Questions for the Record
March 31, 2022, Hearing: "Follow the Money: Tackling Improper Payments"
Ms. Linda Miller
Principal, Grant Thornton, LLP

The following questions were all provided by Chairman Gerald E. Connolly, Subcommittee on Government Operations

1. Even if agencies are taking their mandate to address improper payments and enhance program integrity seriously, current law may still force them to prioritize compliance over outcomes. How can we evolve the law to move from a compliance-focused to an outcomes-based approach?

2. In your testimony, you described Treasury's Do Not Pay system as "broken." Can you elaborate on ways the system can be enhanced? Are there things Congress can do to strengthen Do Not Pay?

3. Data sharing could serve as a key tool to reduce improper payments. What obstacles impede agencies' ability to share and use data effectively, and what can Congress do to mitigate those obstacles?

4. Sometimes, the data the government needs lies in the hands of the private sector. How can private-sector data support the government's efforts to mitigate improper payments in a safe, secure way? Additionally, what private sector practices or innovative information technology applications can government adapt or borrow to improve service delivery and program integrity?

Question 1: Even if agencies are taking their mandate to address improper payments and enhance program integrity seriously, current law may still force them to prioritize compliance over outcomes. How can we evolve the law to move from a compliance-focused to an outcomes-based approach?

An outcomes-based approach would require agencies to be accountable for a reduction in improper payments and fraud. Current laws focus on estimation of improper payments, not a reduction of them. And even those programs considered "high priority" by the Office of Management and Budget (OMB) — and are thus required to report on the root causes quarterly—document the same root causes every quarter and most see a rise, not a decline, in the improper payments each year. There is little, if any, demonstrable improvement in meaningfully addressing the root causes.

Congress can evolve the law to include incentives, such as allowing agencies to keep a portion of improper payments that they reduced from the prior year and including integrity metrics — such as prevention of fraud or reduction in improper payments—for agency senior executives that impact their pay increases and bonuses. Such performance-based incentives could also be applied to staff at all levels—incentivizing them to focus on preventing and detecting improper payments and potential fraud in addition to the delivery of benefits.

Congress should also evolve the law to address a significant root cause of improper payments: the inability to access data needed to verify a payment. Among the reported improper payments in "high-risk" programs tracked by OMB on PaymentAccuracy.gov, more than half report inability to verify information as the key root cause. The reasons for this inability range from statutory limits on access to specific data (e.g., tax data) to restrictions imposed by the *Privacy Act* that create significant barriers to agencies sharing information they could use to reduce improper payments.

Congress should require high-risk programs to undertake the effort outlined in OMB's October 2021 guide on estimating improper payments that are outside an agencies control. Agencies should report to OMB the data needed to verify eligibility for a payment that is simply unavailable to them, so that OMB and Treasury can work to overcome the barriers to accessing the needed data.

Congress should also focus legislative efforts on assisting the highest-priority programs with tangible, outcome-oriented solutions, including helping them collect and use data to verify the accuracy of payments before they are made, identifying trends in the data, and implementing targeted efforts to prevent improper payments. Congress should create a dedicated antifraud office, with a presidentially appointed leader, to oversee these efforts and help facilitate the removal of data sharing barriers, as well as assist with risk assessments, data analytics and other important tools to fight fraud and improper payments.

Congress should also provide additional funding for those agencies with consistently large proportions of total improper payments estimates to conduct proactive, preventative advanced data analytics. Agencies are reluctant to divert appropriated funding to such an effort as they have not planned for and requested that funding in their annual budget. An "integrity fund" for the 13 largest improper payment programs should be established to fund program integrity efforts. Agencies that manage those programs should be required to submit plans for developing advanced analytics programs aimed at preventing improper payments and fraud to the dedicated antifraud office, who would manage the distribution of the integrity fund.

These measures will address several root causes of the continued rise in fraud and improper payments, including systemic data-related barriers and limited priority focus from agency leadership.

Question 2. In your testimony, you described Treasury's Do Not Pay system as "broken." Can you elaborate on ways the system can be enhanced? Are there things Congress can do to strengthen Do Not Pay?

Do Not Pay (DNP) was established in 2011 to provide prepayment data matching to federal agencies to identify and help prevent payments to ineligible beneficiaries. The Payment Integrity Information Act (PIIA) gave DNP the authority to work directly with state agencies that manage federally funded state-administered programs. DNP is designed for agencies to use a secure online interface to check various data sources to verify the eligibility of a vendor, grantee, loan recipient, or beneficiary to receive federal payments. The system holds great promise and enhancing it will yield significant benefits for the stewardship of taxpayer dollars.

The challenges DNP faces have been reported by the GAO and the Treasury Office of Inspector General (OIG). In October 2016, GAO found that DNP offers partial or no access to 3 of 6 databases required by the Improper Payments Elimination and Recovery Audit Improvement Act. These included Bureau of Prisons database, the Credit Alert Interactive Voice Response System (CAIVRS) and the full Social Security Administration (SSA) death data file.

Since the time of that GAO report, DNP has made significant improvements. The CAIVRS system has been to the data DNP uses and, as of March 2022, Treasury is in the process of adding prisoner data. SSA officials stated that sharing full death records requires an amendment to the Social Security Act. In December 2020, Congress passed and the President signed into law the Consolidated Appropriations Act, 2021, which requires SSA, to the extent feasible, to share its full death data with DNP for a 3-year period, effective December 2024. The full death data will be a useful addition to DNP and should help identify improper payments. Congress should hold SSA accountable for meeting this statutory requirement as it would enhance Do Not Pay's usefulness enormously.

The Office of Management and Budget (OMB) also recently clarified its guidance regarding the addition of databases to DNP. In its updated guidance (OMC Circular A-123, Appendix C). OMB announced 12 databases were added to DNP. As of March 2022, that system now leverages 20 critical databases.

It is important to note that Treasury has specifically requested from Congress access to additional data sources and the authority to access more in the future. For instance, in its FY21 Congressional Budget Justification, Treasury requested access to the National Director of New Hires (NDNH). The NDNH is a repository of new hire, quarterly wage, and unemployment insurance information, operated by the Office of Child Support Enforcement (OCSE) in HHS. The Secretary of the Treasury has access to information in the NDNH for debt collection purposes, according to the Treasury's Congressional Justification, but not for the purpose of identifying, preventing or recovering improper payments under the PIIA. Treasury further requested Congress give DNP direct authority to designate publicly available data sources to include in DNP. Under 31 USC 3354(b), any new databases proposed for DNP have to be approved by OMB after a public notice and comment period. The proposed change would expedite the designation of publicly available data sources, shortening the timeframe between a request for designation of publicly available data and its acquisition. And finally, Treasury asked Congress to give DNP increased authority to expand its user base to include other Federally funded government entities, such as Federally funded state administered programs. This would permit the Secretary to work with OMB to select customers that DNP determines can successfully assist in preventing and reducing improper payments.

The addition of databases to Do Not Pay and enhanced processes for adding databases in the future should significantly enhance the usefulness of the system, but agencies must also make better use of DNP. Treasury could address this through the use of a customer experience (CX) approach that seeks to understand the reasons agencies are not using the system and addresses the root causes. For example, GAO reported that because the matching is performed simultaneously with disbursement, agencies generally do not receive the

results in time to stop payments. More timely data matching would prove more useful to agencies, as they could then rely on Do Not Pay for prevention of improper payments, as it is intended.

GAO also recommended that OMB develop and implement monitoring mechanisms--such as goals, benchmarks, and performance measures--to evaluate agency use of the DNP working system. This recommendation remains open. OMB stated that it would "continue to work with agencies to reduce improper payments and encourage agencies to establish goals to improve payment accuracy that will be monitored and evaluated by OMB." In fiscal year 2019, OMB told GAO that Treasury does this monitoring and reports updates to OMB on a quarterly basis and that monitoring would occur in conjunction with the President's Management Agenda. The monitoring has not resulted in enhanced use of DNP. OMB and Treasury can do more to enhance the use of DNP and measure its effect on the reduction of improper payments.

GAO further reported that non-Treasury payments are not automatically matched using DNP, which means major payment sources such as the Defense Finance and Accounting Service and Medicare Fee-for-Service program do not leverage the benefits of DNP. System enhancements must be implemented so that these non-Treasury payments are included in the payment verification process.

GAO found that agencies generally receive database results after payments have been made and that half of agencies think payment integration process is a post payment function. GAO recommended that Treasury's revise its DNP Implementation Guide to clearly describe the limitations of the payment integration process, including the data sources used and the timing of matching. In response, Treasury updated its Guide to clearly describe the limitations of the payment integration process, including the data sources used and the timing of matching. However, clarifying the limitations does not address the causes and, therefore, the impacts, these limitations create.

I believe with increased funding and priority attention, DNP can be an invaluable tool in the fight against improper payments. I encourage Congress to incorporate the administration of DNP into a newly created centralized anti-fraud office and provide it the resources necessary to improve it.

Question 3. Sharing could serve as a key tool to reduce improper payments. What obstacles impede agencies' ability to share and use data effectively, and what can Congress do to mitigate those obstacles?

Obstacles to Data Sharing

Improved data sharing will certainly help reduce improper payments. The obstacles impeding agencies' collaboration largely fall into three categories: cultural, technical, and regulatory.

Cultural obstacles. Overcoming cultural issues requires changing deep-rooted perceptions and attitudes about data sharing. A general lack of trust is one such issue. A 2013 GAO report found that agencies were reluctant to share data due to both a strong sense of ownership over their data and a lack of trust in the receiving agency.[12] In 2018, the Department of Health and Human Services (DHS) noted that even among its own agencies, data owners feared that shared data could be misinterpreted by those receiving it.[3] Still in 2020, a study from IBM noted that "people issues"—including fears of losing competitive advantage and fears of being found to have data quality problems—are the biggest obstacles to sharing intergovernmental data.[4]

Another cultural issue is a perceived lack of incentive to share data. To the data owner, sharing is often seen as a "one-way street." A 2022 study from the Federal Chief Data Officers (CDO) Council found that agencies often cited a "What's in it for me?" argument.[5] A 2018 report from the HHS also notes that there are often no consequences for an agency denying or delaying data sharing.[6] Combined with the reality that data sharing initiatives are often inconvenient and time-consuming, it is difficult to incentivize agencies to expend resources to share their proprietary data for another's benefit.

Technical obstacles. Technical issues are another major area impeding data sharing among agencies. A 2021 study by the Data Foundation and Grant Thornton found that federal CDOs most frequently identified technical issues as a major challenge, including data standardization and interoperability.[7] A lack of standardization across data systems and elements makes linking that data difficult. This challenge applies to the data content as well as the data format. For example, HHS found that even within its own agencies, a single individual's name could be captured differently across multiple records. It also found that its agencies saved data in a range of file formats, including some that were not machine-readable.[8] The problem compounds when you consider the added complexity of data sharing between federal, state, and local entities. This lack of standardization results in time-consuming and tedious data cleaning tasks when agencies receive data.

---

[1] Department of the Treasury Bureau of the Fiscal Service, *Congressional Budget Justification and Annual Performance Plan and Report* (FY 2021) https://home.treasury.gov/system/files/266/14.-Fiscal-FY-2021-CJ.pdf

[2] GAO, *Data Analytics for Oversight & Law Enforcement*, Government Accountability Office, GAO-13-680SP (Washington, D.C.: July 2013), https://www.gao.gov/assets/gao-13-680sp.pdf.

[3] Office of the Chief Technology Officer, *The State of Data Sharing at the U.S. Department of Health and Human Services*, U.S. Department of Health and Human Services (Washington, D.C.: September 2018).

[4] Jane Wiseman, *Silo Busting: The Challenges and Successes of Intergovernmental Data Sharing*, IBM Center for The Business of Government (2020), https://www.businessofgovernment.org/report/silo-busting-challenges-and-successes-intergovernmental-data-sharing.

[5] Federal Chief Data Officers Council, *CDO Council: Summary of RFI Responses*, General Services Administration (Washington, D.C.: February 2022) https://www.cdo.gov/assets/documents/Summary_of_CDOC_RFI_Responses_Feb_22.pdf.

[6] Office of the Chief Technology Officer, *The State of Data Sharing at the U.S. Department of Health and Human Services*.

[7] Nick Hart, Tracy Jones, Jeff Lawton, Leigh Sheldon, and Joe Willey, *CDO Insights: 2021 Survey Results On the Maturation of Data Governance in U.S. Federal Agencies*, Data Foundation (September 2021) https://www.datafoundation.org/cdo-insights-report-2021.

[8] Office of the Chief Technology Officer, *The State of Data Sharing at the U.S. Department of Health and Human Services*

Regulatory obstacles. Regulatory barriers are the third major obstruction to data sharing. One consistent pain point is the legal requirement to negotiate data sharing agreements. These agreements are burdensome and confusing, taking months or even years to complete. A 2021 report from the CDO Council found that often the need for data access is long gone by the time the agreement is in place.[9] Navigating additional legal requirements, like privacy laws, is similarly challenging. A 2013 GAO survey about balancing data sharing and privacy concerns found that 91 percent of respondents identified confusion about the rules as a "great challenge."[10] The 2020 IBM study found that real and perceived concerns about data sharing laws persisted.[11]

Overcoming Data Sharing Obstacles

Congress can help mitigate these obstacles to data sharing. In fact, many useful recommendations are already compiled in a 2021 report from the CDO Council.[12] For example, to change cultural resistance, Congress can incentivize sharing by establishing a recognition mechanism for agencies that complete data sharing initiatives. On the other hand, agencies could be held accountable for denials or delays. The goal should be to build incrementally towards an "Ask Once" policy, where agencies would not have to ask repeatedly for access to one another's data.

To overcome technical challenges, Congress could provide further support to the CDO Council by removing the statutory sunset of the Council, which is currently scheduled for 2025. The CDO Council is already developing resources to help standardize data sharing frameworks across federal agencies. Its recommendations include establishing data sharing centers of excellence within agencies, drafting a data sharing infrastructure playbook, and reinforcing shared tools already in place like the website Data.gov. To ensure that this momentum can continue, Congress should ensure the CDO Council exists beyond 2025.

Supporting CDO Council initiatives will also address regulatory concerns about data sharing agreements. CDO Council recommendations include compiling a collection of standardized templates and developing an agreement building tool to simplify the drafting of agreement documents. Another recommendation is to establish an advisory body to mediate data sharing stalemates. The dedicated antifraud office would be well positioned to lead this body or closely collaborate with them. The federal government can also direct legal counsels to work with the CDO Council to evaluate the federal laws associated with data sharing.

Finally, Congress can increase funding for data sharing initiatives and data-focused offices. CDOs consistently flag a lack of staffing, as well as outdated hardware and software, as top concerns.[13] Empowering this group of specialists will do much to mitigate the challenges impeding data sharing.

---

[9] Federal Chief Data Officers Council, *Data Sharing Working Group: Findings & Recommendations*, General Services Administration (Washington, D.C.: December 2021), https://resources.data.gov/assets/documents/2021_DSWG_Recommendations_and_Findings_508.pdf.

[10] GAO, *Human Services: Sustained and Coordinated Efforts Could Facilitate Data Sharing While Protecting Privacy*, GAO-13-106 (Washington, D.C.: February 2013) https://www.gao.gov/products/gao-13-106.

[11] Wiseman, *Silo Busting*.

[12] *Data Sharing Working Group: Findings & Recommendations* (December 2021).

[13] Hart et al, *CDO Insights.*

Question 4. Sometimes, the data the government needs lies in the hands of the private sector. How can private-sector data support the government's efforts to mitigate improper payments in a safe, secure way? Additionally, what private sector practices or innovative information technology applications can government adapt or borrow to improve service delivery and program integrity?

Private sector industries that are vulnerable to fraud, such as banking and insurance, have long used data from the three major credit bureaus (Equifax, Experian, and TransUnion) to confirm basic identifying information such as names, phone numbers, current and past addresses, and current and past employers. However, more recently other companies, most notably LexisNexis and Socure, have compiled data that go well beyond these traditional platforms in identifying potentially fraudulent activity. Examples include:

1. Internet Protocol (IP) address reputation[14] and location
2. Email reputation and how long an address has been associated with an individual
3. Mobile phone reputation and how long a phone number has been associated with an individual
4. Alerts when a text message is forwarded to an alternate mobile phone number
5. Alerts related to mailing addresses associated with fraud
6. How long a person has been associated with a particular mailing address
7. How many social security numbers are associated with a particular identity

LexisNexis and Socure both engage in a private consortium model to collect these data. As a condition of membership, each company that joins the consortium agrees to provide information from their internal investigation units. In this way, all members of the consortium share information about fraud actors and activities. Although some agencies are already benefitting from using solutions like those offered by LexisNexis and Socure, the federal government could go even further, perhaps starting its own consortia to share reputational data from internal investigations to mitigate improper payments.

The U.S. government could also benefit from adapting some of the private sector's best practices in using publicly available data. For example, since 2019 the banking industry has collaborated with the Social Security Administration in setting up an automated system that instantly evaluates whether a given social security number is valid. U.S. government agencies could and should be able to set up similar automated checks against publicly available Social Security Administration records.

Data analytics is another area in which the private sector is leading the way in using technology to root out fraud. The data analytics techniques that are in practice today range from simple to more advanced, including:

- **Rule-Based Analytics -** A transaction level technique to prevent common fraud based on known patterns.
- **Anomaly Detection Analytics –** An aggregate-level technique that uses "unsupervised modeling" to identify outliers compared to peer groups based on unknown patterns among common and individual fraudsters.
- **Predictive Analytics -** Techniques that use statistical algorithms and machine learning to identify the likelihood of future outcomes based on historical data.
- **Network / Link Analytics –** A technique that can be useful for uncovering organized fraud and associations between fraudsters by using social network analytics, looking at linked patterns for investigation and discovery.
- **Text Analytics –** A technique that scrapes text sources and parse text strings to detect patterns of fraud among social media pages, online reviews, and email content.

[14] "Reputation" is an assessment of whether something has been associated with known fraudulent activity. For example, if a bank's internal investigation identifies an IP address as being associated with fraudulent activity, it will flag that IP address as potentially compromised in its reputation assessment.

The banking industry showcases how data analytics can be used to integrate quick, unseen fraud checks into everyday service delivery. Each time a customer swipes, taps, or inserts a credit card, data analytics are working in the background to provide an instantaneous check on the transaction. If the bank's rule-based analytics and artificial intelligence models indicate that the user and the owner of the credit card are the same, then the system will approve the transaction. If the bank's data analytics indicate that the user and the owner are not the same—perhaps because the user is in another country and the owner is not known to be travelling—then the system will automatically deny the transaction. This approach typifies the private sector's focus on using automated checks to allow for "frictionless" service delivery while protecting against fraudulent activity. In addition, having up-to-the-minute reporting allows organizations to adjust to evolving fraud patterns within minutes rather than days.

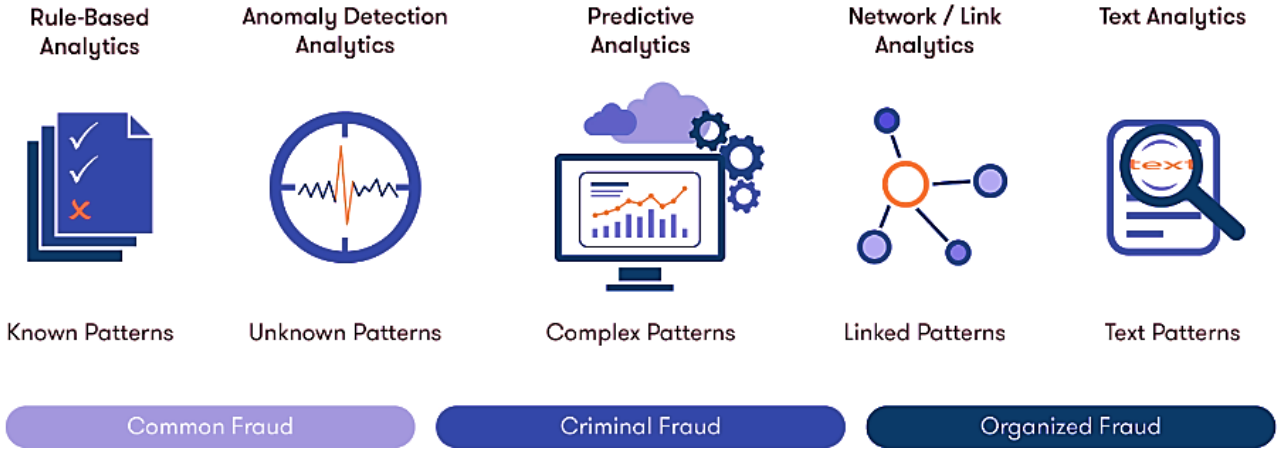

Figure 1. Data analytics techniques range from simpler rule-based analytics to advanced predictive analytics.

One emerging area is clear, deep, and dark web analytics. Firms specializing in these methods can conduct keyword searches of U.S. programs, vendors, systems and technologies, general fraud descriptors, and general government descriptors. They run these searches in English, Russian—which is a common language used among online threat actors—and other languages. Leveraging these analytic methods, the U.S. government could identify hidden marketplaces and communication platforms on which malign actors exchange tools, methods, databases, and credentials to defraud U.S. citizens and businesses.

Other technological advances could be integrated into the public sector's arsenal for mitigating fraud risks while reducing customer friction. Some offerings that are widely used in the private sector include:

- Multi-Factor Authentication capabilities, such as One Time Passcode
- Biometrics, such as a pass list of fingerprint and voice
- Password-less methods for authentication, which can be achieved through the use hardware tokens, one-time password generators, or known mobile device detection
- Matching locations to fiberoptic lines for call center authentication

Before deploying these sorts of tools, however, the U.S. government needs to carefully balance its goals of improving service delivery and program integrity with its goals of protecting individuals and ensuring a right to privacy. Privacy experts are rightfully concerned about government agencies sharing biometric data with private technology providers that offer holistic solutions incorporating all their available data sources. This tension was on full display when the IRS decided to contract with a private firm, ID.me, to deploy facial recognition software to protect tax accounts, only to abandon that plan following backlash from Congress, taxpayers, and privacy advocates. I believe these problems resulted from an absence of regulation of private sector companies and a lack of meaningful alternative solutions for identity proofing.

Beyond identify verification, another key focus within the private sector has been leveraging technological advances and automation to simplify platforms and orchestrate data across multiple locations. These types of

capabilities open the opportunity for organizations to build “fusion teams,” combining antifraud resources that traditionally work independently. For example, the banking industry is now combining its cyber, fraud, anti-money laundering, and credit teams under one group. They have discovered great efficiency and fraud mitigation successes when these teams work together rather than in silos.

It is past time for the U.S. government to adapt these private sector technologies and best practices to improve service delivery and program integrity. The threat is evolving, and like their commercial counterparts, agencies need to be doing the same.