United States Government Accountability Office

Testimony

Before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

COVID-19

Insights and Actions for Fraud Prevention

Accessible Version

Statement of Rebecca Shea,
Director, Forensic Audits and Investigative Service

For Release on Delivery Expected at 2:45 p.m. ET
Tuesday, November 14, 2023

GAO Highlights

Highlights of GAO-24-107157, a testimony before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

November 14, 2023

COVID-19

Insights and Actions for Fraud Prevention

Why GAO Did This Study

Since March 2020, Congress and the administration have provided trillions of dollars in COVID-19 relief funding to help the nation respond to, and recover from, the pandemic. Agencies across the federal government acted quickly to stand up new programs and greatly scale up existing programs.

While COVID-19 relief programs were critical for assuring public health and economic stability, they also created unprecedented opportunities for fraud due to the dollars involved and other risk factors. While the full extent of fraud associated with the COVID-19 relief funds will never be known with certainty, estimates are in the hundreds of billions. In light of what was likely lost to fraud during the pandemic, the importance of fraud prevention cannot be stressed enough.

This testimony discusses (1) insights for prevention from COVID-19 fraud; and (2) recommendations, matters, and resources for improving fraud prevention in normal operations and future emergencies.

GAO reviewed its prior COVID-19 findings and recommendations on internal controls and fraud risk management practices.

What GAO Recommends

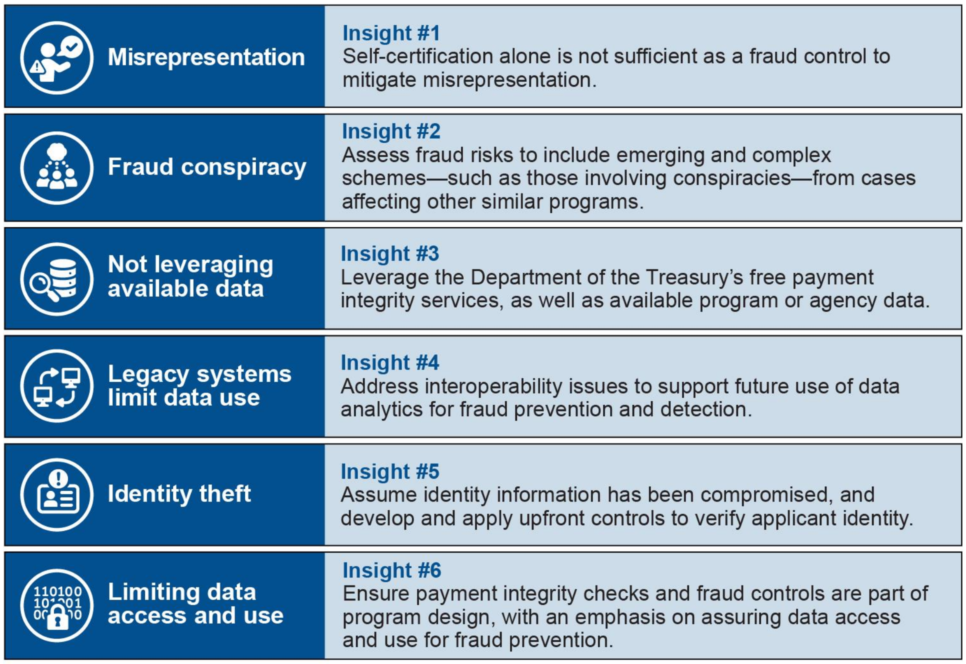
As of August 2023, agencies needed to take additional action to fully address 95 GAO recommendations to help ensure they are effectively managing fraud risks. Additionally, in March 2022, GAO identified 10 actions Congress could take to strengthen internal controls and financial and fraud risk management practices across the government. All 10 remain open.

View GAO-24-107157. For more information, contact Rebecca Shea at (202) 512-6722 or shear@gao.gov.

What GAO Found

Challenges that agencies faced in implementing COVID-19 relief programs provide insights into fraud prevention for normal operations and future emergencies. Specifically, understanding fraud schemes that emerged during the pandemic can provide opportunities for program managers to identify internal controls that had been circumvented and respond to mitigate the related risks. Data and system challenges, such as limited data sharing, highlight the value of data analytics for fraud prevention. Additionally, thoughtful program design choices that consider fraud vulnerabilities can facilitate fraud prevention.

Insights from COVID-19 Relief to Inform Fraud Prevention



Misrepresentation	**Insight #1** Self-certification alone is not sufficient as a fraud control to mitigate misrepresentation.
Fraud conspiracy	**Insight #2** Assess fraud risks to include emerging and complex schemes—such as those involving conspiracies—from cases affecting other similar programs.
Not leveraging available data	**Insight #3** Leverage the Department of the Treasury's free payment integrity services, as well as available program or agency data.
Legacy systems limit data use	**Insight #4** Address interoperability issues to support future use of data analytics for fraud prevention and detection.
Identity theft	**Insight #5** Assume identity information has been compromised, and develop and apply upfront controls to verify applicant identity.
Limiting data access and use	**Insight #6** Ensure payment integrity checks and fraud controls are part of program design, with an emphasis on assuring data access and use for fraud prevention.

Sources: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-107157

Accessible Data for Insights from COVID-19 Relief to Inform Fraud Prevention

Category	Category information
Misrepresentation	Insight #1 Self-certification alone is not sufficient as a fraud control to mitigate misrepresentation.
Conspiracy	Insight #2 Assess fraud risks to include emerging and complex schemes—such as those involving conspiracies—from cases affecting other similar programs.
Not leveraging available data	Insight #3 Leverage the Department of the Treasury's free payment integrity services, as well as available program or agency data.
Legacy systems limit data use	Insight #4 Address interoperability issues to support future use of data analytics for fraud prevention and detection.

Category	Category information
Identity theft	Insight #5 Assume identity information has been compromised, and develop and apply upfront controls to verify applicant identity.
Limiting data access and use	Insight #6 Ensure payment integrity checks and fraud controls are part of program design, with an emphasis on assuring data access and use for fraud prevention.

Sources: GAO (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-107157

With strategic fraud risk management, agencies are better positioned to manage fraud during normal operations and emergencies. Sources that provide additional insight for fraud prevention include recommendations GAO has made to agencies, actions GAO identified that Congress can take to strengthen fraud risk management practices across the government, and resources GAO developed to support strategic fraud risk management. Implementing these recommendations and taking these actions, along with leveraging available resources, can enable agencies to carry out their missions and better protect taxpayer dollars from fraud during normal operations and prepare them to face the next emergency.

An Insight Based on GAO Resources and Recommendations to Agencies and Congress

Actions and resources

Insight #7
Take actions to better prevent fraud by implementing GAO recommendations and using resources.

Source: GAO (information); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

Accessible Data for An Insight Based on GAO Resources and Recommendations to Agencies and Congress

Category	Category information
Actions and resources	Insight #7 Take actions to better prevent fraud by implementing GAO recommendations and using resources.

Source: GAO (information); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

Chair Hassan, Ranking Member Romney, and Members of the Subcommittee:

I appreciate the opportunity to discuss insights into fraud prevention based on challenges that agencies faced in implementing COVID-19 relief programs, as well as what can be done to help prevent fraud in the future.

Since March 2020, Congress and the administration have provided trillions in COVID-19 relief funding to help the nation respond to and recover from the pandemic. Agencies across the federal government acted quickly to stand up new programs and greatly scale up existing programs. Federal COVID-19 relief funds were distributed broadly to tribal, state, local, and territorial governments; businesses; and individuals to combat the effects of the pandemic on the public health system, as well as the economy.

Most of these funds went to the intended recipients in the intended amounts, providing needed assistance. For example, COVID-19 relief funds provided needed assistance to unemployed workers and small businesses. Timely payments from the Department of Labor's (DOL) unemployment insurance (UI) programs allowed unemployed workers to address financial hardships, such as inability to pay for rent, utilities, and groceries. The Small Business Administration's (SBA) Paycheck Protection Program (PPP) and COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program helped small businesses cover eligible operating costs, such as payroll and rent, during the pandemic. COVID-19 relief funding also helped support COVID-19 testing; surveillance; and contact tracing, among other uses.

While COVID-19 relief programs were critical for assuring public health and economic stability, they also created unprecedented opportunities for fraud due to the amount of dollars involved and other risk factors. Because not all fraud will be identified, investigated, and adjudicated through judicial or other systems, the full extent of fraud associated with the COVID-19 relief funds will never be known with certainty.

Despite this, some estimates of fraud in COVID-19 relief programs exist. For instance, in September 2023, we estimated that the fraud in DOL's UI programs during the pandemic—from April 2020 through May 2023—was likely between $100 billion and $135 billion.[1] The SBA Office of Inspector General (OIG) estimated that as of June 2023, SBA had disbursed over $200 billion (approximately 17 percent of SBA's total COVID-19 spending) in potentially fraudulent pandemic relief loans.[2]

In light of what was likely lost to fraud during the pandemic, the importance of fraud prevention cannot be stressed enough. To provide insight into actions to promote fraud prevention, in a report being released today, we have highlighted a wide variety of COVID-19 relief program fraud schemes.[3] These schemes illustrate various risk factors, impacts, and mechanisms used to commit fraud. Insights from these schemes, along with our other reviews of pandemic program delivery, have led GAO to make numerous recommendations and matters for congressional consideration; and to develop resources for improving fraud prevention and payment integrity.

My comments today summarize key findings from our report on COVID-19 fraud schemes and other reports examining fraud in COVID-19 relief programs as well as our recent report on the status of agencies' fraud risk management.[4] Specifically, I will discuss the following:

1. insights from COVID-19 fraud that can be used to inform prevention efforts; and
2. prior GAO recommendations to agencies, matters for congressional consideration, and resources for improving fraud prevention in normal operations and future emergencies.

In preparing this testimony, we reviewed findings from our prior work on internal controls and fraud risk management practices in COVID-19 relief programs. Given the government-wide scope of this work, we undertook a variety of methodologies. These methodologies include examining federal laws and agency documents, guidance, processes, and procedures. We

[1] GAO, *Unemployment Insurance: Estimated Amount of Fraud during Pandemic Likely Between $100 Billion and $135 Billion,* GAO-23-106696 (Washington, D.C.: Sept. 12, 2023).

[2] This includes PPP loans, COVID-19 EIDL program loans, EIDL Targeted Advances, and EIDL Supplemental Targeted Advances. Small Business Administration Office of Inspector General, *COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape*, White Paper Report 23-09 (June 27, 2023).

[3] GAO, *COVID-19: Insights from Fraud Schemes and Federal Response Efforts*, GAO-24-106353 (Washington, D.C.: Nov. 14, 2023).

[4] GAO, *Fraud Risk Management: Agencies Should Continue Efforts to Implement Leading Practices*, GAO-24-106565 (Washington, D.C.: Nov. 1, 2023).

also reviewed public statements from the Department of Justice (DOJ) from March 2020 through June 2023 and corresponding court documentation, to identify and describe federal fraud-related cases.[5] More detailed information about the objectives and methodologies on which this statement is based can be found in the individual reports cited throughout this statement.

We conducted the work on which this statement is based 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.

Insights from COVID-19 Relief to Inform Fraud Prevention

Challenges that agencies faced in implementing COVID-19 relief programs provide insights into fraud prevention for normal operations and future emergencies. However, before discussing the specific challenges faced and the insights to be gained from the COVID-19 relief programs, it is important to recognize the nature of fraud and the heightened risks these programs were facing. With that context, understanding fraud schemes that emerged during the pandemic can provide opportunities for program managers to identify internal controls that are needed or were circumvented, and respond to mitigate the related risks. Also, data and system challenges, such as limited data sharing, highlight the value of data analytics for fraud prevention. Additionally, thoughtful program design choices that consider fraud vulnerabilities upfront can facilitate fraud prevention.

[5] These statements from DOJ sometimes announce cases in the later stages of prosecution. For example, an individual's guilty plea may be announced without an earlier public statement announcing the charges being brought. If those charges were brought from March 2020 through June 2023 but the guilty plea was announced in August 2023, that case would not be included in the scope of our review, since the public statement was made after June 2023. See GAO-24-106353.

Five Principles and Risk Factors for Fraud

Fraud is inevitable where there are opportunities for gain—whether in normal operations or emergencies. (See sidebar for five key principles of fraud and corruption.) Across COVID-19 relief programs, factors associated with heightened risk of fraud, waste, abuse, and other payment integrity issues included[6]

Five Principles of Fraud and Corruption

- **There is always going to be fraud.** It is a fact that some individuals will look to gain where there is opportunity. Organizations need robust processes in place to prevent, detect, and respond to fraud and corruption.
- **Finding fraud is a good thing.** If you do not find fraud, you cannot fight it. This requires a change in perspective so the identification of fraud is viewed as a positive and proactive achievement.
- **There is no one solution.** Addressing fraud needs a holistic response incorporating detection, prevention, and response, underpinned by a strong understanding of risk. It also requires cooperation and collaboration between organizations.
- **Fraud and corruption are ever changing.** Fraud and counter fraud practices evolve very quickly, and organizations must be agile and change their approach to deal with these evolutions.
- **Prevention is the most effective way to address fraud and corruption.** Preventing fraud reduces financial loss and reputational damage. It also requires fewer resources than an approach focused on detection and recovery.

Source: International Public Sector Fraud Forum, *Guide to Managing Fraud for Public Bodies.* | GAO-24-107157

- programs that were new to the agency;

[6] Payment integrity includes efforts to minimize all types of improper payments—payments that should not have been made or were made in the incorrect amount—whether from mismanagement, errors, abuse, or fraud. While all payments resulting from fraudulent activity are considered improper, not all improper payments are the result of fraud. Fraud involves obtaining something 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.

- expansions or major changes in program funding, authorities, practices, or procedures;
- a large volume of payments being made;
- payment or eligibility decisions made outside of the agency, such as those by state governments;
- limitations in the experience or training of those making eligibility determinations or payment certifications; and
- challenges related to eligibility and identity, such as lack of information or data systems to confirm eligibility and reliance on self-certification.

New or expanded programs. Congress created new programs or greatly expanded existing programs in response to the COVID-19 pandemic to quickly deliver needed funds.

These included (1) a temporary UI program—Pandemic Unemployment Assistance—which expanded eligibility for unemployment benefits; (2) PPP, the COVID-19 EIDL program, the Restaurant Revitalization Fund, and the Shuttered Venue Operators Grant to assist small businesses; and (3) economic impact payments (EIP) for taxpayer assistance, among others.

Large volume. COVID-19 relief programs experienced a large volume of activity. For example, as the nation experienced historic levels of job loss, the UI programs faced a large volume of claims. PPP and COVID-19 EIDL loans far exceeded SBA's prepandemic lending volume.

Payment decisions made outside of federal agencies. External entities or agencies made eligibility and payment decisions in many COVID-19 relief programs. For example, state agencies administered UI and federal child nutrition programs; lenders were responsible for PPP loan determinations; and internet service providers offered discounts for broadband access to low-income households, among others.[7]

Inexperienced staff. Having new and inexperienced staff was a risk factor for COVID-19 relief programs. For example, in June 2022, we reported that DOL officials cited new and inexperienced staff as one of

[7] GAO, *Affordable Broadband: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management*, GAO-23-105399 (Washington, D.C.: Jan. 18, 2023).

the factors that provided opportunities for exploitation on UI programs and system vulnerabilities.[8]

Eligibility or identity challenges. Several COVID-19 relief programs did not use data systems to confirm eligibility, while some were prohibited from doing so. Many programs relied on self-certification to make identity and eligibility determinations. For example, SBA officials told us the CARES Act's restriction on obtaining applicants' tax returns for the COVID-19 EIDL program presented a challenge for validating applications. Therefore SBA relied on self-certification.[9]

Considering the inevitability of fraud, identifying it is important, but prevention is ideal, particularly where programs face multiple risk factors, and losses may be significant. Prevention is the hallmark of GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), which agencies should have been adhering to since 2016.[10] However, federal agencies did not strategically manage fraud risks in alignment with the Fraud Risk Framework and were not adequately prepared to prevent fraud when the pandemic began.

Insights from Fraud Schemes

Managing fraud risk is the responsibility of program managers. This responsibility includes assessing the potential for fraud and implementing strategies to appropriately mitigate related risks. Using information from emerging fraud schemes can support ongoing fraud risk management efforts.

Program managers can use the details of existing fraud schemes identified in their programs—including information on the impact of these schemes—to help identify program vulnerabilities. Moreover, program managers can leverage details on fraud schemes and their corresponding impacts to evaluate and adapt fraud risk management activities in

[8] GAO, *Unemployment Insurance: Transformation Needed to Address Program Design, Infrastructure, and Integrity Risks*, GAO-22-105162 (Washington, D.C.: June 7, 2022).

[9] GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs*, GAO-23-105331 (Washington, D.C.: May 18, 2023). The Consolidated Appropriations Act, 2021, enacted on December 27, 2020, removed this restriction.

[10] GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

alignment with leading practices outlined in GAO's Fraud Risk Framework.

Three components in the Fraud Risk Framework include the following leading practices related to using past schemes and related information to help combat fraud:

- The *assess* component directs program managers to consider the financial and nonfinancial impacts of fraud risks and identify specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities.
- The *design and implement* component directs agencies to analyze information on previously detected fraud and consider known or previously encountered fraud schemes to design data analytics.
- The *evaluate and adapt* component directs agencies to collect and analyze data, including data from reporting mechanisms and instances of detected fraud.

At least 1,399 individuals or entities were found guilty or liable in fraud-related cases involving federal COVID-19 relief programs, based on our analysis of DOJ's public statements and court documentation from March 2020 through June 2023.[11] In addition to those individuals and entities found guilty or liable, there were also federal fraud-related charges pending against at least 599 other individuals or entities involving federal COVID-19 relief programs, as of June 30, 2023.[12] The number of individuals or entities facing fraud-related charges related to COVID-19 relief programs has grown since March 2020 and will likely continue to increase, as these cases take time to develop.

Fraud schemes are achieved through various mechanisms. A mechanism is a process, technique, or system used by fraudsters to execute fraudulent activities. Mechanisms include misrepresentation, cybercrime,

[11] The federal government may enforce laws through civil or criminal action. Such action may be resolved through a trial, a permanent injunction, a civil settlement, or a guilty plea. Our analysis is limited to the cases we identified from public sources and may not include all criminal and civil cases charged by DOJ as of June 30, 2023. Additionally, details of fraud cases and schemes presented in court documents may not be complete. Further, cases that reach the prosecution stage in the fraud identification life cycle represent a fraction of the instances of fraud or all possible fraud cases. See GAO-24-106353.

[12] A charge is merely an allegation, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

and document falsification. A mechanism can be an individual action or a group of actions working in concert. Fraud schemes result in financial loss and impacts on taxpayers; agency reputation and integrity; federal program goals; and other areas, such as public health and safety. During the pandemic, fraud schemes involved fairly simple mechanisms, as well as complex schemes and mechanisms involving organized groups and international crime rings.

Misrepresentation. Fraud schemes involve a false statement of a material fact made by one party that affects another party's decisions, such as by misrepresenting identity and eligibility.

Insight #1: Self-certification alone is not sufficient as a fraud control to mitigate misrepresentation.

Source: GAO (analysis); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

Simple fraud schemes circumvented key controls. Many COVID-19 relief program fraud schemes relied on fairly simple misrepresentation mechanisms. These included document manipulation, false declarations, and fictitious entities. These types of schemes and mechanisms leave agencies open to significant fraud risk when they rely on self-certification of eligibility or identity as an internal control for fraud prevention.

We found that federal and state agencies, in an effort to disburse funds quickly to those in need, relied on self-attestation or self-certification for individuals to verify their eligibility or identity to receive assistance from some COVID-19 relief programs. Even if program design decisions allowed for self-certification (as discussed in greater detail below), agencies are responsible for designing and implementing control activities to prevent fraud. Self-certification alone is not sufficient as a fraud control (see sidebar).

Our prior work examining PPP and COVID-19 EIDL fraud schemes identified (1) ineligible, nonoperating businesses that applied for and obtained program funds; (2) legitimate businesses owners misrepresenting eligibility regarding their criminal record, federal debt, or principal place of residence, among others; and (3) falsification of tax or other documents to obtain more funds.[13] In these instances, recipients

[13] GAO-23-105331.

falsely self-certified eligibility. Other fraud controls to mitigate these misrepresentations were either not in place or were not effective.

Confirming eligibility of individuals receiving benefits, such as by confirming wage information or by verifying identity through data and other checks, are key controls to prevent fraud schemes that rely on mechanisms such as misrepresentation.

Fraud conspiracy. Involves an agreement by two or more individuals to commit a crime, such as via collusion between a small group of individuals or larger scale fraud rings.

Insight #2: Assess fraud risks to include emerging and complex schemes—such as those involving conspiracies—from cases affecting other similar programs.

Source: GAO (analysis); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

Complex fraud schemes also emerged during the pandemic. Other COVID-19 relief program fraud schemes relied on more complex mechanisms, such as conspiracies involving organized groups or international criminal gangs. Such cases, including those involving international fraud schemes, continue to emerge, in part because of the time needed to obtain information from foreign jurisdictions. If agencies are not prepared to combat simple fraud schemes, they will not be prepared for emerging complex fraud schemes. As part of assessing their own fraud risks, agencies can gain insights from examining emerging and complex schemes that affected other similar programs such as those with similar mission activities (see sidebar).

Conspiracy. We have previously reported on schemes involving conspiracies to defraud COVID-19 relief programs. For example, four individuals associated with a nonprofit organization pleaded guilty to their roles in a complex scheme to defraud a federal child nutrition program. Nearly 50 individuals are alleged to have engaged in this scheme. The ringleaders of the scheme operated a nonprofit organization. Other individuals—recruited by the nonprofit to participate in the scheme—set up sham program delivery sites to fraudulently claim reimbursements for meal delivery. The nonprofit received more than $18 million in administrative fees to which it was not entitled and, after claiming to open more than 250 sites, it fraudulently obtained and disbursed more than $240 million in program funds that the fraudsters used for their own financial benefit instead of using the funds as intended to feed underserved children during the pandemic.[14]

International schemes. U.S. law enforcement officials have been analyzing and investigating instances of fraud involving foreign actors. For example, SBA OIG analyzed internet protocol (IP) addresses that were used to apply for COVID-19 EIDL funds. SBA disbursed 41,638 COVID-19 EIDL loans and grants to applicants with foreign IP addresses, totaling $1.3 billion. Applications were processed by applicants with IP addresses from Nigeria, Pakistan, Canada, Mexico, United Kingdom, Philippines, Dominican Republic, India, and Germany.[15]

Early in the pandemic, DOL's OIG worked with DOJ to create the National UI Fraud Task Force, a nine-agency federal task force that worked closely with the International Organized Crime Intelligence and Operations Center (IOC-2). Through data analytics and a leads generation process, the National UI Fraud Task Force and IOC-2 partner agencies have identified significant fraud being committed against the UI program by domestic and international criminal organizations. Many of these include street-level criminal organizations with ties to illegal guns and drugs.

Insights from Data and IT System Challenges

Integrated, functional, and secure data and systems are essential for effective fraud risk management. Agencies' responses to the pandemic revealed challenges in leveraging available data, legacy IT systems that were unable to facilitate fraud detection and recovery, and data breaches that facilitated identity fraud.

[14] GAO-24-106353.

[15] Small Business Administration Office of Inspector General, *COVID-19 Economic Injury Disaster Loan Applications Submitted from Foreign IP Addresses*, Report 22-17 (Sept. 12, 2022).

Not leveraging available data. Challenges included not using existing data that could help validate payment eligibility.

Insight #3: Leverage the Department of the Treasury's free payment integrity services as well as available program or agency data.

Source: GAO (analysis); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

Available data. According to the Fraud Risk Framework, a leading practice in fraud data analytics is to conduct data mining and matching. This includes cross-checking of data and using external data sources to validate information, to identify suspicious activities. There are various sources of data available for agencies to use. For example, agencies have access to free payment integrity services provided by the Department of the Treasury.[16] Agencies can also leverage their own program or agency data. However, these data sources are not always fully leveraged (see sidebar).

Internal and external data sharing posed challenges in the administration of COVID-19 relief programs. For example, in May 2023, we determined that, across its programs, SBA did not fully leverage information to help prevent fraud and identify applicants who tried to defraud more than one program. We also found that while SBA obtained access to some government databases, such as the Department of the Treasury's Do Not Pay service, that was after most of the PPP and COVID-19 EIDL funds were disbursed. Also, it did not have access to some other external data sources that could benefit its efforts to detect and prevent fraud. We recommended that SBA ensure that it has mechanisms in place and use them to facilitate cross-program data analytics. We also recommended that SBA identify external sources of data that can facilitate the verification of applicant information and the detection of potential fraud across its programs.[17]

[16] Treasury's Do Not Pay service is an analytics tool that helps federal agencies detect and prevent improper payments made to vendors, grantees, loan recipients, and beneficiaries. Agencies can use the service to check multiple data sources to make payment eligibility decisions.

[17] GAO-23-105331. As of November 7, 2023, SBA has not yet provided us with information on the status of its efforts to implement these recommendations.

Legacy systems limit data use. Challenges included outdated IT systems that constrained capabilities for fraud prevention and detection.

Insight #4: Address interoperability issues to support future use of data analytics for fraud prevention and detection.

Source: GAO (analysis); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

Legacy systems. During the pandemic, due to outdated IT systems, agencies experienced challenges in detecting and recovering improper payments, including from fraud. Addressing interoperability issues can support future use of data analytics for fraud prevention and detection (see sidebar).

A May 2021 DOL OIG report identified legacy IT systems as one of the causes of states' inability to detect and recover improper UI payments, including fraudulent payments.[18] Additionally, in our June 2022 report, state officials reported that their IT systems did not have the capability to perform cross-matches—a method used to detect improper payments—for such a large volume of claims.[19]

Further, in June 2022, we reported that legacy systems may operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address.[20] In the UI programs, this may pose a privacy risk for claimants as their PII could become more easily accessible to criminals who target UI. The increased amount of benefits awarded and legacy IT systems' inability to adequately guard citizens' sensitive information gave criminals incentive and opportunities to commit fraud.

Legacy IT systems made it difficult for many states to prevent cybersecurity attacks or the use of fraudulently obtained identity information, according to DOL OIG officials. These officials stated that some state IT systems were not equipped to handle the volume of claims, and some may not have been easily compatible with the National

[18] Department of Labor, Office of Inspector General, *COVID-19: States Struggled to Implement CARES Act Unemployment Insurance Programs*, Report No. 19-21-004-03-315 (Washington, D.C.: May 28, 2021).

[19] GAO-22-105162.

[20] GAO-22-105162.

Association of State Workforce Agencies UI Integrity Center's Integrity Data Hub resources.[21] However, since the onset of the pandemic, many states have begun using Integrity Data Hub resources, according to DOL officials. For example, as of October 2022, we reported that there were 41 states using the Integrity Data Hub's identity verification service, according to DOL officials.[22] According to the DOL OIG, as of February 2023, 53 states had a participation agreement to use the Integrity Data Hub.[23] However, the DOL OIG also noted that the existence of a participation agreement does not provide information on whether participants are using these resources or the frequency in which they use.

Identity theft. Fraud schemes involve stealing personally identifiable information to fraudulently apply for benefits.

Insight #5: Assume identity information has been compromised, and develop and apply upfront controls to verify applicant identity.

Source: GAO (analysis); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

Data breaches. Stolen personally identifiable information (PII) played a role in large-scale identity fraud during the pandemic. Given the scale of this fraud and known data breaches involving PII to date, agencies can assume that identity information has been compromised. Accordingly, agencies can develop and apply upfront controls for their programs to verify applicant identity (see sidebar).

Data breaches provided a source of PII for fraudsters. In a May 2021 fraud alert, the U.S. Secret Service warned that an international crime ring was filing UI claims in different states using PII belonging to identity theft victims, including first responders, government personnel, and school employees. The fraud alert further noted a well-organized Nigerian

[21] The Integrity Data Hub is a centralized, multistate data system that the UI Integrity Center operates in partnership with DOL, using DOL funding. The Integrity Data Hub provides state workforce agencies with cross-matching capabilities to analyze UI claims data to detect and prevent UI fraud and improper payments.

[22] GAO, *Unemployment Insurance: Data Indicate Substantial Levels of Fraud during the Pandemic; DOL Should Implement an Antifraud Strategy,* GAO-23-105523 (Washington, D.C.: Dec. 22, 2022).

[23] Department of Labor, Office of Inspector General, *COVID-19: ETA Can Improve its Oversight to Ensure Integrity over CARES Act UI Programs*, Report No. 19-23-011-03-315 (Washington, D.C.: Sept. 22, 2023).

fraud ring seeking to commit large-scale fraud against state UI programs. Washington, North Carolina, Massachusetts, Rhode Island, Oklahoma, Wyoming, and Florida were subject to efforts by this ring to defraud their UI programs.

A stakeholder panel we convened in 2022 also shared concerns about identity fraud schemes orchestrated during the pandemic.[24] One panelist, who investigated UI fraud at the state level, explained that many fraudsters who had stolen identity information prior to the pandemic saw the CARES Act UI programs as an opportunity to use that information to obtain benefits.

Insights from Program Design Limitations

Thoughtful program design choices that consider fraud vulnerabilities upfront can facilitate fraud prevention. During the pandemic—because the government needed to provide assistance quickly to those affected by COVID-19 and its economic effects—initial legislative and policy program design posed limitations for effective management of fraud risks. Ensuring that payment integrity checks and fraud controls are part of program design, including emphasizing data access and use for fraud prevention, can facilitate fraud prevention (see sidebar).

Limiting data access and use. Challenges included limitations on data access and use that constrain agencies' capabilities to prevent and detect fraud.

Insight #6: Ensure payment integrity checks and fraud controls are part of program design, with an emphasis on assuring data access and use for fraud prevention.

Source: GAO (analysis); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

For one of DOL's temporary UI programs—Pandemic Unemployment Assistance—and SBA's PPP and COVID-19 EIDL pandemic relief programs, Congress initially allowed reliance on self-certification of participant eligibility and also eliminated certain verification requirements. These program design decisions, coupled with the large scale of the programs, increased fraud risks. For example, the CARES Act allowed Pandemic Unemployment Assistance applicants to self-certify their

[24] GAO-22-105162.

eligibility and did not require them to provide any documentation of self-employment or prior income. Similarly, for COVID-19 EIDL, Congress removed safeguards that had been in place prepandemic in an effort to expedite loan processing. The Consolidated Appropriations Act, 2021, enacted in December 2020, included provisions to help address these risks.

Also early in the pandemic, the Internal Revenue Service's (IRS) disbursement approach that allowed EIPs to go to decedents presented improper payment risks related to ineligibility and fraud. This situation highlights the importance of clearly assuring data use to guide implementation decisions to prevent unnecessary waste in addition to fraud. Specifically, we previously reported that the Treasury and IRS did not use the Social Security Administration's death records to stop payments to deceased individuals for the first three batches of EIPs because of the legal interpretation under which IRS was operating.[25] The first three batches of payments accounted for 72 percent of the payments disbursed as of May 31, 2020. According to the Treasury Inspector General for Tax Administration, as of April 30, 2020, almost 1.1 million payments totaling, nearly $1.4 billion, had gone to decedents. According to IRS officials, IRS counsel determined that IRS did not have the legal authority to deny payments to those who filed a return for 2019, even if they were deceased at the time of payment. IRS officials said that, on the basis of this determination, they did not exclude decedents in their programming requirement. Treasury officials said that upon learning that payments had been made to decedents, the Treasury and IRS, in consultation with counsel, determined that a person is not entitled to receive a payment if they are deceased as of the date the payment is to be paid. Such payments were removed, starting with the fourth payment batch.

[25] GAO, *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts*, GAO-20-625 (Washington, D.C.: June 25, 2020).

Actions and Resources to Better Manage Fraud Risks

Actions and resources. Nearly 100 GAO fraud risk management recommendations remain open.

Insight #7: Take actions to better prevent fraud by implementing GAO recommendations and using resources.

Source: GAO (analysis); Icons-Studio/stock.adobe.com (icon). | GAO-24-107157

With insights for strategic fraud risk management from COVID-19 challenges, agencies are better positioned to manage fraud during normal operations and emergencies. Other sources that provide additional insight for fraud prevention include recommendations we have made to agencies, actions we have identified that Congress can take to strengthen fraud risk management practices across the government, and resources we developed to support strategic fraud risk management. Implementing these recommendations and taking these actions, along with leveraging available resources, can enable agencies to carry out their missions and better protect taxpayer dollars from fraud during normal operations and prepare them to face the next emergency (see sidebar).

Agencies Should Implement GAO Recommendations to More Effectively Manage Fraud Risks

Our work since July 2015 has highlighted areas in which federal agencies need to take additional actions to help ensure they are effectively managing fraud risks, consistent with leading practices in GAO's Fraud Risk Framework. Specifically, as we reported earlier this month, from July 2015 through August 2023, we made 173 recommendations to over 40 agency or program offices related to certain areas aligned with leading practices from the Fraud Risk Framework.[26] As of August 2023, agencies needed to take additional action to fully address 95 of these recommendations. Fully addressing these recommendations can help ensure that federal managers safeguard public resources, including while providing needed relief during emergencies.

[26] GAO-24-106565.

For example, we found that using data analytics to manage fraud risks is one area in need of improvement by federal agencies. The Fraud Risk Framework's leading practices include implementing data-analytics activities as part of an overall antifraud strategy. Data-analytics activities can include a variety of techniques. These techniques include predictive analytics that can identify potential fraud before making payments. Data matching and other techniques to verify self-reported information and other information necessary for determining eligibility for enrolling in programs or receiving benefits are also important tools. In addition, data-mining and data matching techniques can enable agencies to identify potential fraud or improper payments that have already been awarded, thus assisting agencies in recovering these dollars.

We have made recommendations for agencies to use data analytics to better manage fraud risk. Specifically, from July 2015 through August 2023, we made 47 recommendations to federal agencies in this area. These included recommendations to design and implement data-analytics activities to prevent and detect fraud, such as using data matching to verify self-reported information. Of the 47 recommendations, 25 had not been implemented as of August 2023.

Congress Can Take Actions to Better Prevent Fraud

In our March 2022 testimony before the Senate Committee on Homeland Security and Governmental Affairs, we identified actions that Congress could take to strengthen internal controls and financial and fraud risk management practices across the government.[27] These matters for congressional consideration remain open. We continue to believe that such actions will increase accountability and transparency in federal spending in both normal operations and emergencies. Appendix I contains a list of the 10 matters for congressional consideration. Below we highlight three of those matters for which immediate action by Congress would enhance fraud risk management.

[27] 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).

Open Matter for Congressional Consideration

Congress should establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud.

Source: GAO. | GAO-24-107157

Establish a permanent analytics center for identifying fraud and improper payments. Responsibilities for planning and implementing fraud risk management and detection activities start with agency management officials. The oversight community, however, plays a critical role in identifying and investigating suspected fraud. The importance of this role in nonemergency periods is heightened during emergencies, such as the COVID-19 pandemic, as agencies work to implement large-scale relief efforts quickly.

At the outset of the pandemic, there was no permanent, government-wide analytical capability to help inspectors general identify fraud. In March 2021, the American Rescue Plan Act of 2021 appropriated $40 million dollars to the Pandemic Response Accountability Committee, which subsequently established the Pandemic Analytics Center of Excellence (PACE).[28] The role of PACE is to help oversee the trillions of dollars in federal pandemic-related emergency spending. According to the Pandemic Response Accountability Committee, PACE applies best practices, with the goal of building an “affordable, flexible, and scalable analytics platform” to support Offices of Inspector General during their pandemic-related work, including beyond the organization’s sunset date in 2025.

In March 2022, we recommended that Congress establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud.[29] Without permanent, government-wide analytics capabilities to assist the oversight community, agencies will have limited resources to apply to nonpandemic programs to ensure robust financial stewardship, as well as better prepare for applying fundamental financial and fraud risk management practices to future emergency funding.

[28] Pub. L. No. 117-2, 135 Stat. 4.

[29] GAO-22-105715.

Open Matter for Congressional Consideration

Congress should amend the Social Security Act to accelerate and make permanent the requirement for the Social Security Administration to share its full death data with the Department of the Treasury's Do Not Pay working system.

Source: GAO. | GAO-24-107157

Amend the Social Security Act to make permanent the sharing of full death data. Data sharing can allow agencies to enhance their efforts to prevent improper payments to deceased individuals. To enhance identity verification through data sharing, we have previously recommended that Congress amend the Social Security Act to explicitly allow the Social Security Administration to share its full death data with Treasury's Do Not Pay system, a data matching service for agencies to use in preventing payments to ineligible individuals.[30] In December 2020, Congress passed, and the President signed into law, the Consolidated Appropriations Act, 2021, which requires the Social Security Administration to share, to the extent feasible, its full death data with Treasury's Do Not Pay working system for a 3-year period, effective on the date that is 3 years from enactment of the act.[31]

In March 2022, we recommended that Congress accelerate and make permanent the requirement for the Social Security Administration to share its full death data with Treasury's Do Not Pay working system.[32] 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.

[30] GAO, *Improper Payments: Strategy and Additional Actions Needed to Help Ensure Agencies Use the Do Not Pay Working System as Intended*, GAO-17-15 (Washington, D.C.: Oct. 14, 2016); and GAO-20-625.

[31] Pub. L. No. 116-260, div. M and N, 134 Stat. 1182 (2020).

[32] GAO-22-105715.

Open Matter for Congressional Consideration

Congress should amend the Payment Integrity Information Act of 2019 to reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports.

Source: GAO. | GAO-24-107157

Reinstate reporting requirements for fraud risk management. Congress's ability to oversee agencies' efforts to manage fraud risks is hindered by the lack of fraud-related reporting requirements. The Fraud Reduction and Data Analytics Act of 2015 and the Payment Integrity Information Act of 2019 required agencies to report on their antifraud controls and fraud risk management efforts in their annual financial reports.[33] However, the requirement to report such information ended with the fiscal year 2020 annual financial report. Since then, there has been no similar requirement for agencies to report on their efforts to manage fraud risks.[34] In March 2022, we recommended that Congress amend the Payment Integrity Information Act of 2019 to reinstate reporting requirements.[35]

In the absence of reporting on agencies' fraud risk management efforts through annual financial reports, earlier in 2023, we surveyed the 24 Chief Financial Officers Act of 1990 (CFO Act) agencies about steps they have taken to manage fraud risks.[36] In response to our survey, 18 of the CFO Act agencies reported that they have regular and ongoing activities to identify and assess risks to determine the fraud risk profile for programs or operations. Twenty of the agencies indicated that they have regular and ongoing activities to design and implement specific control activities to prevent and detect fraud.

As part of our survey, agencies also rated challenges that could impede their efforts to manage fraud risks. For instance, agencies reported the availability of resources (such as staff and funding) and tools for data analytics as being great or moderate challenges. CFO Act agencies'

[33] Pub. L. No. 114-186, §3(c); Pub. L. No. 116-117, codified at 31 U.S.C. §3357(d).

[34] The Payment Integrity Information Act of 2019 includes multiple ongoing reporting requirements for agencies related to improper payments generally, but none specifically mention fraud.

[35] GAO-22-105715.

[36] GAO-24-106565.

survey responses indicated the following factors as a great or moderate challenge to their fraud risk management efforts:

- Having available staffing, funding, or other resources to conduct fraud risk management activities;
- Having and using tools and techniques for data analytics; and
- Having available expertise to conduct fraud risk management activities.

Agencies also rated factors that could motivate them to manage fraud risk. For example, agencies cited the ability to counter reputational impacts as a factor that would motivate their efforts a lot or somewhat. CFO Act agencies' survey responses indicated the following factors as highly or somewhat motivating to their fraud risk management efforts:

- Congressionally directed prioritization of budget funds for program integrity improvements;
- Ability to counter reputational impacts if fraud is found; and
- Ability to demonstrate financial returns from fraud risk management.

Resources Available to Better Manage Fraud Risks

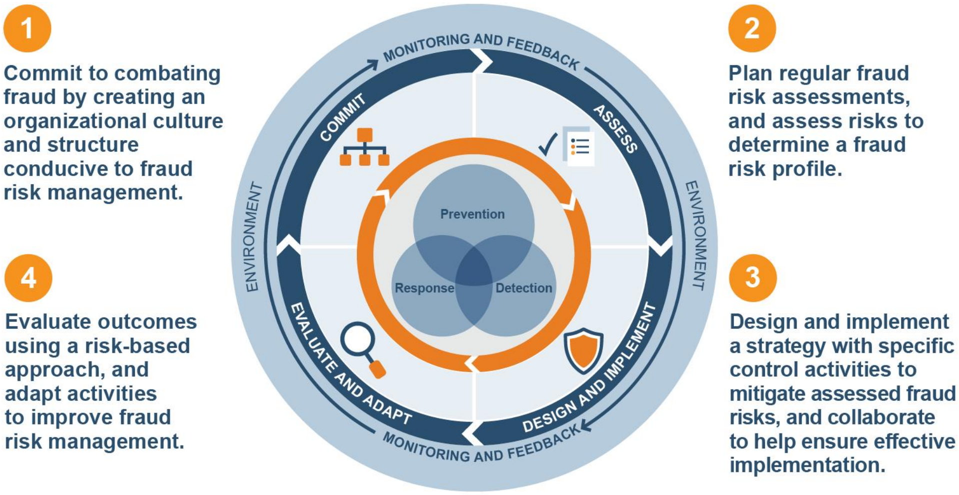
Agencies have the opportunity to learn from the experiences during the pandemic and ensure that they are strategically managing their fraud risks in the future. Doing so by leveraging available resources and adhering to requirements will enable them to carry out their missions and better protect taxpayer dollars from fraud during normal operations and prepare them to face the next emergency.

One such resource is GAO's Fraud Risk Framework, issued in July 2015. This framework provides a comprehensive set of key components and leading practices to help agency managers combat fraud in a strategic, risk-based way. The Payment Integrity Information Act of 2019 requires that the guidelines for federal agencies established by the Office of

Management and Budget (OMB)—which incorporate the leading practices from the Fraud Risk Framework—remain in effect.[37]

As depicted in figure 1, the Fraud Risk Framework describes leading practices for managing fraud risk and includes four components: commit, assess, design and implement, and evaluate and adapt. These leading practices are applicable during normal operations, as well as during emergencies.

Figure 1: The Four Components of the Fraud Risk Framework


1
Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
2
Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile.
3
Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation.
4
Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management.
MONITORING AND FEEDBACK
MONITORING AND FEEDBACK
ENVIRONMENT
ENVIRONMENT
COMMIT
ASSESS
DESIGN AND IMPLEMENT
EVALUATE AND ADAPT
Prevention
Response
Detection

Source: GAO (information and icons). | GAO-24-107157

[37] Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357. The act requires these guidelines to remain in effect, subject to modification by OMB as necessary, and in consultation with GAO. The Fraud Reduction and Data Analytics Act of 2015 required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. The act further required OMB to incorporate the leading practices from the Fraud Risk Framework in the guidelines. Pub. L. No. 114-186, 130 Stat. 546 (2016). In October 2022, OMB issued a Controller Alert reminding agencies that, consistent with the guidelines contained in OMB Circular A-123, which are required by Section 3357 of the Payment Information Integrity Act of 2019, Pub. L. No. 116-117, they must establish financial and administrative controls to identify and assess fraud risks. In addition, OMB reminded agencies that they should adhere to the leading practices in GAO’s Fraud Risk Framework as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. Office of Management and Budget, CA-23-03, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk* (Oct. 17, 2022).

Accessible Data for Figure 1: The Four Components of the Fraud Risk Framework

1. Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
2. Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile.
3. Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation.
4. Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management.

Source: GAO (information and icons). | GAO-24-107157

Another resource is the Bureau of the Fiscal Service's Antifraud Playbook that provides a how-to guide for implementing the Fraud Risk Framework's leading practices.[38] The playbook consists of a four-phased approach—aligned with the four components of the Fraud Risk Framework—and 16 best-practice plays for combatting fraud.

In addition to the Fraud Risk Framework, we have developed other resources—specifically our web-based Antifraud Resource and *A Framework for Managing Improper Payments in Emergency Assistance Programs* (Managing Improper Payments Framework)—to help agencies combat fraud and improve payment integrity.[39] These resources can help agencies better understand and combat the causes and impacts of fraud.

Antifraud Resource. Our prior work found that agencies have had challenges in effectively assessing and managing their fraud risks and that federal managers may not fully understand how fraud affects their programs. GAO created the online Antifraud Resource to help federal officials and the public better understand and combat federal fraud. The Antifraud Resource is based on a conceptual fraud model and provides insight on fraud schemes that affect the federal government, their underlying concepts, and how to combat such fraud. Figure 2 references the online location of this antifraud resource.

[38] Bureau of the Fiscal Service, *Program Integrity: The Antifraud Playbook* (Oct. 17, 2018).

[39] GAO, "The GAO Antifraud Resource" (Washington, D.C.: Jan. 10, 2022), accessed Nov. 3, 2023, https://gaoinnovations.gov/antifraud_resource/; and *A Framework for Managing Improper Payments in Emergency Assistance Programs,* GAO-23-105876 (Washington, D.C.: July 13, 2023).

Figure 2: Reference to GAO’s Antifraud Resource

Sources: GAO and Production Perig/stock.adobe.com (image). | GAO-24-107157

Accessible Data for Figure 2: Reference to GAO’s Antifraud Resource

The GAO Antifraud Resource

Visit https://gaoinnovations.gov/antifraud_resource/

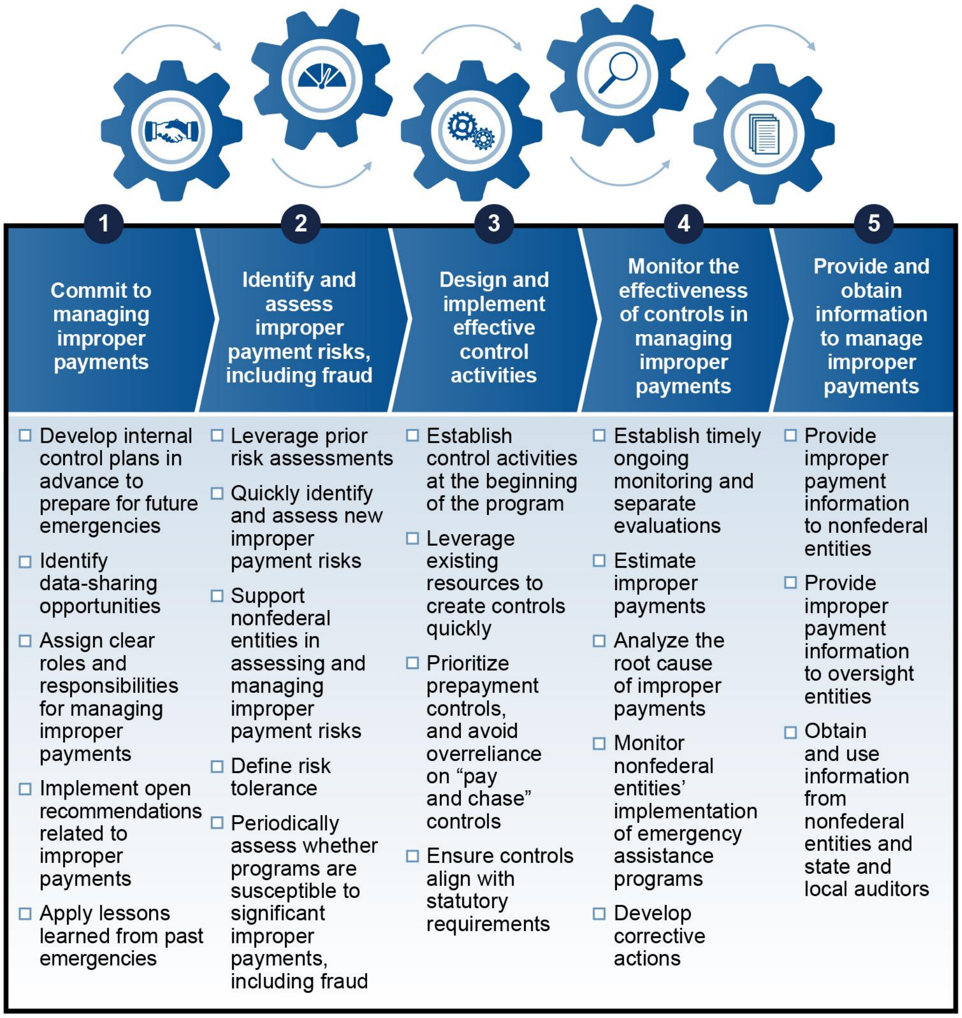
Sources: GAO and Production Perig/stock.adobe.com (image). | GAO-24-107157

Managing Improper Payments Framework. When the federal government provides emergency assistance, the risk of improper payments may be higher because the need to provide such assistance quickly can detract from the planning and implementation of effective controls. Our past work has shown that federal agencies should better plan for, and take a more strategic approach to, managing improper payments in emergency assistance programs. In response, in July 2023, we published the Managing Improper Payments Framework.[40]

This framework includes principles and corresponding practices to help federal agencies mitigate improper payments, including those stemming from fraud, in emergency and nonemergency programs before they occur. It is also intended as a resource for Congress to use when designing new programs or appropriating additional funding in response to emergencies. It includes an overall five-step approach, as described in figure 3, that includes principles aligned with leading practices from our Fraud Risk Framework, such as identifying and assessing fraud risks that cause improper payments.

[40] GAO-23-105876. This framework can also be useful for managing improper payments in nonemergency assistance programs or during normal program operations. This framework should be used by federal agencies in conjunction with existing requirements related to managing improper payments, including those stemming from fraud.

Figure 3: 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 (analysis and icons). | GAO-24-107157

Accessible Data for Figure 3: Framework for Managing Improper Payments in Emergency Assistance Programs

Commit to managing improper payments	Identify and assess improper payment risks, including fraud	Design and implement effective control activities	Monitor the effectiveness of controls in managing improper payments	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 (analysis and icons). | GAO-24-107157

Chair Hassan, Ranking Member Romney, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions.

GAO Contact and Staff Acknowledgments

For further information about this testimony, please contact Rebecca Shea, Director, Forensic Audits and Investigative Service, at (202) 512-6722 or shear@gao.gov.

Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

GAO staff who made key contributions to this testimony are Irina Carnevale (Assistant Director), Paulissa Earl (Analyst in Charge), Gabrielle Fagan, Lauren Kirkpatrick, Barbara Lewis, Maria McMullen, Tina Paek, and Sabrina Streagle.

Appendix I: Matters for Congressional Consideration

In a March 2022 testimony before the Senate Committee on Homeland Security and Governmental Affairs, we recommended the following 10 matters for congressional consideration:[1]

- Congress should pass legislation requiring the Office of Management and Budget (OMB) to provide guidance for agencies to develop plans for internal control that would then immediately be ready for use in, or adaptation for, future emergencies or crises and requiring agencies to report these internal control plans to OMB and Congress. (Matter for Congressional Consideration 1)
- Congress should amend the Payment Integrity Information Act of 2019 to designate all new federal programs making more than $100 million in payments in any one fiscal year as “susceptible to significant improper payments” for their initial years of operation. (Matter for Congressional Consideration 2)
- Congress should amend the Payment Integrity Information Act of 2019 to reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports. (Matter for Congressional Consideration 3)
- Congress should establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud. (Matter for Congressional Consideration 4)
- Congress should clarify that (1) chief financial officers (CFO) at CFO Act agencies have oversight responsibility for internal controls over financial reporting and key financial management information that includes spending data and improper payment information; and (2) executive agency internal control assessment, reporting, and audit requirements for key financial management information, discussed in an existing matter for congressional consideration in our August 2020

[1] 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).

report,[2] include internal controls over spending data and improper payment information. (Matter for Congressional Consideration 5)

- Congress should require agency CFOs to (1) submit a statement in agencies' annual financial reports certifying the reliability of improper payments risk assessments and the validity of improper payment estimates, and describing the actions of the CFO to monitor the development and implementation of any corrective action plans; and (2) approve any methodology that is not designed to produce a statistically valid estimate. (Matter for Congressional Consideration 6)
- Congress should consider legislation to require improper payment information required to be reported under the Payment Integrity Information Act of 2019 to be included in agencies' annual financial reports. (Matter for Congressional Consideration 7)
- Congress should amend the DATA Act to extend the previous requirement for agency inspectors general to review the completeness, timeliness, quality, and accuracy of their respective agency data submissions on a periodic basis. (Matter for Congressional Consideration 8)
- Congress should amend the DATA Act to clarify the responsibilities and authorities of OMB and the Department of the Treasury for ensuring the quality of data available on USAspending.gov. (Matter for Congressional Consideration 9)
- Congress should amend the Social Security Act to accelerate and make permanent the requirement for the Social Security Administration to share its full death data with the Department of the Treasury's Do Not Pay working system. (Matter for Congressional Consideration 10)

[2] GAO, *Federal Financial Management: Substantial Progress Made since Enactment of the 1990 CFO Act; Refinements Would Yield Added Benefits*, GAO-20-566 (Washington, D.C.: Aug. 6, 2020).