U.S. Government Accountability Office

Improper Payments and Fraud: How They Are Related but Different

GAO-24-106608
Q&A Report to Subcommittee on Legislative Branch, Committee on Appropriations, House of Representatives
December 7, 2023

Why This Matters

Improper payments are a long-standing, significant problem in the federal government.[1] Since fiscal year 2003, executive agencies have reported cumulative improper payment estimates of about $2.4 trillion, including $247 billion for fiscal year 2022. Improper payments are any payments that should not have been made or that were made in an incorrect amount, which can stem from various causes, including fraud. Fraud involves obtaining a thing of value through willful misrepresentation. Willful misrepresentation can be characterized by making material false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity. The extent of fraud government-wide will likely never be known with certainty because not all fraud will be detected, investigated, and adjudicated through judicial or other systems. As of December 2023, we are exploring ways to estimate the amount of fraud that affects the federal government.

Both improper payments and fraud result in significant financial and nonfinancial impacts to the integrity of federal programs. They erode public trust in government, waste taxpayer dollars, and hinder agencies' efforts to execute their missions and program objectives effectively and efficiently. Legislation, guidance from the Office of Management and Budget (OMB), and standards for internal control in the federal government have increasingly focused on the need for program managers to strategically address improper payments, including those resulting from fraud. Understanding the relationships and distinctions between improper payments and fraud is important to more effectively target the associated root causes and mitigate the impacts of each.

House Report 117-389, accompanying the Legislative Branch Appropriations Act, 2023, includes a provision for GAO to provide quarterly reports in improper payments. In fiscal year 2023, we issued three reports under this provision.[2] In this fourth report, we describe examples of the relationships and distinctions between improper payments and fraud. We also describe relevant GAO and other federal guidance and executive agency efforts since 2015 to manage and reduce the causes and impacts of improper payments and fraud.

Key Takeaways

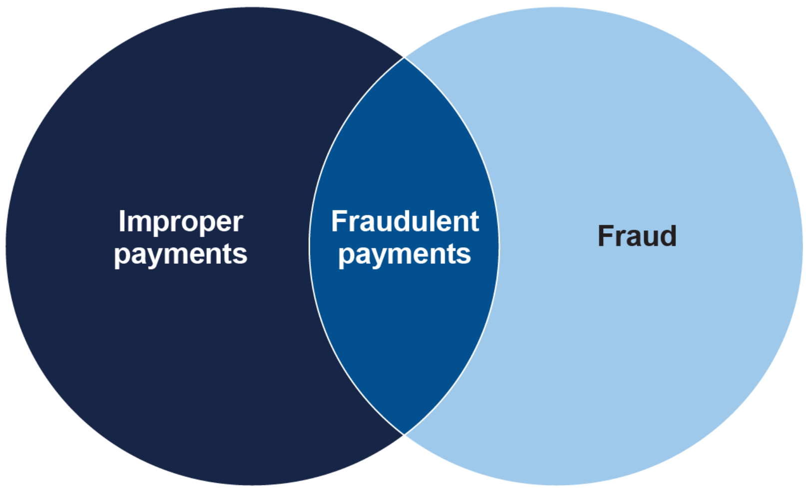
- Improper payments and fraud are distinct concepts. Improper payments can have fraud-related root causes and impacts, but not all are caused by fraud.
- We have made over 40 recommendations to agencies and published guidance to help them better use data to manage fraud risks that include fraud-related improper payments. Agencies had not fully implemented more than half of these recommendations as of August 2023. We have also recommended that Congress take action in this area, which it had not yet done as of September 2023.

- Implementing our recommendations and guidance can help agencies address the challenges of fraud-related improper payments, save taxpayer dollars, and better accomplish their missions and objectives.

Are improper payments and fraud the same thing?

No. Improper payments and fraud are two distinct concepts that are not interchangeable but are related, as figure 1 shows. For example, while all fraudulent payments are considered improper, not all improper payments are due to fraud. Similarly, there are types of fraudulent activity that do not result in improper payments (i.e., nonfinancial fraud).

Figure 1: Relationship between Improper Payments and Fraud

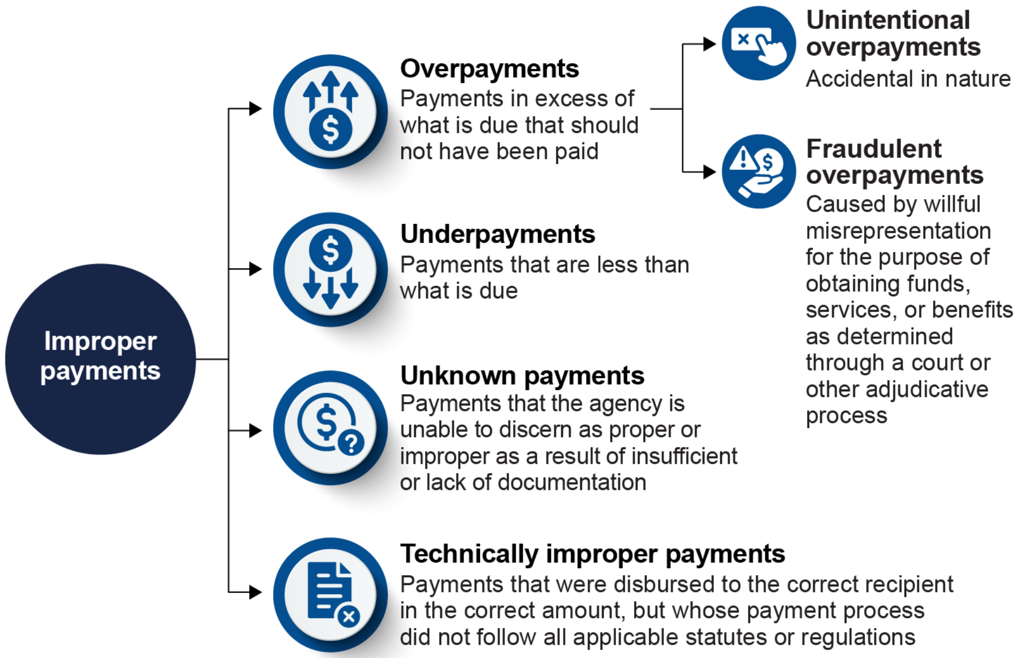


Source: GAO. | GAO-24-106608

Note: This figure is intended to show the relationship between improper payments and fraud and is not to scale.

As figure 2 shows, improper payments of federal funds, including those administered by state and local governments, can include different types of erroneous payments. Some improper payments are fraud-related and some are not. For example, a non-fraud-related improper payment might result from unintentional administrative errors or payments made in the correct amount but without following applicable statutes and regulations. Improper payments can also include underpayments caused by nonpayment or incomplete payment to recipients to which the funds are owed.

Figure 2: Components of Executive Agency Improper Payment Estimates

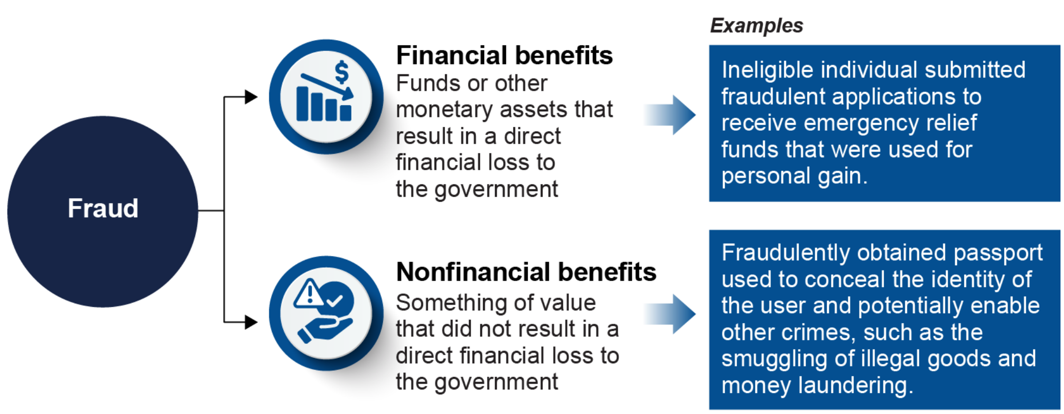


Source: GAO analysis of relevant laws and Office of Management and Budget guidance; Icons-Studio/stock.adobe.com (icons). | GAO-24-106608

Fraud-related improper payments are different from other types of improper payments because they generally involve individuals or entities intentionally or knowingly providing false information (e.g., incorrect eligibility or identity information to receive a benefit from the federal government).

Two other distinctions are that (1) improper payment determinations are made by agency officials while fraud determinations can only be made through the judicial or other adjudicative system, and (2) improper payments involve payments (i.e., financial benefits) whereas fraud can involve benefits that are nonfinancial in nature, as figure 3 illustrates.

Figure 3: Examples of Financial and Nonfinancial Benefit Fraud



Source: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-106608

Fraudulently obtained nonfinancial benefits can lead to improper payments by providing access to payments that individuals, businesses, or other entities are not eligible to receive. For example, companies have falsely certified their ownership or other eligibility criteria to the government to fraudulently obtain status as a small or disadvantaged business eligible for contracts or Small Business Administration set-aside programs.[3] This nonfinancial benefit resulted in improper payments when these companies improperly received government contracts specifically set aside for small or disadvantaged businesses.

Fraudulently obtained nonfinancial benefits may not always result in improper payments but can still have other impacts, such as on trust in government and an agency's reputation. They can also create national security, criminal, health, safety, and other risks. For example, we have previously reported that fraudulently obtained aircraft registrations pose a risk because they can be used to conceal the identity of an aircraft's owner, facilitate criminal activity, and pose national security and safety risks.[4]

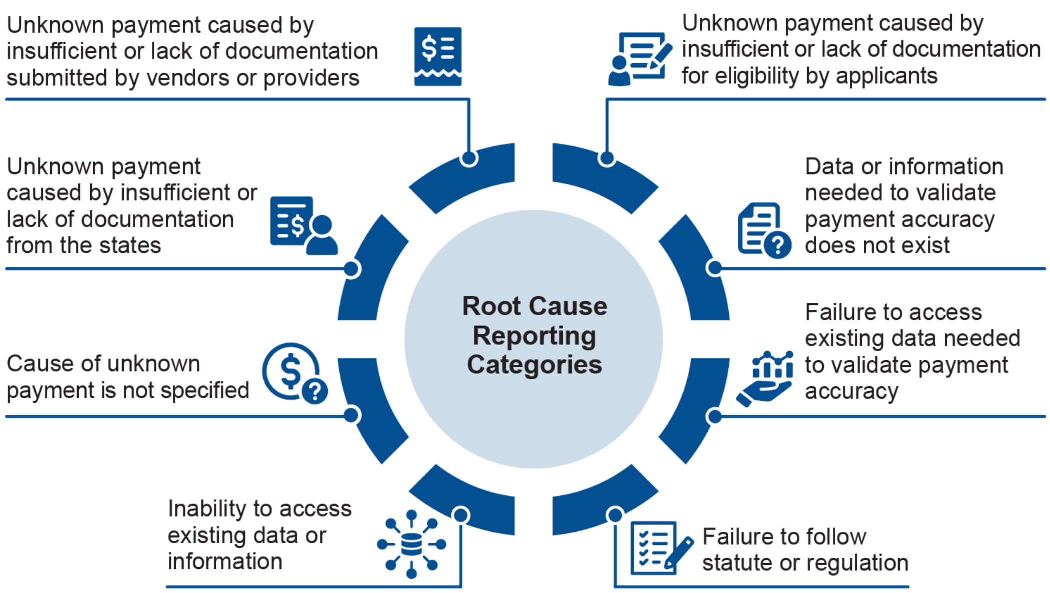
What are the root causes of improper payments, including those related to fraud?

Root causes are activities that lead to improper payments—including those due to fraud—and that, if corrected, would prevent the improper payment from occurring. The causes of improper payments can vary from unintentional administrative errors to the willful misrepresentation inherent in fraud. According to OMB guidance, identifying root causes of improper payments is critical to formulating effective corrective actions.[5]

Improper payment root causes. OMB guidance provides root cause categories for program administrators to use as a starting point when identifying reasons improper payments occurred. This guidance directs agencies to categorize their improper payment estimates by root cause and to distribute its total improper payment estimate across the root cause categories provided by OMB.

Although fraudulent activities could be associated with each of OMB's categories, OMB guidance does not identify fraud as a separate root cause category. For fiscal year 2022, agencies reported the root cause categories detailed in figure 4 to OMB.

Figure 4: Improper Payment Root Cause Categories That Agencies Reported to the Office of Management and Budget for Fiscal Year 2022



Source: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-106608

While OMB's guidance is provided to agencies as a starting point for categorizing root causes, it notes that further work may be needed to identify the true root cause that ultimately led to an improper payment. Agencies attributed about $225.5 billion (approximately 91.3 percent) of improper payment estimates reported for fiscal year 2022 to four root cause categories specified in OMB guidance, as table 1 shows.

Table 1: Major Improper Payment Root Cause Reporting Categories for Fiscal Year 2022

Root cause reporting category	Root cause example	Fiscal year 2022 estimated improper payment amount (rate)
Failure to access data/information needed	Failure to access the appropriate information to determine whether a beneficiary or recipient should be receiving a payment, even though such information exists and is accessible to the agency or entity making the payment. For example, when an agency with access to the Social Security Administration Death Master File fails to utilize it and improperly sends payment to a deceased individual.	About $145.1 billion (approximately 58.8 percent)
Inability to access the data/information	A situation in which the data or information needed to validate payment accuracy exists but the agency or entity making the payment does not have access to it. For example, statutory constraints preventing an agency from being able to access recipients' earning or work status through existing databases that would help prevent improper payments.	About $35.9 billion (approximately 14.5 percent)
Data/information needed does not exist	A situation in which there is no known database, dataset, or location currently in existence that contains the data/information needed to validate the payment accuracy prior to making the payment. For example, an agency unable to confirm that an individual receiving a benefit based on their health or a medical condition provided complete medical evidence because no database with that information exists.	About $24.2 billion (approximately 9.8 percent)
Unknown payment caused by insufficient or lack of documentation from applicants to determine eligibility	A payment that could be either proper or improper, but the agency is unable to discern whether the payment was proper or improper because of insufficient or lack of documentation. For example, an agency conducting a periodic review to determine continued eligibility for a benefit does not have all the information in the beneficiary's case file to confirm continued eligibility.	About $20.3 billion (approximately 8.2 percent)

Source: GAO information and relevant Office of Management and Budget guidance. | GAO-24-106608

Although not required, agencies may also provide additional details on improper payment root causes in their annual financial reports, such as the reason an agency did not access available data.

Fraud root causes. *Standards for Internal Control in the Federal Government*, *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), and our prior reporting have identified opportunity, incentive, and rationalization as risk factors that can contribute to fraud in federal programs.[6] We have also reported that programs with weak internal controls can be more vulnerable to fraud and may lack the necessary safeguards to prevent, detect, and respond to fraud. In addition, we have previously reported on specific mechanisms that individuals can use to engage in fraudulent activities, such as misrepresentation, document falsification, social engineering, data breaches, cybercrime, and coercion.[7]

These fraud mechanisms can also align with OMB's improper payment root cause categories, reflecting the risk for both inadvertent errors and fraud. For example, the fraud mechanisms of document falsification or misrepresentation could also underlie the root cause categories of improper payments related to the inability or failure to access data, such as eligibility or identity verification information.

Agencies relying on program participants to self-report and self-certify information on agency forms—without independently verifying such information—could miss opportunities to prevent improper payments or fraud. In October 2021, we identified fraudulent activities related to unemployment insurance programs that included individuals' use of stolen or fake identity information or personally identifiable information to apply for and receive unemployment benefits.[8] The Department of Labor has also reported that fraud has historically been a leading cause of unemployment insurance improper payments. In addition, it noted that stolen personally identifiable information and program weaknesses have allowed criminals to defraud unemployment insurance programs.

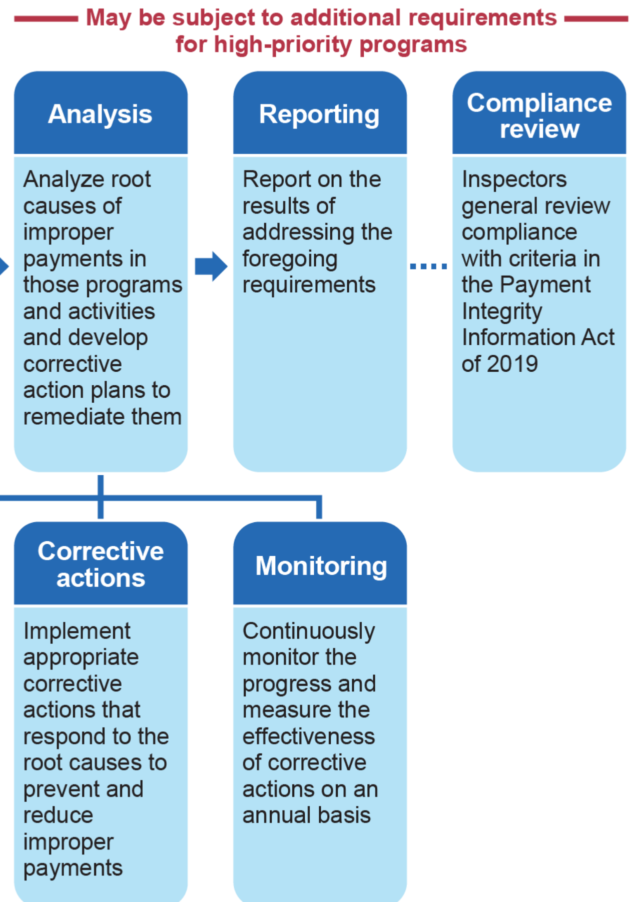
How are federal agencies required to manage improper payments and fraud?

The Payment Integrity Information Act of 2019 (PIIA) contains requirements for managing improper payments and fraud.[9] Requirements for agencies to manage improper payments include identifying risks, taking corrective actions, and estimating and reporting on improper payments in programs they administer. The improper payment estimation process is not designed to detect or measure the amount of fraud that may exist.

PIIA's requirements related to fraud generally involve implementing control activities to prevent, detect, and respond to fraud.

Requirements for managing improper payments. Under PIIA, agencies are required to develop improper payment estimates for programs that may be susceptible to significant improper payments.[10] Improper payments are considered "significant" if in the preceding fiscal year they may have exceeded either (1) 1.5 percent of program outlays and $10 million or (2) $100 million (regardless of the improper payment rate). Under PIIA, agencies with high-priority programs are subject to additional reporting requirements.[11] OMB has assigned a high-priority designation to programs with estimates of improper payments resulting in monetary losses that are greater than or equal to $100 million annually. PIIA and related OMB guidance also contain reporting and corrective action requirements to follow to manage improper payments, as figure 5 illustrates.

Figure 5: Key Federal Requirements for Agencies to Manage Improper Payments



Source: GAO analysis of relevant laws and Office of Management and Budget guidance. | GAO-24-106608

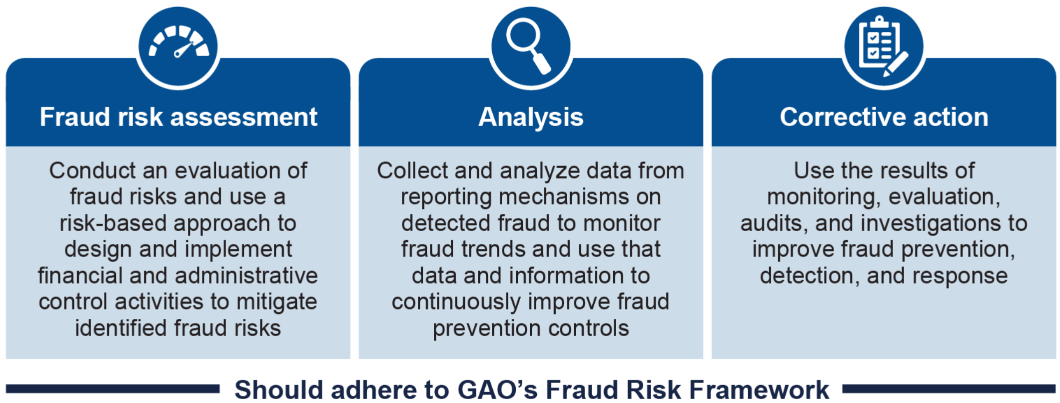
PIIA requires agencies with programs susceptible to significant improper payments to report a description of the causes of the improper payments identified, actions that the agency has planned or taken to address those causes, and the planned or actual completion dates of those actions.

OMB develops guidance for executive branch agencies on estimating and reporting improper payments. OMB Circular A-123 Appendix C, *Requirements for Payment Integrity Improvement* (OMB M-21-19), carries out OMB's responsibility to issue guidance under PIIA. For example, OMB M-21-19 provides guidance to agencies on their responsibilities to monitor and measure the effectiveness and progress of improper payment mitigation strategies and corrective actions.

OMB requires agencies to report their improper payment estimates and categorize them by root cause, which are both reported on www.PaymentAccuracy.gov. This U.S. government website is managed by OMB and provides current and historical improper payment data.

Requirements for managing fraud. PIIA requires OMB to maintain guidelines for agencies to establish financial and administrative controls to identify and assess fraud risks and that incorporate leading practices detailed in our Fraud Risk Framework.[12] The Fraud Risk Framework, discussed in detail later in this report, encompasses control activities to prevent, detect, and respond to fraud. The framework emphasizes prevention and environmental factors that help managers achieve their objective to mitigate fraud risks. OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB M-16-17) directs agencies to adhere to the Fraud Risk Framework's leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses financial and nonfinancial fraud risks. Figure 6 illustrates key federal requirements for agencies to manage fraud risk.

Figure 6: Key Federal Requirements for Agencies to Manage Fraud Risk



Source: GAO analysis of relevant laws and Office of Management and Budget guidance; Icons-Studio/stock.adobe.com (icons). | GAO-24-106608

OMB also published a notification in October 2022 reminding agencies of these requirements and stating that in adherence with PIIA, agencies must establish financial and administrative controls to identify and assess fraud risks.[13] The notification informs agencies that all programs, regardless of their improper payment risks or rates, should strategically manage their fraud risks. The notification further directs agencies to consider both financial and nonfinancial fraud risks, such as individuals obtaining beneficiary payments or personally identifiable information through willful misrepresentation.

Since fiscal year 2017, OMB has directed agencies to provide data on dollars associated with confirmed fraud—cases that have been adjudicated as fraud by a court—on its PaymentAccuracy.gov website. Beyond this directive, agencies are not required to report financial and nonfinancial fraud. Agencies are also not required to report the root causes of the confirmed fraud reported on PaymentAccuracy.gov.

PIIA contained fraud risk management agency reporting requirements for agencies' annual financial reports, but those requirements expired in 2020. In March 2022, we recommended that Congress amend PIIA to reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports.[14] As of October 2023, Congress had not passed legislation reinstating this requirement.

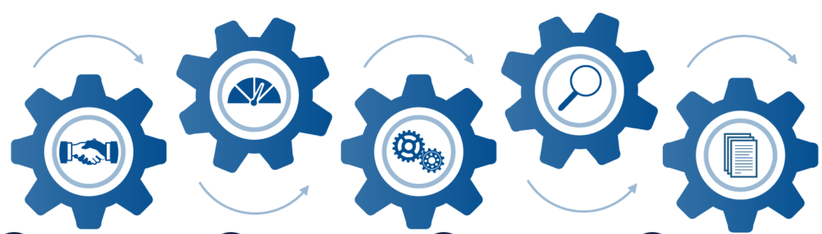
Estimated improper payment amounts cannot be used to determine the extent of fraud in a particular program. Agencies' Inspectors General may report on certain results of investigations but do not uniformly record and report fraud and related data. Similarly, federal programs that report improper payment data do not consistently assess what proportion of those payments were the result of fraud. As we reported in January 2023, an estimate of the amount of fraud across all federal programs does not currently exist because existing data on fraud make it difficult to produce reliable government-wide estimates.[15] We are exploring ways to estimate the amount of fraud that affects the federal government.

What resources does GAO have to help agencies manage improper payments and fraud?

We have developed several resources to help agencies combat improper payments, including those related to fraud. These resources include guidance such as *A Framework for Managing Improper Payments in Emergency Assistance Programs* (Managing Improper Payments Framework) and our Fraud Risk Framework, and the web-based Antifraud Resource. These resources can help agencies better understand and combat the causes and impacts of improper payments and fraud.

Managing Improper Payments Framework. In July 2023, we issued our Managing Improper Payments Framework.[16] This framework includes leading practices to help federal agencies combat improper payments, including those stemming from fraud, in emergency and nonemergency programs before they occur. Agencies should also use this framework with existing requirements related to managing improper payments, including those stemming from fraud. Such requirements include the internal control standards outlined in *Standards for Internal Control in the Federal Government*. Our Managing Improper Payments Framework includes an overall five-step approach, as figure 7 describes.

Figure 7: Framework for Managing Improper Payments in Emergency Assistance Programs



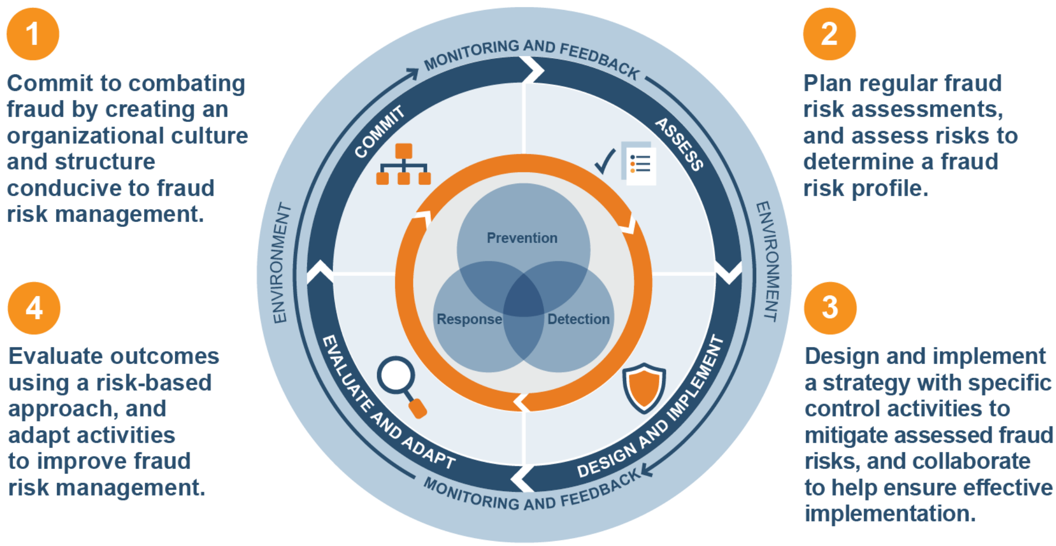
1 Commit to managing improper payments	2 Identify and assess improper payment risks, including fraud	3 Design and implement effective control activities	4 Monitor the effectiveness of controls in managing improper payments	5 Provide and obtain information to manage improper payments
☐ Develop internal control plans in advance to prepare for future emergencies ☐ Identify data-sharing opportunities ☐ Assign clear roles and responsibilities for managing improper payments ☐ Implement open recommendations related to improper payments ☐ Apply lessons learned from past emergencies	☐ Leverage prior risk assessments ☐ Quickly identify and assess new improper payment risks ☐ Support nonfederal entities in assessing and managing improper payment risks ☐ Define risk tolerance ☐ Periodically assess whether programs are susceptible to significant improper payments, including fraud	☐ Establish control activities at the beginning of the program ☐ Leverage existing resources to create controls quickly ☐ Prioritize prepayment controls and avoid overreliance on "pay and chase" controls ☐ Ensure controls align with statutory requirements	☐ Establish timely ongoing monitoring and separate evaluations ☐ Estimate improper payments ☐ Analyze the root cause of improper payments ☐ Monitor nonfederal entities' implementation of emergency assistance programs ☐ Develop corrective actions	☐ Provide improper payment information to nonfederal entities ☐ Provide improper payment information to oversight entities ☐ Obtain and use information from nonfederal entities and state and local auditors

Source: GAO (information and icons). | GAO-24-106608

This approach includes principles that align with leading practices described in our Fraud Risk Framework, such as identifying and assessing fraud risks that cause improper payments. Federal agencies should use the Managing Improper Payments Framework in conjunction with GAO's Fraud Risk Framework's leading practices for combatting fraud and improper payments in a strategic, risk-based manner.

Fraud Risk Framework. GAO's Fraud Risk Framework outlines four key components that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way. As figure 8 illustrates, the four key components of GAO's Fraud Risk Framework are commit, assess, evaluate and adapt, and design and implement.[17]

Figure 8: The Four Components of Our Fraud Risk Framework



Source: GAO (information and icons). | GAO-24-106608

Antifraud resource. In January 2022, we issued our antifraud resource.[18] This online interactive tool can help inform federal officials, Congress, the media, and the public about key characteristics of fraud schemes and provide resources for combating them. The resource includes GAO's Conceptual Fraud Model, which was developed to describe the nature of known fraud, both financial and nonfinancial, that affects federal programs and operations. The primary intended users of GAO's Antifraud Resource are U.S. federal government managers and employees. It may also be applicable to state, local, and foreign government agencies, as well as nonprofit entities and others responsible for fraud risk management. Figure 9 references the online location of this antifraud resource.

Figure 9: Reference to GAO's Antifraud Resource

Source: GAO (information); Production Perig/stock.adobe.com (image). | GAO-24-106608

How can agencies' efforts to combat improper payments support efforts designed to combat fraud?

We have previously reported on features of corrective actions that agencies have taken to reduce improper payment rates, such as establishing accountability, facilitating collaboration, and providing technology, tools, and training (see table 2).[19]

Table 2: Examples of Features of Corrective Actions Agencies Have Taken to Reduce Improper Payments

Establishing accountability	Department of Veterans Affairs's (VA) Veterans Health Administration (VHA) established program-level senior accountable officials to increase accountability and involvement of program offices in reducing improper payments. In addition, VHA established compliance benchmarks for all VHA high-risk programs and set goals for each senior accountable official to meet Payment Integrity Information Act of 2019 (PIIA) compliance by specified dates.
Facilitating collaboration	Health and Human Services (HHS) supported states in establishing mitigation strategies and corrective actions for Child Care and Development Fund (CCDF) improper payments. The CCDF program provides tribal governments, states, and U.S. territories with funding to help low-income families access childcare HHS also promoted collaboration by conducting site visits in states needing assistance to address improper payment root causes.
Providing technology, tools, and training	Federal Communications Commission (FCC) and the Universal Service Administrative Company (USAC), a not-for-profit company administering FCC programs, launched the National Verifier to address program integrity issues. According to the FCC, National Verifier reduces improper payments related to ineligible, deceased, and duplicate subscribers and oversubscribed addresses. National Verifier uses a combination of automated and manual processes to verify eligibility and avoid duplicate enrollments, confirming whether a consumer is qualified for the Lifeline program. In addition, FCC officials stated that the Schools and Libraries program's use of open data and other coding capabilities allowed the FCC to improve its eligibility validation for invoices. USAC also implemented outreach efforts to reduce improper payments and the causes of errors identified during audits and payment quality assurance reviews. These outreach efforts include newsletters and webinars to educate carriers on rules and program requirements.

Source: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-106608

Note: These examples were from GAO, *Improper Payments: Programs Reporting Reductions Had Taken Corrective Actions That Shared Common Features*, GAO-23-106585 (Washington, D.C.: June 30, 2023).

Corrective actions designed to reduce improper payments, such as those described in table 2, can help identify improper payments that are due to errors in providing inaccurate information. These corrective actions can further support existing or future antifraud fraud controls designed specifically to prevent, detect, and respond to fraud, such as those described in table 3. For example, improper payment corrective actions focusing on accountability, collaboration, and tools and training can also help combat fraud-related improper payments.

Table 3: Examples of How Corrective Actions to Reduce Improper Payments Align with Efforts to Combat Fraud

Establishing accountability	Centers for Medicare and Medicaid Services (CMS) created the Center for Program Integrity (CPI), a dedicated and centralized antifraud entity accountable for strategically managing improper payment risks related to fraud in the Medicare and Medicaid programs. This entity is an executive-level office with a direct reporting line to executive-level management at CMS. According to CMS officials, CPI has heightened visibility across CMS and is involved in executive-level conversations.[a]
Facilitating collaboration	U.S. Export and Import Bank of the United States (EXIM) took collaborative steps to develop and implement an antifraud strategy. Its control activities are based on results of a fraud risk assessment and corresponding fraud risk profile. These control activities help mitigate fraud risks impacting EXIM's various loan programs. For instance, EXIM established working groups of internal officials from various divisions to help implement EXIM's antifraud strategy. The working groups did so by assessing the fraud risk within their respective divisions; designing, implementing, and operating an internal control system for their financial programs; and reporting issues related to fraud or compliance objectives in their respective areas.[b]
Providing technology, tools, and training	Federal Communications Commission's (FCC) program administrator, the Universal Service Administrative Company (USAC), established payment recapture audits and an improper payment testing program. Specifically, the program included corrective actions such as technology, guidance, and auditor training to detect and deter improper payments to telecommunication carriers. Improper payments can result from carriers' fraudulent misrepresentation of discounted telecommunication services or goods to schools and libraries.[c]

Source: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-106608

[a]GAO, *Medicare: Actions Needed to Better Manage Fraud Risks*, GAO-18-660T (Washington, D.C.: July 17, 2018).

[b]GAO, *Export-Import Bank: Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts*, GAO-22-105340 (Washington, D.C.: Sept. 27, 2022).

[c]GAO, *Improper Payments*: *Programs Reporting Reductions Had Taken Corrective Actions That Shared Common Features*, GAO-23-106585 (Washington, D.C.: June 30, 2023), and *Telecommunications: FCC Should Take Action to Better Manage Persistent Fraud Risks in the Schools and Libraries Program*, GAO-20-606 (Washington, D.C.: Sept. 16, 2020).

What challenges exist in using data to manage improper payments and fraud?

We have reported many existing challenges that can limit agencies' abilities to use data to manage improper payments and fraud.[20] Such challenges include using and accessing complete and reliable data to prevent and identify fraud-related improper payments, as the examples in table 4 illustrate. We have also made recommendations to agencies and Congress to help address these challenges (see table 4). Implementing these recommendations can help agencies combat the related causes and impacts of fraud-related improper payments.

Table 4: Examples of Challenges Agencies Face in Using Data to Manage Fraud-Related Improper Payments and GAO's Recommendations to Address Them

Incomplete or unreliable data	Some agencies work with incomplete or unreliable data when managing fraud-related improper payments. For example, we reported in 2018 that the Department of Defense (DOD) needs to take steps to collaborate with its component agencies to improve the reliability and completeness of the data obtained on all foreign military payments. Doing so would help ensure that no fraud-related improper payments were made to civilian personnel conducting oversight of DOD contracts. We made recommendations to address this issue. DOD agreed with these recommendations, but had not yet implemented them as of October 2023.[a] We also recommended in 2023 that the Department of Housing and Urban Development (HUD) develop guidance for state and local entities that receive HUD's disaster recovery grants to collect complete and consistent data to better support applicant eligibility determinations and fraud risk management. HUD agreed with this recommendation, but had not yet implemented it as of October 2023.[b]
Not leveraging available data	Some agencies do not use existing data that could help validate payment eligibility and compliance. For example, we recommended in 2018 that the Internal Revenue Service (IRS) take steps to assess the benefits and costs of using available wage data to identify potential fraud-related improper tax refunds before sending the refunds to recipients. We reported that using such data could help IRS identify the underreporting of wages, employment fraud, and other noncompliance before issuing refunds. IRS has taken some steps that partially respond to this recommendation, but, as of October 2023, it had not yet taken the additional steps needed to fully implement this recommendation.[c]
Data sharing limitations	Legal requirements can inhibit sharing of key personally identifiable information data with some agencies that could help identify fraud-related improper payments. For example, we reported earlier in 2023 that the Small Business Administration (SBA) faces statutory obstacles that prevent the Social Security Administration from sharing key data, including Social Security numbers, with SBA. These data could help SBA effectively detect and prevent fraud-related improper payments in SBA's pandemic-relief programs, consistent with leading practices in our fraud risk framework. We recommended that SBA develop a plan for obtaining access to those external sources of data, which might involve pursuing statutory authority or entering into a data-sharing agreement to obtain such access. SBA agreed with this recommendation, but had not yet implemented it as of October 2023.[d]
Limited access to data and data capabilities	Limitations on data access and data capabilities can constrain agencies' oversight capabilities and resources. For example, most of the 24 Chief Financial Officers Act of 1990 agencies that we surveyed in 2023 reported challenges with accessing relevant data. They also reported limited staff, tools, and funding to support data analytical capabilities, impeding efforts to identify or prevent fraud-related improper payments.[e] We also reported in 2022 that many agencies face limited access to data on deceased individuals that the Social Security Administration (SSA) is currently required to share in Treasury's Do Not Pay (DNP) system for 3 years. The DNP system is a data matching service for agencies to use in preventing fraud-related improper payments, including those to deceased individuals. As result, we recommended that Congress accelerate and make permanent this existing requirement.[f] Treasury officials have informed us that by the end of this calendar year, the Do Not Pay working system should have full access to the full death data. However, under current law, that access will end in 2026. As of October 2023, Congress had not yet taken action on this recommendation.

Source: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-106608

[a]GAO, *Foreign Military Sales: Financial Oversight of the Use of Overhead Funds Needs Strengthening,* GAO-18-553 (Washington, D.C.: July 30, 2018).

[b]GAO, *Disaster Recovery: HUD Should Develop Data Collection Guidance to Support Analysis of Block Grant Fraud Risks,* GAO-23-104382 (Washington, D.C.: Aug. 17, 2023).

[c]GAO, *Tax Fraud and Noncompliance: IRS Can Strengthen Pre-refund Verification and Explore More Uses,* GAO-18-224 (Washington, D.C.: Jan. 30, 2018).

[d]GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs,* GAO-23-105331 (Washington, D.C.: May 18, 2023).

[e]GAO, *Fraud Risk Management: Information on Agencies' Current Status*, GAO-24-106565 (Washington, D.C.: Nov. 1, 2023).

[f]GAO, *Emergency Relief Funds: Significant Improvements Are Needed to Ensure Transparency and Accountability for COVID-19 and Beyond*, GAO-22-105715 (Washington, D.C.: Mar. 17, 2022).

Since 2015, we have made over 40 recommendations for agencies to use data analytical capabilities to help manage fraud risk, such as to verify self-reported data and identify fraud-related improper payments. More than half of these recommendations had not been fully implemented as of August 2023.[21]

How GAO Did This Study

We reviewed relevant federal statutes, standards, and guidance that focused on management of, or distinctions and relationships between, improper payments and fraud. We also conducted a literature review of relevant GAO products and other federal reports that focused on these issues and that were issued since we published our Fraud Risk Framework in 2015.

The distinctions and relationships between improper payments and fraud that we describe in this report are not intended to be an exhaustive list. Similarly, examples of federal requirements, standards, and guidance described in this report are not intended to present a comprehensive, detailed analysis of all improper payment and fraud risk management requirements, standards, or guidance that may exist.

We conducted this performance audit from January 2023 to December 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

List of Addressees

The Honorable Mark E. Amodei
Chairman
The Honorable Adriano Espaillat
Ranking Member
Subcommittee on Legislative Branch
Committee on Appropriations
House of Representatives

We are sending copies of this report to the appropriate congressional committees. We are also sending informational copies to OMB, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

GAO Contact Information

For more information, contact: Rebecca Shea, Director, Forensic Audits and Investigative Service, at (202) 512-6722 or SheaR@gao.gov.

Chuck Young, Managing Director, Public Affairs, YoungC1@gao.gov, (202) 512-4800.

A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400.

Staff Acknowledgments: Gabrielle Fagan (Assistant Director), Flavio Martinez (Analyst in Charge), Daniel Silva (Senior Auditor), Jim Ashley, Leia Dickerson, Colin Fallon, Daniel Flavin, Jason Kirwan, Barbara Lewis, Maria McMullen, James Murphy, Hannah Padilla, Amanda Stogsdill, and Matthew Valenta made key contributions to this report.

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.

Visit GAO on the web at https://www.gao.gov.

Endnotes

[1]Improper payments are any payments that should not have been made or that were made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. Improper payments include any payment to an ineligible recipient or ineligible service, duplicate payments, payments for services not received (except where authorized by law), and any payment for an incorrect amount. 31 U.S.C. § 3351(4). Executive agency estimates of improper payments also treat as improper any payments whose propriety cannot be determined due to lacking or insufficient information. 31 U.S.C. § 3352(c)(2).

[2]GAO, *Improper Payments: Fiscal Year 2022 Estimates and Opportunities for Improvement*, GAO-23-106285 (Washington, D.C.: Mar. 29, 2023); *Improper Payments: Programs Reporting Reductions Had Taken Corrective Actions That Shared Common Features*, GAO-23-106585 (Washington, D.C.: June 30, 2023); and *Improper Payments: Opportunities for Interagency Collaboration and Improvements*, GAO-23-106761 (Washington, D.C.: Sept. 28, 2023).

[3]GAO, *Defense Procurement*: *Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership,* GAO-20-106 (Washington, D.C.: Nov. 25, 2019).

[4]GAO, *Aviation: FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration*, GAO-20-164 (Washington, D.C.: Mar. 25, 2020).

[5]Office of Management and Budget, *Requirements for Payment Integrity Improvement*, *Circular No. A-123, Appendix C,* OMB-M-21-19 (Washington, D.C.: Mar. 5, 2021).

[6]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014); *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015); and *Medicare and Medicaid*: *CMS Needs to Fully Align Its Antifraud Efforts with the Fraud Risk Framework*, GAO-18-88 (Washington, D.C.: Dec. 5, 2017).

[7]GAO, *Federal Student Loans: Education Needs to Verify Borrowers' Information for Income-Driven Repayment Plans*, GAO-19-347 (Washington, D.C.: June 25, 2019); *Fake Caller ID Schemes: Information on Federal Agencies' Efforts to Enforce Laws, Educate the Public, and Support Technical Initiatives,* GAO-20-153 (Washington, D.C.: Dec. 18, 2019); *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO-21-288 (Washington, D.C.: Mar. 24, 2021); and *DOD Fraud Risk Management: Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks,* GAO-21-309 (Washington, D.C.: Aug. 19, 2021).

[8]GAO, *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response*, GAO-22-105051 (Washington, D.C.: Oct. 27, 2021).

[9]Pub. L. No. 116-117, 134 Stat. 113 (2020) (codified at 31 U.S.C. §§ 3351-58).

[10]31 U.S.C. § 3352(a)(1)(B).

[11]31 U.S.C. § 3352(b)(2).

[12]31 U.S.C. § 3357(b). The Fraud Reduction and Data Analytics Act of 2015 (FRDAA) originally required OMB to establish these guidelines for agencies in 2016. Pub. L. No. 114-186, 130 Stat. 546 (2016). FRDAA was repealed and replaced by PIIA in 2020.

[13]Office of Management and Budget, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk,* CA-23-03 (Washington, D.C.: Oct. 17, 2022).

[14]GAO, *Emergency Relief Funds: Significant Improvements Are Needed to Ensure Transparency and Accountability for COVID-19 and Beyond,* GAO-22-105715 (Washington, D.C.: Mar. 17, 2022).

[15]GAO, *Fraud in the Federal Government: Challenges Determining the Extent of Federal Fraud,* GAO-23-106110 (Washington, D.C.: Jan. 23, 2023).

[16]GAO, *A Framework for Managing Improper Payments in Emergency Assistance Programs*, GAO-23-105876 (Washington, D.C.: July 13, 2023).

[17]GAO-15-593SP.

[18]GAO, "The GAO Antifraud Resource," (Washington, D.C.: Jan. 10, 2022), accessed Sept. 6, 2023, https://gaoinnovations.gov/antifraud_resource/.

[19]GAO, *Improper Payments: Programs Reporting Reductions Had Taken Corrective Actions That Shared Common Features*, GAO-23-106585 (Washington, D.C.: June 30, 2023).

[20]GAO, *Foreign Military Sales: Financial Oversight of the Use of Overhead Funds Needs Strengthening,* GAO-18-553 (Washington, D.C.: July 30, 2018); *Disaster Recovery: HUD Should Develop Data Collection Guidance to Support Analysis of Block Grant Fraud Risks,* GAO-23-104382 (Washington, D.C.: Aug. 17, 2023); *Tax Fraud and Noncompliance: IRS Can Strengthen Pre-refund Verification and Explore More Uses,* GAO-18-224 (Washington, D.C.: Jan. 30, 2018); *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs,* GAO-23-105331 (Washington, D.C.: May 18, 2023); *Fraud Risk Management: Information on Agencies' Current Status*, GAO-24-106565 (Washington, D.C.: Nov. 1, 2023); and *Emergency Relief Funds: Significant Improvements Are Needed to Ensure Transparency and Accountability for COVID-19 and Beyond*, GAO-22-105715 (Washington, D.C.: Mar. 17, 2022).

[21]GAO, *Fraud Risk Management: Information on Agencies' Current Status*, GAO-24-106565 (Washington, D.C.: Nov. 1, 2023).