits program silos; oversight systems must be permitted to see horizontally.

7. **Early warning triggers, such as formal Inspector General case acceptance or substantiated material misrepresentation, should carry automatic administrative consequences**. Risk identification without consequence, including enhanced review or temporary payment controls, does not satisfy the framework's response requirement.

8. **Agencies and officials acting in good faith on documented fraud risk should receive safe-harbor and indemnification protections.** The framework assumes an institutional environment that supports action on risk rather than penalizing it. Likewise, program officials should have, as part of their performance expectations and job requirements, a specific requirement relating to preventing and reducing fraud and improper payments along with specific quantitative goals.

A Tiered Due-Process Framework at the Point of Payment

To address a significant weakness in fraud prevention at the federal level, Congress should provide the Treasury Department the authority to use the data analytics tools it has acquired to expeditiously stop high-risk payments. Although the commonly mentioned federal Do Not Pay (DNP) Initiative may seem to fit the bill, it is fundamentally an information-sharing and analytics platform rather than enforcement authority. It enables agencies to review eligibility before making payments, but it does not confer any independent power on the Department of the Treasury to deny, cancel, or withhold payments based on DNP matches.

Treasury's role remains limited to hosting and operating the DNP system, while responsibility for verifying matches and making eligibility decisions rests entirely with the program agencies themselves. As a result, even high-confidence fraud indicators

surfaced by Treasury's systems cannot, under current law, prevent a payment from being disbursed unless the agency acts.

Congress should modernize the federal payment process by establishing a *tiered due-process framework* that allows Treasury to act on objective fraud indicators at disbursement while preserving agencies' responsibility for eligibility determinations and full notice and appeal rights.

At the first tier, Treasury should be prohibited from disbursing payments when a statutorily defined prohibited payee condition is present. These conditions would be limited to objective, high-confidence indicators already recognized across federal programs, such as verified death where post-death payment is not authorized, inclusion on sanctions, debarment, or exclusion lists that bar federal payment, or use of a financial account previously designated as compromised in connection with confirmed fraud or identity theft. **In these circumstances, payment is legally improper regardless of program discretion. Treasury would cancel the payment and notify the certifying agency, which would remain responsible for any underlying eligibility determination and post-deprivation notice.**

At the second tier, when a payment triggers a high-confidence fraud flag based on data sources designated under the Do Not Pay Initiative, Treasury should be authorized to impose a short-term pre-disbursement hold measured in days. During this brief hold, Treasury would notify the certifying agency immediately, the agency would verify the data to the extent practicable, and the payee would be promptly notified and given a fast, accessible opportunity to contest the information. If the agency does not confirm ineligibility before the hold expires, the payment would be released automatically. This tier allows analytics to function as real-time controls while preserving due process.

At the third tier, Congress should permit program agencies, with concurrence from OMB and Treasury, to designate specific data matches as determinative of payment ineligibility for defined programs. In these cases, payment certification would be conditioned by law on the absence of the determinative flag. If Treasury detects the flag at disbursement, the payment would be cancelled automatically, after which the agency would follow existing statutory procedures to provide notice, an opportunity to contest, and any appeal rights.

This tiered approach aligns the strength of the response with the confidence of the risk signal and embeds proportional, data-driven action directly into the payment lifecycle.

Conclusion

Today's hearing rightly focuses on innovative tools to detect and prevent fraud. The Minnesota experience demonstrates that detection alone is insufficient. Without statutory

authority, judicial standards, modern payment architecture, and due-process frameworks that allow agencies to act on analytic insights, even the most advanced tools will arrive too late.

Operationalizing the GAO Fraud Risk Framework requires aligning law, oversight authority, payment systems, and due-process protections with the government's analytical capabilities. Doing so would convert early warning into early prevention and ensure that innovation in fraud detection produces durable, lawful results.

Respectfully submitted,

Linda Miller
President, Program Integrity Alliance