Chapter Twelve

Future of Payment Integrity within the U.S. Federal Government

By Renata Miskell
U.S. Department of the Treasury

INTRODUCTION

Paying the right person, in the right amount, at the right time—from Social Security benefits to tax refund payments—constitutes a bedrock of trust in government. Disbursing payments, whether via check or (ideally) direct deposit, is one of the most direct ways that the federal government interacts with the public. It also represents one of the primary levers that the federal government uses to provide a safety net to vulnerable populations, promote economic prosperity, and ensure national security. Put simply, payment integrity stands as one of the most important functions that government performs to promote the public good.

Payment integrity can strengthen trust in government by reducing improper payments and preventing fraud in federal programs. An improper payment is defined by the most recent payment integrity legislation, the Payment Integrity Information Act (PIIA) of 2019,[1] as a payment that should not have been made.[2] Improper payments occur when funds go to the wrong recipient, the right recipient receives the wrong amount; absent documentation to support a payment. As such, improper payments may not ultimately result in a monetary loss to the government. While not all improper payments are due to fraud and not all improper payments will ultimately represent a monetary loss to the government, all improper payments degrade the integrity of government programs and compromise citizens' trust in government.

This chapter explores a vision that would empower agencies and federally funded programs, including state administered programs, to use data proactively in promoting payment integrity. This vision involves collaborating with federal and state agencies to share data and provide actionable business solutions to transform the identification, prevention, and recovery of improper payments; and to mitigate the effects of fraud. It also emphasizes a pivot from compliance to prevention-focused strategies, promoting the use of data and analytics and collaboration across government and the private commercial sectors. Emerging technologies like artificial intelligence and machine learning are crucial catalysts for this transformation, enhancing data analysis, streamlining processes, facilitating data sharing and the reuse of data, and improving fraud detection and prevention; all while prioritizing data privacy and security.

From Recovery to Prevention

For American citizens, government must get payments right. A late unemployment insurance payment—or worse, one intercepted in an act of fraud—can have severe consequences for a family relying on that assistance during

a time of financial hardship. Similarly, if tax dollars are wasted on duplicate payments or payments to ineligible recipients, public trust in government will erode, and taxpayers and lawmakers will be less willing to fund future financial assistance programs. Moreover, when the federal government reissues a payment to correct an improper payment, it bears significant additional operational costs, on top of the inconvenience and added burden to the recipient.

The government recently saw the positive effects of federal disaster support in the form of loans and direct payments delivered in record time. The U.S. Department of the Treasury (Treasury) rapidly issued three waves of direct relief payments, or Economic Impact Payments (EIP), during the COVID-19 pandemic. The amounts of these payments dwarfed the size of similar historic efforts and were delivered in record speed, including a third round of payments where Treasury issued 174 million payments totaling $407 billion within a few days of the enactment of authorizing legislation.

At the same time, unprecedented spending in response to the COVID-19 pandemic exposed vulnerabilities in federal and state government payment systems, leading to increased fraud, and exacerbating long-standing payment integrity challenges. For example, in a rush to quickly get relief to businesses and nonprofits, the Small Business Administration (SBA) disbursed over 4.5 million potentially fraudulent loans and grants via the Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program totaling over $200 billion. Despite substantial oversight and law enforcement efforts, only $30 billion in EIDL and PPP funds have been seized or returned to SBA as of June 2023.[3]

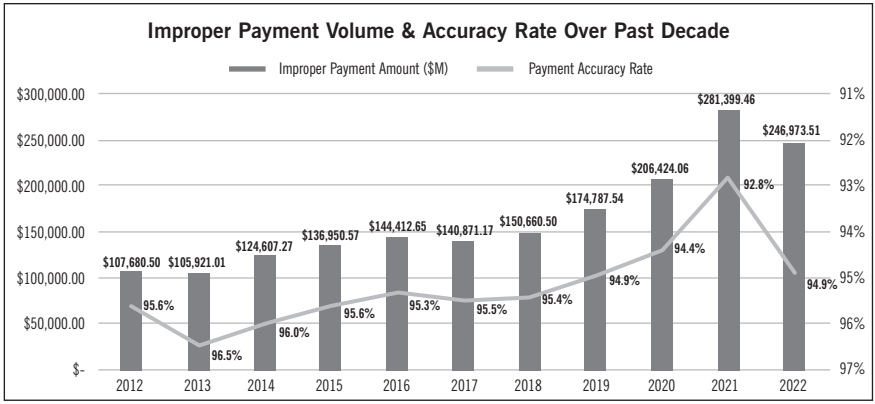
The federal government needs to do more to manage risk and shift the focus from recovery to prevention. No one can predict when the next large-scale emergency or disaster will occur, but when they do, fraudsters will look to exploit weaknesses in government assistance programs. Just as Treasury issues payments rapidly to those in need, it also needs to stop fraudsters and improper payments more broadly in near real-time.

Current Issues and Challenges

Over the past two decades, the focus of laws and regulations governing the identification and recovery of improper payments has evolved from reporting to emphasize prevention and promoting the use of centralized services. Despite positive advancements in legislation and policy as well as improvements in compliance reporting and overall transparency as federal government spending has increased over the past decade, so have improper payments.

According to the Government Accountability Office (GAO), since 2003, when federal agencies began keeping track of improper payments, cumulative improper payment estimates total almost $2.4 trillion.[4] The payment accuracy rate has hovered around 95 percent, with a high of 96.5 percent in 2013 and a low of 92.8 percent in 2021. Five programs account for 78 percent of all improper payments;[5] however, approximately 92 percent of overpayments in high-priority programs were beyond the control of a single agency.[6] While this was a decrease from the FY2021 estimated total of $281 billion, the payment accuracy rate remains unchanged at 95 percent (see Table 1).

Table 1: Improper Payment Volume & Accuracy Rate over the Past Decade



Source: U.S. Government Accountability Office

Persistent challenges make it difficult for any single federal program or agency to move the needle in advancing payment integrity. The urgency to "get money out the door" in an emergency is a challenge for federal programs, and so are their efforts to access and use data in a timely manner to prevent improper payments and fraud. Eligibility criteria such as death and income are recurring payment integrity challenges because of the difficulty in accessing verification data. Insufficient data analytics for fraud prevention only exacerbate the problem. Moreover, misaligned incentives and complex systems limit accountability. While government has advanced in its ability to estimate improper payments, reporting is after the fact and not integrated into the pre-payment and pre-award processes.

Vision for Advancing Payment Integrity

The best way to reduce fraud and improper payments is to prevent them from happening at all, by performing risk assessments and building in proper internal controls at the front end when designing and executing federal pro-

grams. Guidance from OMB[7] and GAO,[8] as well as resources that promote best practices,[9] emphasize the importance of assessing risk and accessing and using quality information and data to detect, prevent, and monitor improper payments and fraud. Given the importance of timely access to data, the use of technology and advanced analytics are crucial catalysts for also advancing payment integrity.

Imagine if the federal government could enable agencies and federally funded state administered (FFSA) programs to prevent and detect fraud and improper payments in real-time throughout the payment lifecycle—from pre-award to pre-payment, through sub-award, to post payment processes. As the primary disbursing agency responsible for over 90 percent of federal payments, Treasury has developed a bold vison to empower government to use data proactively in promoting payment integrity. The vision involves collaborating with federally funded and state-administered programs to provide actionable solutions to transform the identification, prevention, and recovery of improper payments and to mitigate the effects of fraud.

This vision mirrors the experience the public has engaging in financial transactions through banks or when using credit cards. Private sector financial institutions and payment networks arguably have greater access to capital, more flexibility to innovate, and fewer constraints and dependencies than government agencies. However, Treasury has three distinct advantages—scale, scope, and authority—that can springboard the federal government's ability to advance payment integrity. In FY2022, Treasury's Bureau of the Fiscal Service (Fiscal Service) securely disbursed approximately 1.4 billion payments totaling more than $5.3 trillion. These payments went to 100+ million individuals and entities, with 96 percent disbursed electronically, creating a modern, seamless, and cost-effective payment experience.[10] Treasury's central disbursing authority enables it to touch virtually every aspect of the payment lifecycle. Just as Treasury has accelerated the speed with which government can make payments, so too can it accelerate the government's ability to prevent fraud and reduce improper payments by leveraging technology and advanced analytics.

Three Strategies for Advancing Payment Integrity

Payment integrity relies on a complex web of stakeholders, systems, processes, and controls throughout the payment lifecycle. Advancing Treasury's vision of real-time detection and prevention will require a digital transformation throughout the payment lifecycle. Three key strategies can advance this vision: focusing on prevention, embracing best practices, and strengthening partnerships.

Focus on prevention

The best way to reduce the fraud and improper payments rate is to make sure they do not happen in the first place. Shifting to real-time detection and prevention is the building block on which the other strategies rest. This foundational focus makes moving forward on payment integrity possible.

Payment integrity as a service. To achieve real time detection and prevention, government needs to move away from siloed, manual processes and shift to digitized, modular payment integrity capabilities using cloud technology. Digitization of payment integrity activities is a force multiplier, enabling government to meet the enormous scale, scope, and complexity of federal award and payment processes. A digital operating model enables rapid learning that can drive continuous improvement, expedite connections across the payment lifecycle, create the ability to scale quickly as funding increases, and efficiently implement payment integrity capabilities as new programs are established. This also helps prevent improper payments before they go out the door.

Just like the "All Electronic Treasury" initiative that converted millions of paper check payments to electronic payments over the past decade, this transformative shift to a digital operating model as a service is achievable with sustained leadership commitment. Treasury's Bureau of the Fiscal Service has jump started such an effort. Since 2011, it has been developing and enhancing the Do Not Pay (DNP) Working System (previously named DNP Business Center) to assist agencies in identifying and preventing improper payments.

Moreover, with the recently established Office of Payment Integrity, the Fiscal Service has brought together detection and prevention services with payment and post-payment functions. This has already enabled a more holistic and integrated set of payment integrity solutions. For example, in FY2021, the Fiscal Service launched its commercial Account Verification Service (AVS) pilot. The AVS's main purpose was to verify bank account status (e.g., open or closed) prior to payment in advance of the third round of EIP and the Advance Child Tax Credit (ACTC). By the end of FY2022, the Fiscal Service screened 2.7 million accounts through AVS, preventing $130 million of improper payments. In addition to expanding access to AVS to FFSA programs via DNP, Treasury can build on the success of using commercial and government data sources to provide actionable payment integrity services.

Leverage emerging technology and advanced analytics. Treasury continues to modernize DNP's platform to scale and optimize data pipelines, support artificial intelligence (AI) and machine learning (ML) processes, and advance analytics toward a fully digitized "payment integrity as a service." Emerg-

ing technologies like AI and ML are crucial catalysts for this transformation, enhancing data analysis, streamlining processes, facilitating the reuse of data, and improving fraud detection and prevention. As the central federal disbursing agency, Treasury has the unique advantage of having access to 1.4 billion payment records in a given fiscal year. Supervised machine learning could assist human experts in deciding whether to issue a payment based on data and prior history, such as reoccurring benefit payments. Unsupervised learning could help detect fraud by identifying anomalies in the payment data across federal agencies and programs. These models can enable continuous monitoring throughout the payment lifecycle, ensuring swift and adaptive responses to emerging fraud threats.

Advanced analytics can integrate additional data sources and calibrate AI/ML models to meet their unique program requirements. For example, an agency could leverage the location data from a computer or phone being used to apply for federal programs to provide location data or behavioral patterns that help flag potential risk or anomalies. Treasury could become the central hub for reporting suspicious or fraudulent activity in the federal payment lifecycle, as the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) does as the operational lead for federal cybersecurity.

Embrace best practices

At the heart of promoting payment integrity is our ability to use data to learn and respond to new and changing requirements, emerging threats, and opportunities to improve the customer experience with digital services.

Payment integrity data catalog and schema. A payment integrity data catalog can support payment decisions by assembling data to be easily identified and integrated into agency pre-award and pre-payment processes. Given the bespoke nature of federal programs, to make centralized data actionable, the data will need to be well documented to include relevant metadata. This payment integrity data catalog should include information including data definitions, authoritative source, formatting, and validation. Moreover, Treasury can expedite the use of authoritative data by mapping the relationships between data and documenting validation rules and logic to enable reuse. Specifically, Treasury can promote connections between payment and award processes by enforcing the use of standard entity identifiers and contract and financial assistance award identifiers in the payment process.

Treasury can build upon the Governmentwide Spending Data Model (GSDM), which powers USAspending.gov and is the authoritative source for the terms, definitions, formats, and structures for hundreds of distinct data elements that show how federal dollars are spent. The benefit of this

approach is that the GSDM already makes the fundamental connections between government accounting, budget, procurement, and financial assistance data and is widely adopted by federal agencies to meet federal transparency requirements.[11] Moreover, improper payments reporting requirements established under PIIA and reported in to PaymentAccuracy.gov could be incorporated to improve the connection and alignment with existing federal transparency, financial, and performance reporting, ultimately advancing transparency and accountability to the public.

Secure data sharing. A secure, robust, and scalable computational infrastructure along with well documented Application Program Interfaces (APIs) can streamline access to data and enable data sharing all while protecting privacy and security. For example, the government could address privacy concerns and improve data sharing by establishing "yes"/"no" attribute validation services for key sensitive data such as validating income. Once mature, Congress could point to digital payment integrity validations when developing legislation that establishes new programs or expands existing programs.

The government has already implemented similar services, notably the Social Security Administration's Electronic Consent Based Verification Service (eCBVS) that enables financial institutions to conduct Social Security Number verifications.[12] Similarly, the newly established National Accuracy Clearinghouse (NAC) can help states prevent issuing duplicate Supplemental Nutrition Assistance Program (SNAP) benefits without requiring the storage of personally identifiable information (PII).[13]

Payment monitoring as a service. As with monitoring identity theft using commercial services, the government could empower individuals to monitor payments they receive from the federal government. Today, individuals must go to multiple government agencies to get the status of their benefit payments. Just as government has implemented a centralized platform for vendor invoicing and grant payments,[14] this service could help protect against fraud and identity theft by alerting users of changes to reoccurring payments or new payments. Similarly, with appropriate privacy and security controls in place, federal agencies could subscribe to the service to monitor potentially duplicate or improper payments.

Strengthen partnerships

Strengthening partnerships through collaboration is critical to defending against current payment integrity threats and building toward this future vision. Collaboration and partnerships can reduce startup costs and increase the scale of solutions that reduce improper payments. Three key partnerships will be essential to build and nurture at each level:

Federal agencies and FFSA programs. Given that hundreds of billions of federal funds (over $720 billion annually prior to the COVID-19 pandemic) are administered at the state level, a majority of improper payments are made by programs administered by the state, such as Medicaid or unemployment insurance. Moreover, with federal grants being the fastest growing source of revenue for states, ensuring payment integrity between federal agencies and states is more important than ever.[15] The recently enacted PIIA legislation provides state agencies that manage federally funded state-administered programs, "access to, and use of, the Do Not Pay Initiative for the purpose of verifying payment or award eligibility for payments."[16]

Chief financial officers (CFOs)/financial managers and program managers. One of the biggest disincentives that agencies face in preventing and detecting improper payments and/or fraud is the pressure to get "money out the door" to respond to an emergency and/or to meet statutory requirements. Unfortunately, this can lead to the program office not establishing adequate internal controls up front. At the same time, agency CFOs and financial managers must comply with improper payment reporting requirements but may not have adequate visibility or ability to improve payment integrity. Keeping in mind that financial managers and program managers are ultimately aligned in their desire to execute the agency mission, agencies should promote collaboration and proactive information sharing.

Oversight entities and implementing agencies. Consistent with OMB Memorandum M-22-04, Promoting Accountability through Cooperation among Agencies and Inspectors General (December 3, 2021), collaboration and the sharing of best practices between implementing agencies and the oversight community should be promoted, especially when initiating or significantly expanding new programs.[17] The OMB-led "Gold Standard Meetings" demonstrated that oversight and implementing agencies can promote a cooperative and early prevention model for fraud prevention and program integrity, while still respecting the independence of the oversight community.

In addition to collaboration and information sharing, government needs to gain a deeper understanding of the challenges that stakeholders in the payment lifecycle face to advance payment integrity. Specifically, Treasury can conduct targeted user research to gain a better understanding of current agency and state challenges to detecting and preventing fraud and improper payments. These insights can help Treasury direct its limited resources towards highest value efforts and design payment integrity solutions that integrate with business processes throughout the payment lifecycle.

LOOKING FORWARD

The unprecedented spending in response to the COVID-19 pandemic was a necessary intervention that also exposed federal and state award and payment systems and processes to greater fraud and exacerbated long-standing improper payment challenges. When the need arises to address similar emergencies in the future, the government should be able meet this need without waste, fraud, or abuse.

There is progress being made[18] but more needs to be done. Treasury can play a greater role in promoting payment integrity by empowering federal programs to pursue the vision of detecting and preventing fraud and improper payments in real-time. This vision can be achieved by focusing on prevention through the use of technology and advanced analytics, embracing best practices in data sharing, and strengthening partnerships through collaboration at every level of government. By embracing this vision, the federal government can make significant strides in payment integrity, reduce fraud, and safeguard taxpayer resources.

Renata Miskell *is the Deputy Assistant Secretary for Accounting Policy and Financial Transparency, at the U.S. Department of the Treasury, Washington, D.C.*

Endnotes

1 S.375—Payment Integrity Information Act of 2019, Public Law 116-117, https://www.congress.gov/bill/116th-congress/senate-bill/375/text.

2 31 U.S.C. 3351(4).

3 U.S. Small Business Administration, "COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape," Report 23-09, June 27, 2023, https://www.sba.gov/document/report-23-09-covid-19-pandemic-eidl-ppp-loan-fraud-landscape.

4 U.S. Government Accountability Office, Improper Payments: Fiscal Year 2022 Estimates and Opportunities for Improvement, GAO-23-106285, March 29, 2023, https://www.gao.gov/products/gao-23-106285.

5 The five program areas include: (1) Medicaid ($81 billion), (2) Medicare ($47 billion), (3) the Paycheck Protection Program ($29 billion), (4) Unemployment Insurance ($19 billion), and (5) Earned Income Tax Credit ($18 billion). See GAO-23-106285.

6 Per OMB, high-priority programs are those programs for which agencies report estimated monetary loss from improper payments in excess of $100 million.

7 See Circular A-123, Appendix C; U.S. Government Accountability Office, Standards for Internal Control in the Federal Government, September 2014, https://www.gao.gov/products/gao-14-704g.

8 U.S. Government Accountability Office, Standards for Internal Control in the Federal Government, September 2014, https://www.gao.gov/products/gao-14-704g.

9 See: U.S. Chief Financial Officers Council and U.S. Treasury, Bureau of the Fiscal Service, The Antifraud Playbook, October 2018, https://www.cfo.gov/assets/files/Interactive-Treasury-Playbook.pdf; U.S. Government Accountability Office, A Framework for Managing Fraud Risks in Federal Programs, July 2015, https://www.gao.gov/assets/gao-15-593sp.pdf; and U.S. Government Accountability Office, A Framework for Managing Improper Payments in Emergency Assistance Programs, July 2023, https://www.gao.gov/assets/gao-23-105876.pdf.

10 U.S. Department of the Treasury, Bureau of the Fiscal Service, Progress Statement 2022: The Future of Federal Financial Management, February 2023, https://fmvision.fiscal.treasury. gov/files/progress-statement-2022.pdf.

11 The Federal Funding Accountability and Transparency Act (FFATA) and the Digital Accountability and Transparency (DATA) Act of 2014.

12 U.S. Social Security Administration, "Information About eCBSV," https://www.ssa.gov/dataexchange/eCBSV/?tl=0.

13 U.S. Department of Agriculture, Food and Nutrition Service, "National Accuracy Clearinghouse (NAC)," Updated February 15, 2023, https://www.fns.usda.gov/snap/nac.

14 Invoice Processing Platform (IPP) for vendors and the Automated Standard Application for Payments (ASAP) for federal agencies and recipient organizations.

15 GAO, see "Federal Grants to State and Local Governments," https://www.gao.gov/federal-grants-state-and-local-governments.

16 S.375—Payment Integrity Information Act of 2019, Public Law 116-117, https://www.congress.gov/bill/116th-congress/senate-bill/375/text.

17 Office of Management and Budget Memorandum 22-04, Promoting Accountability through Cooperation among Agencies and Inspectors General, December 3, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-04-IG-Cooperation.pdf.

18 For example, the GAO, OMB, Treasury, and the Office of Personnel Management (OPM) are partnering to advance payment integrity under the Joint Financial Management Improvement Program (JFMIP). This effort seeks to strengthen trust in government by promoting payment integrity in federal programs, focusing on prevention, promoting best practices, and strengthening partnerships.