Subcommittee on Oversight of
the House of Representatives Committee on Ways and Means

Hearing: Investigating Pandemic Fraud – Preventing History from Repeating Itself

Testimony of Linda Miller

October 19, 2023

Subcommittee Chairman Schweikert, Ranking Member Pascrell, and esteemed members of the Subcommittee, I am pleased to be here today to share my perspectives on enhancing the government's efforts to prevent, detect, and respond to fraud. I am the Founder and CEO of a boutique consultancy specializing in fraud risk management. I also bring to bear my former experience both as the Deputy Executive Director of the Pandemic Response Accountability Committee, or PRAC, and as an Assistant Director in the Forensic Audits and Investigative Service group at the Government Accountability Office (GAO).

The nearly $5 trillion in government relief spending during the COVID-19 pandemic — much of which was disbursed as direct payments to citizens — created the perfect storm for fraud. A combination of inadequate oversight and internal controls, large-scale organized fraud rings, and antiquated data and information systems contributed to the massive, widespread fraud we saw during the pandemic. Agencies were unprepared for the fraud they encountered largely due to a lack of attention on fraud risks. GAO issued its Framework for Managing Fraud Risks in Federal Programs in 2015, but regrettably little attention was paid to establishing the preventative controls GAO called for to manage fraud risks.

Today, fraud actors have at their disposal massive amounts of personal information on nearly every American. Coupled with sophisticated technological tools, this makes committing fraud far easier than it's ever been. Congress has the opportunity to demonstrate a commitment to preventing fraud in the future, following the devastating fraud losses experienced during the pandemic.

My testimony today focuses on five key actions Congress can take to help ensure history doesn't repeat itself: 1) Create a dedicated antifraud office; 2) explore ways to enhance data-driven fraud prevention; 3) revise improper payment laws to focus on high-risk programs; 4) incentivize fraud prevention; and 5) earmark fraud prevention funding in large spending bills.

Create a Dedicated Antifraud Office with Senior Level Authority

Senior levels of government have long neglected the prevention of fraud and improper payments. To change that, focused senior level attention is needed. Agencies struggle with competency in fraud and data analytics, they struggle with data sharing, and they struggle with a lack of incentives to allocate resources to these activities.

An all-of-government strategy should be established and implemented by a well-funded, centralized office with the authority to effect real change. A dedicated antifraud office would have the necessary skills and focus to work solely on addressing the data, accountability, and technology challenges facing agencies at every level of government.

A dedicated federal antifraud office would serve as the focal point for identifying emerging technology, establishing guidance, and providing technical assistance to help agencies adopt new data analytics technology and techniques. The United Kingdom established such an office in 2018 and has seen enhanced focus on program integrity as a result.

As part of this office, Congress should direct the creation of a fraud analytics center of excellence. Modeled on the PRAC's Pandemic Analytics Center of Excellence, which can only be used by oversight entities to address fraud that has already occurred, a similar analytics center of excellence on the management side of government would allow for a data-driven emphasis on fraud *prevention*, where fraud risk management is most efficient and effective.

Today, agencies spend valuable time and money building redundant analytics systems and buying commercial tools duplicatively, wasting taxpayer dollars. Centralizing this effort would save taxpayer money by creating an economy of scale.

Treasury has made progress enhancing its Do Not Pay system along with its Payment Integrity Center of Excellence. With additional funding and a mandate to create a centralized, data analytics capability, this system could establish an unprecedented government-wide data analytics platform to identify and prevent potential fraud and improper payments across government programs.

Explore Ways to Enhance Data-Driven Fraud Prevention

Conventional wisdom holds that you can promote citizen access to government services or you can prevent fraud, but you can't do both. This tradeoff doesn't exist in the private sector, and it shouldn't in government. Banks effectively balance the competing business imperatives of attracting and retaining customers and preventing fraud every day. Both are vitally important to their bottom line. But in government, we often only focus on attracting and retaining customers, erroneously thinking that if we focus on preventing fraud, we will impede citizen access to needed services.

The government 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. State and federal agencies were and are vulnerable to fraud because they lack the tools necessary to detect fraud patterns. One example: a cyber intelligence research firm identified 259 variations of a single email address used by a crime ring to create accounts on state and federal websites with the intent to carry out fraud. Government agencies must begin to catch up with the technology used by sophisticated fraud actors.

Part of the challenge lies in outdated laws, including the Fair Credit Reporting Act (FCRA) and the Privacy Act. These laws severely limit agencies' ability to use data to prevent fraud, especially given the rise of data breaches and the epidemic of identity-theft based fraud perpetrated by sophisticated organized criminal groups. Rapid technological developments, digitalization and datafication of society and the economy require innovative regulatory approaches, in addition to traditional laws, regulations and regulatory policies. The tension between privacy protection and fraud prevention creates an untenable paralysis within government that fraudsters happily exploit.

Innovative approaches to assisting agencies use data include:

- **Statutory code of practice for sharing private information.** Data sharing is an enormous challenge in the government, and for many agencies, the perceived risks of getting it wrong— reputational damage or enforcement action by the regulator— outweigh the benefits that can be gained from data sharing, leading to missed opportunities for innovation and improved fraud prevention. A code of practice, like one created in the U.K., can help provide a common understanding of best practice in data sharing.
- **Regulatory sandbox**[1]. A regulatory sandbox would allow the private sector to partner with agencies on data-driven fraud-prevention approaches with a

[1] A regulatory sandbox is a set of rules and appropriate safeguards, usually summarized in writing and published, that allows for live, time-bound testing of innovations under a regulator's oversight. A sandbox creates a conducive and contained space for experimenting with innovations at the edge or even outside of an existing regulatory framework.

degree of assurance that the experimental and testing phases are unlikely to run afoul of statutory or regulatory requirements.

- **Public-private partnership with financial institutions**. Partnering with financial institutions, who have more mature fraud prevention tools, agencies can learn how to balance the need to ensure timely access to government services with effective fraud prevention. The Senate Appropriations Committee's FY24 Financial Services and General Government bill report contains language directing the Treasury Department to lead a multisectoral whole-of-society effort to counter the increasing threats associated with financial fraud. This public-private partnership will encourage information sharing between government and private sector participants, develop best practices for relevant stakeholders, and encourage innovations in counter-fraud technologies, data-analytics, and approaches. I encourage the Subcommittee to engage with its Senate counterparts to help enact this provision.

Piloting the implementation of some of the more innovative data-driven tools in use in the financial sector, within the context of a regulatory sandbox, would yield meaningful progress. Congress can also use the results of these efforts to reform the laws that impede data-driven fraud prevention, proving that you can prevent fraud while protecting privacy and maintaining timely access to government services.

Revise Improper Payment and Fraud Prevention Laws to Focus on High-Risk Programs

The current approach to preventing fraud and improper payments in the federal government is costly, inefficient, and ineffective. As currently written, the Payment Integrity and Information Act (PIIA) creates burdensome compliance requirements on low-risk agencies and programs but does little to reduce improper payments made by larger, higher risk programs.

Government cannot afford to waste limited resources on low-risk activities. The Congressional Research Service analyzed 2017 data and found that 85 to 98 percent of all improper payments were made by 20 programs identified as high priority following Executive Order 13520, which established criteria for such programs.

Yet today, all agencies with programs of at least $10 million are currently required to undertake burdensome compliance activities, which they do with a check-the-box approach, wasting valuable time and resources that could be better spent on data- and outcome-oriented efforts.

Real progress in areas of fraud and improper payments can only be made by transitioning to a risk-based, data- and outcome-focused approach. Those agencies with programs susceptible to fraud and improper payments should be required to implement proactive, intelligence- and analytics-driven initiatives to prevent, detect, and respond to fraud threats and demonstrate meaningful progress in measuring and reducing improper payments.

Amending PIIA to eliminate burdensome requirements on low-risk programs, setting a threshold (e.g., $50 billion or more in outlays) and requiring those programs above that threshold to implement advanced analytics programs for fraud prevention and detection will help focus attention on the areas of highest risk, thereby enhancing both effectiveness and efficiency.

Incentivize Fraud Prevention

Try to imagine a scenario where the CEO of a private sector company could save millions of dollars by obtaining the needed data to verify the accuracy of customer-provided information, but simply does not do so. It's hard to fathom shareholders would accept that. So why is this the case in government?

Because as citizens, we are both the government's customers and its shareholders. And we hold government accountable for little other than quickly providing us the benefits we are entitled to or eligible for. When citizens complain about wait times or complex application processes, agency leaders listen. In recent years, government agencies have prioritized “customer experience.” In fact, an entire industry focused on customer experience (it even has an acronym, CX) is at work across government, making things easier for customers to navigate.

This problem must be addressed at the root—agency leaders need more institutional incentives to manage fraud, waste, and abuse in their programs more systematically. They must be held accountable for using data and tools to prevent fraud, waste, and abuse before it happens.

That accountability should start with benchmarking what proactive fraud prevention programs agencies should have in place. Currently agencies employ a wide range of tools and activities in service to fraud prevention. Some of the larger programs have some of the less-mature fraud risk programs and vice versa. A centralized office could dedicate the time and expertise to establishing benchmarks and providing technical assistance to agencies to put the needed tools in place.

Congress can also incentivize agency leaders by holding regular hearings with agency leaders to discuss their actions to prevent fraud. A word of caution on incentives: The hidden nature of fraud makes it easy to ignore. If agencies are only measured on the “amount of fraud” they have, the unintended outcome will be that agency leaders will simply look the other way, underreporting their fraud by establishing meaningless definitions and giving the false impression that fraud is well controlled. *Incentives in fraud prevention should be focused on the actions agencies are taking and the rigor with which they are measuring the effectiveness of those actions.*

Building fraud prevention into agency leaders’ performance metrics and those of their managers, measuring their activities against an established benchmark, scheduling regular “fraud hearings” and requiring agency leaders to share how they are working to prevent and detect fraud could all help incentivize fraud prevention.

Earmark Fraud Prevention Funds in Large Spending Bills

Preventing fraud and improper payments is a data game. Large spending bills like the Bipartisan Infrastructure Law and the Inflation Reduction Act contained enormous grant and loan programs but provided no funding or requirements for safeguarding the integrity of those funds. Like many pandemic programs, fraud actors will target those programs with coordinated fraud schemes. Data and analytics can be a game changer, for example:

- The acceleration of machine learning and artificial intelligence tools offers government agencies the ability to identify fraud schemes quickly.
- Natural language processing text analytics engines can identify duplicate passages in grant applications in seconds.
- Massive amounts of third-party data can be mined and leveraged to identify past criminal activity and other suspicious indicators related to applicants.
- Third-party data analysis can also identify patterns indicative of stolen or synthetic identities used in grant, loan, and benefit applications.
- Social network analytics can identify the relationships between applicants that could indicate the existence of a fraud ring.
- Device metadata, such as geolocation, can also be mined to identify potential fraud indicators. And all this data analysis can be done in seconds with the tools available today.

To protect taxpayer resources, government agencies must invest in the tools needed to fight fraud. Establishing dedicated funding for fraud prevention to accompany large spending bills and directing agencies to establish metrics for preventing fraud actors from stealing the funds provided in any large new spending bill will provide the needed focus on fraud prevention.

These observations and recommendations are the result of my decades of work supporting fraud risk activities in the federal government. There were simple steps that could have been taken to minimize the extent of fraud we saw in many of the pandemic response programs. Hopefully, we can take the lessons learned from that experience to ensure we don’t suffer that extent of fraud in the future.