United States Government Accountability Office

Report to Congressional Committees

November 2023

COVID-19

Insights from Fraud Schemes and Federal Response Efforts

GAO-24-106353

GAO Highlights

Highlights of GAO-24-106353, a report to congressional committees

November 2023

COVID-19

Insights from Fraud Schemes and Federal Response Efforts

Why GAO Did This Study

Since March 2020, Congress provided over $4.6 trillion to help the nation respond to and recover from the COVID-19 pandemic. The public health crisis, economic instability, and increased flow of federal funds associated with the pandemic increased pressures on federal agency operations and presented opportunities for individuals to commit fraud. The COVID-19 pandemic saw an increase in the number of fraud-related charges, including schemes by individuals and large complex syndicates.

The CARES Act of 2020 includes a provision for GAO to report regularly on the federal response to the pandemic.

This report describes: (1) the status of federal COVID-19 fraud-related cases announced by DOJ, including examples of fraud schemes and (2) examples of federal efforts that have been taken to combat COVID-19 fraud.

GAO reviewed public statements from DOJ from March 2020 through June 2023 to identify federal fraud-related cases. Specifically, GAO identified cases involving COVID-19 relief program fraud; consumer scams; and other types of fraud. GAO then analyzed court documents for details on fraud schemes. GAO also reviewed federal agency documentation and rules, proposed legislation, and proposed antifraud efforts.

What GAO Recommends

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-24-106353. For more information, contact Rebecca Shea at (202) 512-6722 or shear@gao.gov.

What GAO Found

The Department of Justice (DOJ) has brought federal fraud-related charges against at least 2,191 individuals or entities in cases involving federal COVID-19 relief programs, consumer scams, and other types of fraud as of June 30, 2023. Based on GAO's analysis of the cases announced in DOJ press releases, at least 1,525 individuals or entities facing fraud-related charges were found guilty or liable. Courts have ordered individuals to pay restitution ranging up to over $60 million and serve prison terms up to 10 years or more. GAO's analysis of fraud schemes highlights the resulting financial losses and impacts on taxpayers, agency reputation, federal program goals, and health and safety. Agencies can use information about schemes to improve their fraud risk management efforts.

Examples of Fraud Schemes Involving Federal COVID-19 Relief Programs or Consumer Scams

Key mechanism	Fraud scheme description
Conspiracy	A group allegedly conspired to obtain more than $240 million from a federal child nutrition program in a complex fraud scheme. Individuals colluded to open shell companies acting as program sites to claim they were serving thousands of meals a day to underserved children during the pandemic. Instead, these funds were diverted for self-enrichment. Four individuals pleaded guilty but have not been sentenced. Over 40 others are awaiting trial.
Misrepresentation	Two company owners attempted to obtain a total of $5 million by applying for 14 Paycheck Protection Program loans and 12 COVID-19 Economic Injury Disaster Loans. They submitted fabricated tax and other documents inflating the companies' number of employees and payroll. The owners received almost $650,000 in funds they used for personal items, such as a luxury car. Both pleaded guilty, were ordered to pay more than $800,000 in restitution, and were sentenced to 2 to 3 years in prison.
Mislabeling	A company owner sold and mailed pesticide marketed as an air purifier to kill airborne viruses such as COVID-19. The product contained sodium chlorite, a substance declared unmailable under U.S. postal regulations because of its propensity to cause a fire or explosion. The owner was sentenced to 8 months in prison and ordered to pay a total penalty of $556,443 through restitution, fines, and forfeiture.
Health care fraud	A licensed medical practitioner pleaded guilty to selling homeopathic immunizations, falsely claiming they provided immunity to COVID-19. She received over $74,000 for fabricated COVID-19 vaccination and immunization records, knowing this would mislead school officials enforcing the state's vaccination laws. She was sentenced to almost 3 years in prison.

Source: GAO Antifraud Resource and analysis of court documentation (information); Icons-Studio/stock.adobe.com (icons). | GAO-24-106353

Various interagency task forces and the Pandemic Response Accountability Committee (PRAC) were established to combat COVID-19 fraud. For example, the COVID-19 Fraud Enforcement Task Force conducted an enforcement sweep and reported taking law enforcement actions against fraudsters responsible for approximately $836 million in fraud. Similarly, the PRAC estimated its information and resource sharing with investigative agencies supported hundreds of criminal convictions and the recovery of more than $1 billion.

Contents

Letter		1
	Background	3
	DOJ Has Prosecuted Over Two Thousand COVID-19 Fraud-Related Cases, and the Schemes Illustrate a Variety of Participants, Mechanisms, and Impacts	12
	Pandemic Oversight Entity, Interagency Task Forces, and Federal Resources Have Been Established to Combat COVID-19 Fraud	24
Appendix I	GAO Contact and Staff Acknowledgments	34

Tables

Table 1: Key Federal COVID-19 Relief Programs and Funding	4
Table 2: Examples of Fraud Schemes Affecting Federal COVID-19 Relief Programs	17
Table 3: Examples of Schemes Involving Consumer Scams Related to COVID-19	20
Table 4: Examples of Other Fraud Schemes Related to COVID-19	23

Figures

Figure 1: Stages of Fraud Detection	6
Figure 2: The Four Components of the Fraud Risk Framework and Selected Leading Practices	9
Figure 3: Framework for Managing Improper Payments in Emergency Assistance Programs	11
Figure 4: Number of Individuals or Entities That Were Found Guilty or Liable for Fraud-Related Charges Involving One or More COVID-19 Relief Programs, as of June 30, 2023	13
Figure 5: Sentencing Outcomes for Individuals or Entities That Were Found Guilty or Liable for Fraud-Related Charges Involving COVID-19 Relief Programs, as of June 30, 2023	14
Figure 6: Court Ordered Restitution for Individuals or Entities That Were Found Guilty or Liable for Fraud-Related Charges Involving COVID-19 Relief Programs, as of June 30, 2023	15

Abbreviations

COVID-19 EIDL	COVID-19 Economic Injury Disaster Loan
DOJ	Department of Justice
DOL	Department of Labor
EIP	economic impact payment
FBI	Federal Bureau of Investigation
Fraud Risk Framework	*A Framework for Managing Fraud Risks in Federal Programs*
FRDAA	Fraud Reduction and Data Analytics Act of 2015
FTC	Federal Trade Commission
HEERF	Higher Education Emergency Relief Fund
HHS	Department of Health and Human Services
HRSA	Health Resources and Services Administration
IFFR	Identity Fraud Reduction & Redress
IRS	Internal Revenue Service
Managing Improper Payments Framework	*A Framework for Managing Improper Payments in Emergency Assistance Programs*
NUIFTF	National Unemployment Insurance Fraud Task Force
OIG	Office of Inspector General
OMB	Office of Management and Budget
PACE	Pandemic Analytics Center of Excellence
PACER	Public Access to Court Electronic Records
PIIA	Payment Integrity Information Act of 2019
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SBA	Small Business Administration
UI	unemployment insurance
USDA	Department of Agriculture

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 14, 2023

Congressional Committees

Since March 2020, Congress has provided over $4.6 trillion to help the nation respond to and recover from the COVID-19 pandemic. The government's quick disbursement of funds and other assistance to those most affected by the pandemic and its economic effects also increased the risk of fraud to COVID-19 relief programs. When the federal government provides emergency assistance, the risk of payment errors—including those attributed to fraud—may increase because the need to provide this assistance quickly can lead agencies to relax or forego effective safeguards. 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 challenges identifying the full extent of fraud, some estimates of fraud in COVID-19 relief programs exist. For instance, the Small Business Administration's (SBA) Office of Inspector General (OIG) estimated that as of June 2023, SBA disbursed over $200 billion (approximately 17 percent of SBA's total COVID-19 spending) in potentially fraudulent pandemic relief loans.[1] In September 2023, we estimated that the fraud in the Department of Labor's (DOL) unemployment insurance (UI) programs during the pandemic—from April 2020 through May 2023—was likely between $100 billion and $135 billion.[2]

Many individuals and entities facing fraud-related charges in cases involving COVID-19 relief programs have already been found guilty of criminal violations or were found liable for civil violations.

In addition to fraud in the COVID-19 relief programs, scammers have also targeted consumers. Such scams can result in financial losses and undermine health and safety. According to the Department of Health and

[1]This includes Paycheck Protection Program (PPP) loans, COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program loans, EIDL Targeted Advances, and Supplemental Targeted Advances. GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs*, GAO-23-105331 (Washington, D.C.: May 18, 2023).

[2]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).

Human Services OIG, COVID-19 consumer fraud schemes include scammers using testing sites, telemarketing calls, text messages, social media platforms, and door-to-door visits to perpetrate COVID-19-related scams. In some instances, fraudsters offer COVID-19 services such as home testing kits in exchange for personal details, including Medicare information. The personal information collected can be used to fraudulently bill federal health care programs and commit medical identity theft.

The CARES Act includes a provision for GAO to report regularly on the federal response to the pandemic. Specifically, the act requires us to monitor and oversee the federal government's efforts to prepare for, respond to, and recover from the COVID-19 pandemic.[3] This report describes: (1) the status and characteristics of federal COVID-19 fraud-related cases announced by the Department of Justice (DOJ) and (2) examples of federal efforts that have been taken to address COVID-19 fraud.

To determine the status and characteristics of federal COVID-19 fraud-related cases announced by DOJ, we reviewed public statements from DOJ from March 2020 through June 2023 to identify federal fraud-related cases.[4] Specifically, we identified cases involving: (a) various federal COVID-19 relief programs (e.g., Paycheck Protection Program (PPP), COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program, and UI); (b) consumer scams (i.e., fraud resulting in losses to consumers or other efforts to undermine health and safety); and (c) other types of fraud related to COVID-19, such as cases involving health care fraud. We identified these cases by establishing a search query for Westlaw Edge to identify relevant DOJ press releases. We also analyzed corresponding court documentation available in Public Access to Court Electronic

[3]Pub. L. No. 116-136, § 19010(b), 134 Stat. 281, 580 (2020). All of GAO's reports related to the COVID-19 pandemic are available on GAO's website at https://www.gao.gov/coronavirus.

[4]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.

Records (PACER) to describe various examples of federal COVID-19 fraud-related cases in terms of the five key elements of a fraud scheme.[5]

To describe examples of federal efforts that have been taken to address COVID-19 fraud, we reviewed agency rules and documentation, proposed legislation, and antifraud efforts. Examples were selected to cover the range of COVID-19 relief programs and types of fraud that occurred. They are not exhaustive of all federal efforts to address COVID-19 fraud, but rather are illustrative of different types of government-wide efforts undertaken since the beginning of the pandemic.

We conducted this performance audit from October 2022 to November 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.

Background

COVID-19 Relief Funding

Since March 2020, Congress has provided over $4.6 trillion through the CARES Act and other laws that were enacted to fund federal efforts to help the nation respond to and recover from the COVID-19 pandemic.[6] This COVID-19 relief funding included a number of programs and funds. Key federal COVID-19 relief programs and funding are described in table 1.

[5] PACER is a service of the federal judiciary that enables the public to search online for case information from U.S. district, bankruptcy, and appellate courts. Federal court records available through this system include case information (such as names of parties, proceedings, and documents filed) as well as information on case status. The five key elements reflect the highest-level components of the Conceptual Fraud Model. Systematically organized subcomponents of the full model are available for download and exploration from GAO's Antifraud Resource website. GAO, "The GAO Antifraud Resource" (Washington, D.C.: Jan. 10, 2022), accessed Oct. 4, 2023, https://gaoinnovations.gov/antifraud_resource/.

[6] American Rescue Plan Act of 2021, Pub. L. No. 117-2, 135 Stat. 4; Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, div. M and N, 134 Stat. 1182 (2020); Paycheck Protection Program and Health Care Enhancement Act, Pub. L. No. 116-139, 134 Stat. 620 (2020); CARES Act, Pub. L. No. 116-136, 134 Stat. 281 (2020); Families First Coronavirus Response Act, Pub. L. No. 116-127, 134 Stat. 178 (2020); and the Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020, Pub. L. No. 116-123, 134 Stat. 146.

Table 1: Key Federal COVID-19 Relief Programs and Funding

Small Business Administration (SBA)	SBA's **Paycheck Protection Program** (PPP) was authorized under SBA's 7(a) small business lending program. This program provided small businesses with funds to pay up to 8 weeks of payroll costs, including benefits. Funds could also be used to pay interest on mortgages, rent, and utilities. Congress provided over $800 billion for this program.
	SBA's **COVID-19 Economic Injury Disaster Loan** (COVID-19 EIDL) program, which was a continuation of SBA's existing Disaster Loan Program, provided low-interest loans to help small businesses and non-profit organizations meet obligations or pay ordinary and necessary operating expenses. Congress provided about $105 billion for this program.
Department of Labor (DOL)	DOL's **unemployment insurance** (UI) programs served as a pandemic safety net for individuals who lost their jobs through no fault of their own. Congress provided $701.6 billion for four temporary UI programs.
Department of the Treasury and Internal Revenue Service (IRS)	Treasury's **Coronavirus Relief Fund** provided payments to tribal governments, states, localities, the District of Columbia, and U.S. territories to help offset costs of their response to the COVID-19 pandemic. Congress provided $150 billion for this program.
	Treasury's **Emergency Rental Assistance** program provided funding to grantees, such as local governments, to help low-income households at risk of housing instability pay rent and utilities. Congress provided about $46 billion for this program.
	Treasury's and IRS's **economic impact payments** were enacted as a stimulus payment from the IRS to help taxpayers offset the economic effects of the COVID-19 pandemic. Congress provided nearly $860 billion for this program.
Department of Agriculture (USDA)	USDA's **Coronavirus Food Assistance Program** provided financial assistance to farmers and ranchers that gave them the ability to offset sales losses and increased marketing costs. Congress provided about $31 billion for this program.
	USDA's **child nutrition programs** received additional funding for COVID-19 to provide meals to children involved in educational-based programs or activities. Congress provided $8.8 billion for these programs.
Department of Health and Human Services (HHS)	HHS's Health Resources and Services Administration's (HRSA) **Provider Relief Fund** awarded grants to eligible health care providers for health care related expenses or lost revenues that were attributable to the COVID-19 pandemic. Congress provided approximately $178 billion for this program.
	HRSA's **COVID-19 Uninsured Program** reimbursed health care providers generally at Medicare rates for testing, treating, and administering vaccines to uninsured individuals for COVID-19. The federal government has paid providers about $24.5 billion for program claims.
Department of Education	The Department of Education's **Higher Education Emergency Relief Fund** enabled colleges and universities to provide cash grants to current students for educational related expenses and costs incurred because of disruptions to their education. Congress provided about $14 billion for this program.

Federal Reserve		The Federal Reserve established the **Main Street Lending Program** to support lending to small and medium-sized for-profit businesses and non-profit organizations. Treasury made about $13.9 billion available under the CARES Act to support the Main Street Lending Program facilities. Under the program, five facilities in total were designed to support small and mid-sized for-profit businesses and non-profit organizations by purchasing participations in eligible loans.[a]

Source: GAO analysis; SBA, DOL, Treasury, IRS, USDA, HHS, Department of Education, Federal Reserve (agency seals). | GAO-24-106353

Note: This table does not include all federal programs enacted to address COVID-19 related issues. Also, we use the term COVID-19 relief programs to refer to the programs and assistance outlined in six laws to help the nation respond to and recover from the COVID-19 pandemic. These six COVID-19 relief laws are the American Rescue Plan Act of 2021, Pub. L. No. 117-2, 135 Stat. 4; Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, div. M and N, 134 Stat. 1182 (2020); Paycheck Protection Program and Health Care Enhancement Act, Pub. L. No. 116-139, 134 Stat. 620 (2020); CARES Act, Pub. L. No. 116-136, 134 Stat. 281 (2020); Families First Coronavirus Response Act, Pub. L. No. 116-127, 134 Stat. 178 (2020); and the Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020, Pub. L. No. 116-123, 134 Stat. 146. For the purposes of our review, COVID-19 relief funding is the cumulative amount of funding provided in the COVID-19 relief laws. Consequently, the COVID-19 relief funding amounts reported in this report do not reflect the permanent rescissions enacted in the Fiscal Responsibility Act of 2023, Pub. L. No. 118-5, 137 Stat. 10.

[a]The Main Street Lending Program comprised five facilities: the Main Street New Loan Facility, Main Street Priority Loan Facility, Main Street Expanded Loan Facility, Nonprofit Organization New Loan Facility, and Nonprofit Organization Expanded Loan Facility. The Federal Reserve Bank of Boston administers the Main Street Lending Program.

Fraud, Fraud Risk Management, and Managing Improper Payments in Emergency Assistance Programs

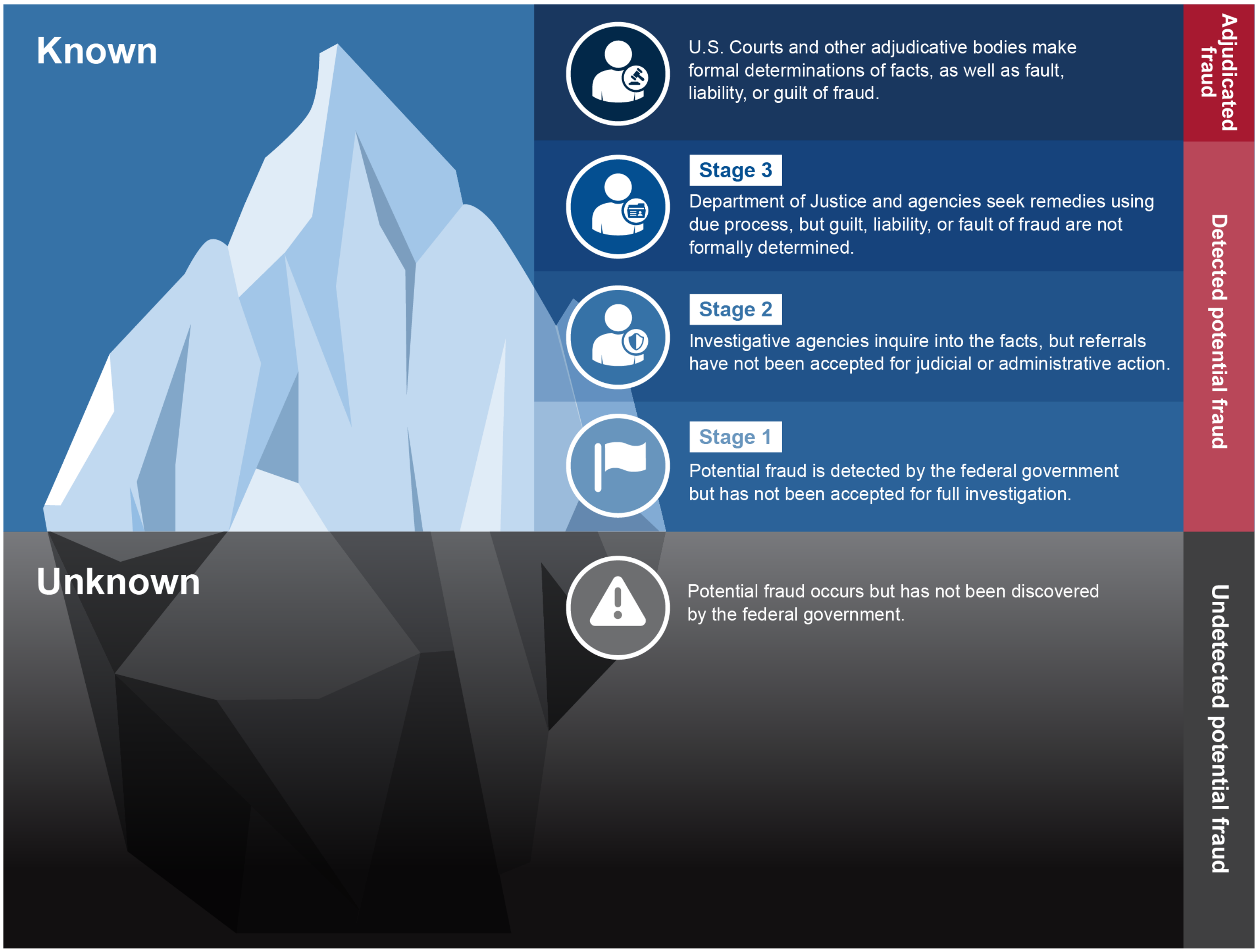
Fraud. Fraud involves obtaining something of value through willful misrepresentation. Willful misrepresentation can be characterized by making material false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity. Whether an act is fraudulent is determined through the judicial or other adjudicative system.

Fraud is challenging to detect because of its deceptive nature. As a result, not all fraudulent activity will be detected or discovered. Generally, once potential fraud is detected and investigated, DOJ may bring charges of fraud against the alleged fraudster.

If a court determines that fraud took place, then fraudulent spending may be recovered through various means. However, recoveries are often a fraction of fraud losses and some amounts may never be recovered. Fraud can also involve benefits that are non-financial in nature. While this type of fraud does not result in a direct financial loss to the government, it can have other impacts such as on trust in government and an agency's reputation. It can also create national security, criminal, health, safety, and other risks.

Figure 1 illustrates stages of fraud identification, including the known—detected potential fraud and adjudicated fraud—and unknown aspects of fraud.

Figure 1: Stages of Fraud Detection



Source: GAO (information); thailerderden10/stock.adobe.com (iceberg); Icons-Studio/stock.adobe.com (icons). | GAO-24-106353

Fraud risk management. We have reported that federal agencies did not strategically manage fraud risks and were not adequately prepared to prevent fraud when the pandemic began.[7] Fraud risk is greatest when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud. When fraud risks can be identified and mitigated, fraud may be less likely to occur. Although the occurrence of fraud indicates there is a fraud risk, the risk can exist even if actual fraud has not yet happened.

The public health crisis, economic instability, and increased flow of federal funds associated with the COVID-19 pandemic increased pressures on federal agency operations and presented opportunities for individuals to commit fraud. The heightened risk and prevalence of fraud in various COVID-19 relief programs underscore the importance of prevention and imperative for federal agencies to manage fraud risks strategically.

In our March 2022 testimony before the Senate Committee on Homeland Security and Governmental Affairs, we identified 10 actions that Congress could take to strengthen internal controls and financial and fraud risk management practices across the government.[8] For example, we suggested Congress (1) establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud; (2) amend the Social Security Act to make permanent the sharing of full death data with the Department of the Treasury's Do Not Pay working system; and (3) reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports, among other actions. 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.

To help federal program managers strategically manage their fraud risks during both normal operations and emergencies, we published *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk

[7]GAO, *Emergency Relief Funds: Significant Improvements Are Needed to Address Fraud and Improper Payments,* GAO-23-106556 (Washington, D.C.: Feb. 1, 2023).

[8]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).

Framework) in July 2015.[9] A provision of the Payment Integrity Information Act of 2019 (PIIA) requires the Office of Management and Budget (OMB) to maintain guidelines for agencies to establish financial and administrative controls to identify and assess fraud risks and that incorporate leading practices from GAO's Fraud Risk Framework.[10] OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* implements this requirement and directs agencies to follow the leading practices outlined in the Fraud Risk Framework.[11]

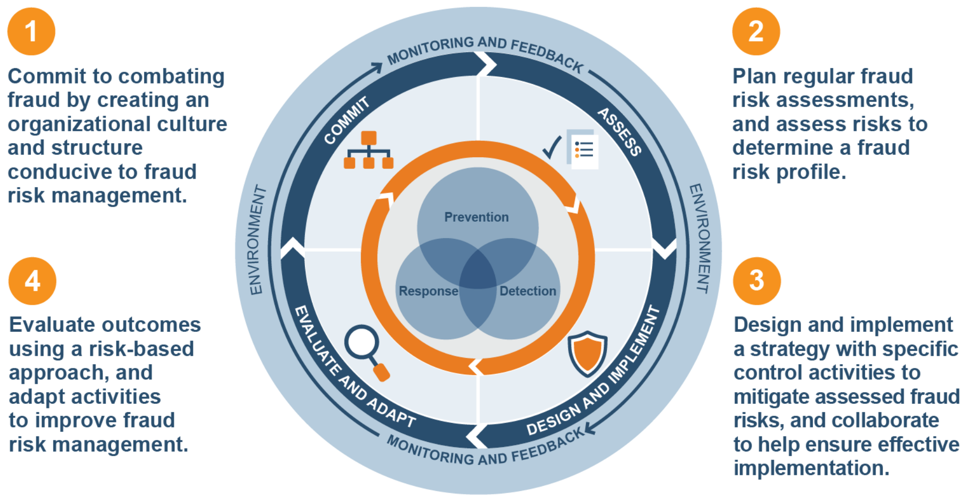
The Fraud Risk Framework describes leading practices in four components: commit, assess, design and implement, and evaluate and adapt, as depicted in figure 2.

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

[10]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. PIIA requires these guidelines to remain in effect, subject to modification by OMB as necessary, and in consultation with GAO. Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357.

[11]In October 2022, OMB issued a Controller Alert reminding agencies that consistent with the guidelines contained in OMB Circular A-123, 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. OMB, CA-23-03, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk* (Oct. 17, 2022).

Figure 2: The Four Components of the Fraud Risk Framework and Selected Leading Practices



Source: GAO (information and icons). | GAO-24-106353

To further assist federal managers in their efforts to manage fraud risk, we created the online Antifraud Resource to help federal officials and the public better understand and combat federal fraud.[12] The Antifraud Resource provides insight on fraud schemes that affect the federal government, their underlying concepts, and how to combat such fraud, and is based on a conceptual model of fraud in the federal government.[13] The conceptual fraud model identifies five key elements of fraud schemes: (1) affected federal programs or operations; (2) participants (those involved in the execution of the scheme and those affected by it); (3) types of fraud activities (e.g., wire fraud, grant fraud, identity fraud); (4) mechanisms (processes, techniques, or systems used to execute the activity); and (5) impacts (financial or non-financial). We describe COVID-19 fraud cases in terms of the five key elements of a fraud scheme in this report.

Managing improper payments in emergency assistance programs. Our oversight of emergency assistance programs—including COVID-19

[12]https://gaoinnovations.gov/antifraud_resource/.

[13]The Conceptual Fraud Model is organized as an "ontology." An ontology is an explicit description of categories in a subject area and their characteristics, as well as the relationships among them. To develop our fraud model, we collected, reviewed, and analyzed multiple sources of information, including over 200 adjudicated federal criminal and civil fraud cases to validate and refine the fraud model.

relief programs—has identified substantial shortcomings in agencies' application of fundamental internal controls as well as fraud risk management practices. These shortcomings can result in significant improper payments—payments that should not have been made or were made in the incorrect amount as a result of mismanagement, errors, abuse, or fraud. While all payments resulting from fraudulent activity are considered improper, not all improper payments are the result of fraud.

When the federal government provides emergency assistance, the risk of improper payments may be higher than in non-emergency programs 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 *A Framework for Managing Improper Payments in Emergency Assistance Programs* (Managing Improper Payments Framework) to help Congress and federal program managers.[14] This framework includes leading practices to help federal agencies combat improper payments, including those stemming from fraud, in emergency and non-emergency programs before they occur. It includes an overall five-step approach described in figure 3.

[14]GAO, *A Framework for Managing Improper Payments in Emergency Assistance Programs,* GAO-23-105876 (Washington, D.C.: July 13, 2023). This framework should be used by federal agencies in conjunction with existing requirements related to managing improper payment, 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-24-106353

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.

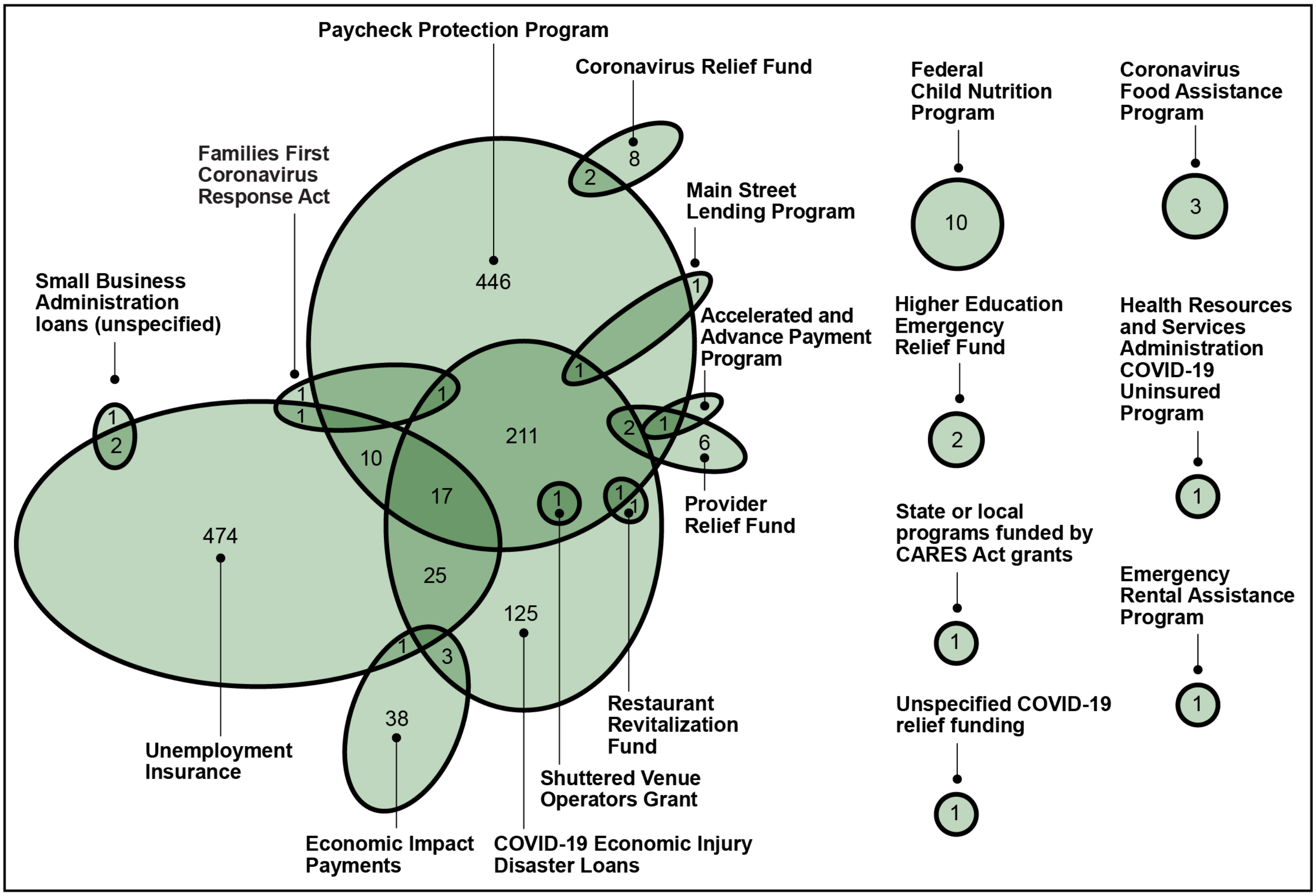
DOJ Has Prosecuted Over Two Thousand COVID-19 Fraud-Related Cases, and the Schemes Illustrate a Variety of Participants, Mechanisms, and Impacts

About 1,400 Fraud-Related Cases Involving COVID-19 Relief Programs Have Resulted in Findings of Guilt

At least 1,399 individuals or entities were found guilty or liable in 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.[15] The cases with findings of guilt or liability involve COVID-19 relief programs such as SBA's PPP and COVID-19 EIDL program, DOL's UI programs, and Treasury's economic impact payments (see fig. 4).

[15]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 lifecycle represent a fraction of the instances of fraud or all possible fraud cases.

Figure 4: Number of Individuals or Entities That Were Found Guilty or Liable for Fraud-Related Charges Involving One or More COVID-19 Relief Programs, as of June 30, 2023

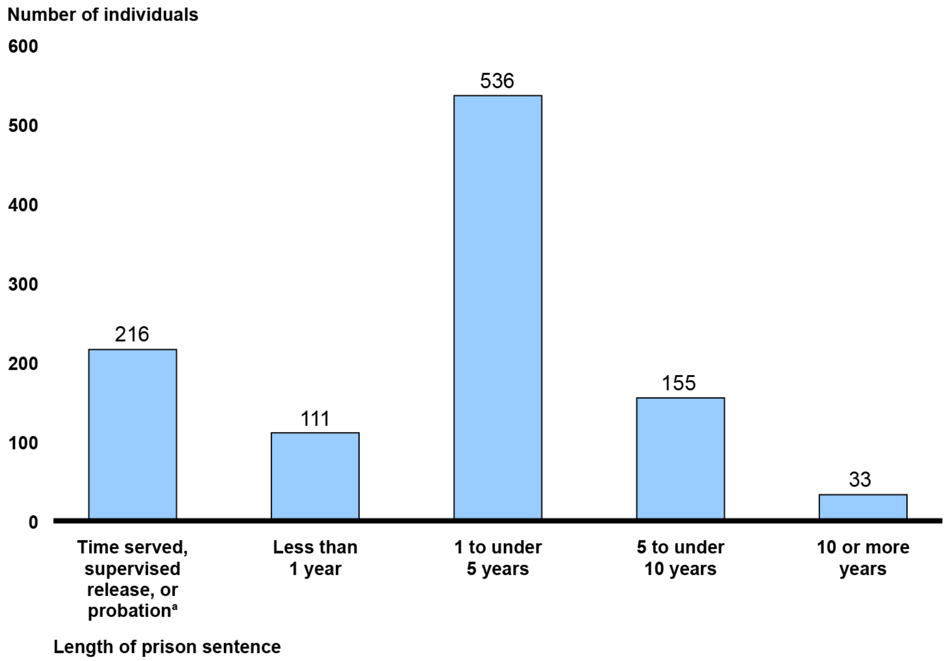


Source: GAO analysis of Department of Justice case information. | GAO-24-106353

Note: 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.

Of the individuals found guilty, at least 1,051 had been sentenced as of June 30, 2023 (see fig. 5). The range in length of prison sentencing varies in part based on other relevant factors, such as prior convictions and whether there were other charges in addition to COVID-19 related fraud.[16]

Figure 5: Sentencing Outcomes for Individuals or Entities That Were Found Guilty or Liable for Fraud-Related Charges Involving COVID-19 Relief Programs, as of June 30, 2023



Source: GAO analysis of Department of Justice case information. | GAO-24-106353

Note: Some of these individuals or entities were sentenced for additional charges not related to COVID-19 relief programs. In addition to prison time, sentences can include restitution, fines, or other fees. 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.

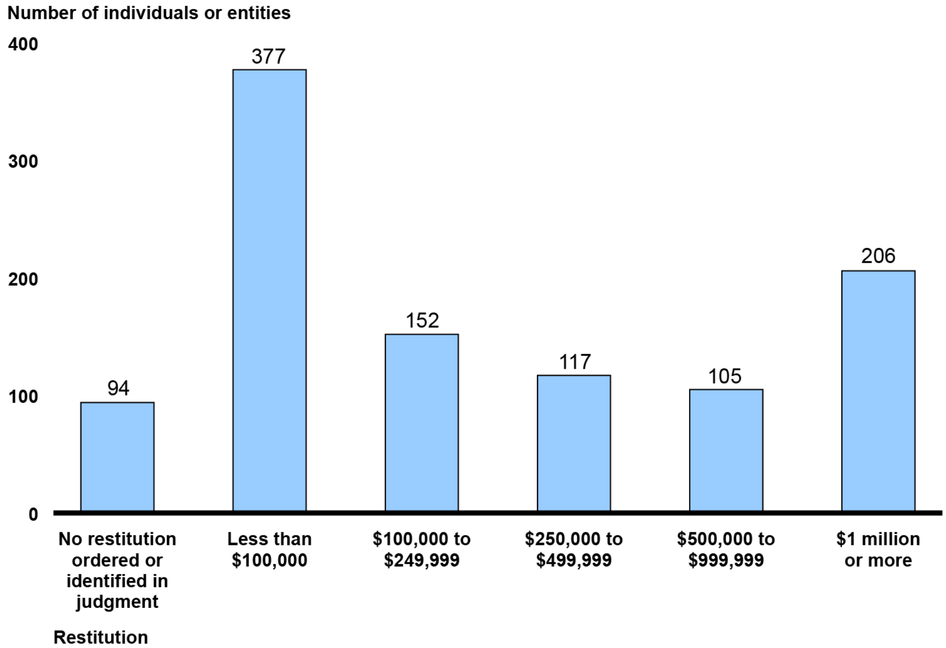
[a]These individuals were sentenced to time served, supervised release, or probation but no prison sentence.

Some individuals and entities found guilty have also been ordered to pay restitution and fines. Courts ordered restitution amounts ranging from

[16]Courts refer to the United States Sentencing Commission Guidelines to determine the particular sentence in each individual case. Under 28 U.S.C. § 994, the Guidelines should reflect a variety of factors and considerations to determine an appropriate sentence. The Guidelines set a base offense level and then add or subtract levels due to aggravating or mitigating circumstances, such as the dollar amount of the loss caused by offense and the defendant's criminal history, ultimately arriving at a suggested sentencing range. Additionally, many of the defendants we reviewed were convicted on additional charges beyond fraud against COVID-19 relief programs, which would impact the length of their sentences.

zero to over $60 million. Individuals or entities in over 200 cases were ordered to pay $1 million or more in restitution (see fig. 6).

Figure 6: Court Ordered Restitution for Individuals or Entities That Were Found Guilty or Liable for Fraud-Related Charges Involving COVID-19 Relief Programs, as of June 30, 2023



Source: GAO analysis of Department of Justice case information. | GAO-24-106353

Note: 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.

Hundreds of COVID-19 Fraud-Related Cases Are Pending

In addition to those individuals and entities with findings of guilt, 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.[17] 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. For example, an individual charged in an indictment in 2022 may not receive a trial until 2023 and if found guilty, the sentencing may occur in 2024 or later. As of August 2022, the statute of limitations has

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

been extended to 10 years to prosecute individuals who committed PPP and COVID-19 EIDL-related fraud.

Fraud Schemes Illustrate a Variety of Participants, Mechanisms, and Impacts

We identified examples of various fraud schemes through our analysis of court documentation for adjudicated cases involving federal COVID-19 fraud-related charges. We found that the fraud scheme participants ranged from individuals with co-conspirators to very large complex fraud syndicates that include foreign nationals.

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, and document falsification. A mechanism can be an individual action or a group of actions working in concert. These 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.

Program managers can use the details of existing fraud schemes identified in their programs—including information on the impact of these schemes—to 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 alignment with leading practices outlined in GAO's Fraud Risk Framework.[18] 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 non-financial 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.

[18]GAO-15-593SP.

Table 2 provides examples of various fraud schemes affecting federal COVID-19 relief programs. The examples include some of the mechanisms used to carry out the fraud activity, as well as the participants and impacts. Although the examples are categorized by a particular mechanism, the same mechanisms may be present in other fraud scheme examples as well. Also, the examples below do not reflect all of the fraud schemes, mechanisms, or affected COVID-19 relief programs.

Table 2: Examples of Fraud Schemes Affecting Federal COVID-19 Relief Programs

Key mechanism	Fraud scheme description
 **Conspiracy.** Cases involve a secret agreement by two or more individuals to commit a crime.	**Participants and affected program:** Nearly 50 individuals are alleged to have engaged in a complex scheme to defraud a federal child nutrition program. The ringleaders of the scheme operated a non-profit organization that served as a program sponsor prior to the pandemic. Other individuals—recruited by employees of the non-profit to participate in the scheme—set up sham program delivery sites to fraudulently claim reimbursements for meal delivery. **Fraud scheme:** Employees of the non-profit recruited individuals to establish dozens of shell companies to enroll as program delivery sites throughout the state in order to fraudulently claim program reimbursements. The non-profit employees solicited and received bribes and kickbacks from the sponsored delivery sites. Owners of the sham delivery sites claimed to be serving meals to thousands of children a day within just days or weeks of being formed. They created fictitious names and ages of children for their enrollment applications, created and submitted false documentation such as fraudulent meal count sheets, invoices, and attendance rosters, and used shell companies to receive and launder program proceeds. **Impacts:** As of June 30, 2023, four defendants have pleaded guilty to relevant charges but have not yet been sentenced. The remaining individuals are still awaiting trial. In exchange for sponsoring these sites' fraudulent participation in the program, the non-profit received more than $18 million in administrative fees to which it was not entitled. In total, the non-profit organization claimed to have opened more than 250 sites throughout the state of Minnesota and fraudulently obtained and disbursed more than $240 million in program funds for their own financial benefit instead of using the funds as intended to feed underserved children.
	Participants and affected program: Two foreign nationals and suspected leaders of an overseas-based transnational organized crime group fraudulently obtained unemployment insurance (UI) benefits. **Fraud scheme:** The two foreign nationals submitted multiple fraudulent applications to receive UI benefits. They both fraudulently claimed to be U.S. citizens and provided fake Social Security numbers. They used the illicit funds from unemployment benefits, along with funds they received by pawning stolen goods, and laundered these funds through wiring money to entities in another country. Their crimes included the robbery of $1.4 million in jewelry from residents of elderly communities. **Impacts:** Together with their co-conspirators, the two foreign nationals received a total of approximately $32,250 in UI benefits they were not eligible to receive. They both pleaded guilty to conspiracy to launder monetary instruments, but have not been sentenced as of June 30, 2023.

Key mechanism	Fraud scheme description
 **Misrepresentation.** Cases involve a false statement of a material fact made by one party that affects another party's decisions. This includes other mechanisms such as document manipulation, eligibility misrepresentation, and false statements.	**Participants and affected program:** Two individuals owned and operated seven companies engaged in a fraud scheme involving the Paycheck Protection Program (PPP) and COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program. **Fraud scheme:** The individuals applied for 14 PPP loans for approximately $2 million and 12 COVID-19 EIDL loans seeking approximately $3 million. In their applications they submitted false documents, including fabricated tax documents, that inflated the number of employees and corresponding payroll of their companies. **Impacts:** The individuals received almost $650,000 in funds intended to help businesses keep their workforce employed during the pandemic, but these funds were instead used for personal gain, including the purchase of a $100,000 luxury car. Both individuals pleaded guilty and were ordered to pay more than $800,000 in restitution. One defendant was sentenced to more than 3 years in prison, while the other was sentenced to over 2 years in prison.
	Participants and affected program: Two individuals engaged in PPP and COVID-19 EIDL fraud. **Fraud scheme:** These individuals submitted applications claiming bogus employees. They used residential addresses claiming they were farmers employing 15 total employees with annual earnings over $1.2 million. In actuality they employed no one and the farms did not exist. **Impacts:** They obtained over $1 million in PPP and COVID-19 EIDL funds. This money that was intended to help businesses keep their workforce employed during the pandemic were instead used for personal gain. Collectively they were ordered to pay over $218,000 in restitution. One individual was sentenced to 18 months in prison and the other was sentenced to 30 months in prison.
 **Money laundering.** Cases involve the processing of criminal proceeds to disguise their illegal origin (e.g., money mules).	**Participants and affected program:** A social media influencer engaged in PPP and COVID-19 EIDL fraud. **Fraud scheme:** The influencer applied for PPP and COVID-19 EIDL funds through fraudulent documents he created, such as tax forms and bank statements. He deposited fraudulently obtained funds into accounts he opened specifically for that purpose. He then laundered the funds by engaging in several monetary transactions, including purchasing and trading securities and cryptocurrency, settling personal debts and making payments to his girlfriend. **Impacts:** In total, the influencer fraudulently applied for and received $146,000 in PPP funds and $284,000 in COVID-19 EIDL funds intended to help sustain businesses during the pandemic. The influencer pleaded guilty to wire fraud, aggravated identity theft, and money laundering involving PPP and COVID-19 EIDL. The individual has not been sentenced as of June 30, 2023.
	Participants and affected program: An owner of an internet clothing retailer defrauded the Main Street Lending Program. **Fraud scheme:** The individual claimed the funds requested would be used for working capital and payroll only, but they but were not. Instead the individual transferred amounts from the company account to her personal account and used the funds to pay for construction on her home and a down payment for a personal vehicle. **Impacts:** She received $424,168 from the Main Street Lending Program. Funds set aside to help small businesses remain operational were instead used for her personal gain. She pleaded guilty to bank fraud and wire fraud and has not been sentenced as of June 30, 2023.

Key mechanism	Fraud scheme description
 **Conflict of interest.** Cases involve an individual or a corporation (either private or governmental) in a position to exploit their own professional or official capacity in some way.	**Participants and affected program:** An individual who worked for the U.S. Postal Service committed fraud involving Treasury's economic impact payments (EIP). **Fraud scheme:** The individual stole credit cards and blank checkbooks from the mail at the post office where she was employed as a clerk, and provided them to her co-conspirators in exchange for cash. She worked with her co-conspirators to create counterfeit EIP checks to deposit in accounts of solicited accountholders for them to later withdraw for cash. She also filed false and fraudulent COVID-19 EIDL applications for fake businesses that did not exist, but those applications were not approved by the Small Business Administration (SBA). **Impacts:** Along with her co-conspirators, they deposited or attempted to deposit thousands of dollars of counterfeit EIP checks. She pleaded guilty to conspiracy to commit bank fraud and false statements to the SBA and was sentenced to 3 years in prison and ordered to pay more than $60,000 in restitution.
	Participants and affected program: An individual was a lead claims examiner at a state's UI agency and engaged in UI benefit fraud. **Fraud scheme:** This individual worked with outside co-conspirators to use his network credentials to override "fraud stops" on UI claims that the state's system had identified as potentially fraudulent. Some of these claims were made in the name of people who did not exist. **Impacts:** In total, his actions resulted in the fraudulent disbursement of over $1.1 million of federal and state UI funds, with an additional attempt to override another $761,000 in funds that was prevented. He pleaded guilty to conspiracy to commit wire fraud and was sentenced to 24 months in prison and approximately $1 million in restitution.
 **Theft.** Cases involve the act of stealing, such as monetary theft and personally identifiable information theft.	**Participants and affected program:** Three individuals engaged in UI benefit fraud. **Fraud scheme:** The group used information stolen from prison inmates to file approximately 50 applications for UI benefits. An incarcerated cousin of one of the individuals provided the inmate information. These funds were transferred to electronic benefits transfer debit cards accounts held in the names of persons, including prison inmates, who were not entitled to receive UI benefits.[a] **Impacts:** In total, the group fraudulently received around $1.2 million in UI benefits. Given the amount the group was able to obtain from the program and the fact that the fraud ring used state prisoners to accomplish their scheme, the state may suffer reputational damage. The group all pleaded guilty to fraud in connection with emergency benefits and wire fraud. The longest sentence one individual in the group received was for almost 2 years in prison. This individual was also ordered to pay more than $450,000 in restitution.
	Participants and affected program: Two college students engaged in fraud involving the Higher Education Emergency Relief Fund (HEERF). **Fraud scheme:** The two students used stolen personally identifiable information, specifically nine individual's student identification numbers and passwords, to access their school's online student portal to apply for emergency financial aid from HEERF. **Impacts:** One of the students fraudulently obtained $800 in HEERF funds while the other student obtained $400 in HEERF funds. In total nine individuals were affected by the identity theft scheme, which can result in them having to take steps to address the fraud committed in their name. Both students pleaded guilty to theft of government money under $1,000 and were sentenced to 1 year of probation and ordered to pay $5,600 in restitution.

Source: GAO Antifraud Resource and analysis of court documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-106353

Note: Although the examples are categorized by a particular mechanism, the same mechanisms may be present in other fraud scheme examples as well.

[a]Electronic benefits transfer is a system similar to a debit card that allows recipients of government assistance to pay directly for purchases.

Numerous Prosecutions Have Targeted COVID-19 Fraud-Related Cases Involving Consumer Scams and Other Types of Fraud

Fraud involving consumer scams. In addition to fraud against federal relief programs, COVID-19 related fraud can result in financial losses to consumers and undermine health and safety. Fraud involving consumer scams are cases that involve deceptive business practices that may cause consumers (individuals or businesses) to suffer financial or other losses. At least 37 individuals or entities facing federal fraud-related charges involving consumer scams related to COVID-19 have pleaded guilty and three individuals or entities received a guilty verdict at trial, according to DOJ public information and court information from March 2020 through June 2023.[19]

Table 3 provides examples of various fraud schemes involving consumer scams related to COVID-19. The examples include some of the mechanisms used to carry out the fraud activity, as well as the participants and impacts. Although the examples are categorized by a particular mechanism, the same mechanism may be present in other fraud scheme examples as well. Mechanisms reflect how fraud activities are carried out and are therefore present across many different types of schemes.

Table 3: Examples of Schemes Involving Consumer Scams Related to COVID-19

Key mechanism	Fraud scheme description
 **Health care fraud.** Cases that involve an individual, a group of people, or a company knowingly misrepresenting or misstating something about the type, the scope, or the nature of the medical treatment or service provided, in a manner that could result in unauthorized payments being made.	**Participants:** A licensed medical practitioner engaged in a health care fraud scheme related to the COVID-19 pandemic. **Fraud scheme:** The practitioner used the COVID-19 pandemic as an opportunity to sell products known as homeopathic immunizations, falsely claiming they would provide lifelong immunity to COVID-19. She provided customers purchasing these products vaccine record cards to make it appear that they received government-approved vaccines. **Impacts**: She received $74,483 in payments for the provision of fabricated COVID-19 vaccination record cards. She provided the false documents knowing that the vaccine record cards would be used to mislead school officials enforcing the state's vaccination laws, creating health and safety risks for customers and the public at large. She pleaded guilty to wire fraud and false statement, and was sentenced to almost 3 years in prison.

[19]There were also federal charges pending against at least 40 other individuals or entities related to consumer scams as of June 30, 2023.

Key mechanism	Fraud scheme description
 **Embezzlement.** Cases involve the unlawful misappropriation or misapplication by an offender to his or her own use or purpose of money, property, or some other thing of value entrusted to his or her care, custody, or control.	**Participants:** An office manager engaged in fraud involving the Paycheck Protection Program (PPP). **Fraud scheme:** The office manager and her husband devised a scheme to defraud the company she was employed by. The company appropriately received a PPP loan. However, the office manager used her access to the company's bank accounts and credit cards to make transfers of more than $43,000 from the loan to pay personal bills or to bank accounts she and her husband controlled. **Impacts:** The office manager's actions took federal funds from the company so it could not use those funds for their intended purpose. The office manager pleaded guilty to wire fraud, and was sentenced to 4 years in prison and ordered to pay approximately $587,000 in restitution.
 **Mislabeling.** Cases involve mislabeling products.	**Participants:** A business owner mislabeled products related to the COVID-19 pandemic. **Fraud scheme**: A company and its business owner unlawfully imported, sold, and mailed unregistered pesticide product marketed as a killer of airborne viruses such as COVID-19. The product was falsely described as an air purifier rather than a pesticide. The company shipped products to individuals who purchased from their website via U.S. mail. The product contained sodium chlorite, which is an item declared to be unmailable under U.S. postal rules and regulations because of its propensity to cause a fire or explosion. **Impacts:** The company and its business owner were ordered to jointly pay restitution of $86,754 and forfeit $427,689 in proceeds. In addition, the company agreed to pay a fine of $42,000, for a total financial penalty of $556,443. The company sold this mislabeled product to customers purchasing it with the hopes of killing the COVID-19 virus, creating potential health and safety risks for customers and the public at large. The business owner pleaded guilty to the entry of goods falsely classified and was sentenced to 8 months in prison.
 **Smuggling.** Cases involve exporting or importing something in violation of customs laws.	**Participants:** An individual engaged in smuggling mislabeled products to treat COVID-19. **Fraud scheme:** The smuggler imported chloroquine from a manufacturer overseas with the intent to divide it into gel capsules and distribute it to others for preventing and treating COVID-19. He was not a licensed medical provider or pharmacist and has no medical background or training. **Impacts:** The smuggler caused the package in which the chloroquine was shipped to be mislabeled and undervalued to evade detection at the U.S. border creating potential health and safety risks for customers and the public at large. He pleaded guilty to a violation of the Federal Food, Drug and Cosmetics Act, and was sentenced to 2 years of probation and ordered to pay a $1,000 fine.

Source: GAO Antifraud Resource and analysis of court documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-106353

Note: Although the examples are categorized by a particular mechanism, the same mechanisms may be present in other fraud scheme examples as well.

Other fraud cases. In addition, we identified other types of COVID-19 fraud-related cases that either involve a federal program that is not a COVID-19 relief program or involve a COVID-19 related issue other than consumer scams. Eighty-one individuals or entities pleaded guilty to federal charges related to these other federal cases and five individuals or entities received a guilty verdict at trial according to DOJ public information and court information we reviewed from March 2020 through June 2023.[20]

Table 4 provides examples of fraud schemes involving COVID-19 fraud in a federal program that is not a COVID-19 relief program or involves a COVID-19 related issue other than consumer scams. The examples include some of the mechanisms used to carry out the fraud activity, as well as the participants and impact of fraud. Although the examples are categorized by a particular mechanism, the same mechanisms may be present in other fraud scheme examples as well.

[20]In addition to the individuals or entities who pleaded guilty to these other types of federal charges that were related to COVID-19 fraud, there were also federal charges pending against at least 27 other individuals or entities as of June 30, 2023

Table 4: Examples of Other Fraud Schemes Related to COVID-19

Key mechanism	Fraud scheme description
 **Medical self-referral.** Cases whereby a physician unlawfully refers certain designated health services payable by Medicare to an entity with which the physician or an immediate family member has a financial relationship (ownership, investment, or compensation), unless an exception applies.	**Participants:** Three individuals were involved in a fraud scheme to commit Medicare fraud that included purported COVID-19 testing. **Fraud scheme:** Two of the individuals solicited, received, and concealed kickbacks and bribes from a third conspirator who owned a company that purportedly provided genetic and COVID-19 testing and other laboratory testing services. The company owner billed Medicare for various purported services, without regard to whether the patients needed any tests or were eligible for Medicare reimbursement. The company owner also paid over $190,000 to the co-conspirators in kickbacks for the referrals. **Impacts:** Medicare paid more than $800,000 based on the fraudulent claims submitted. By stealing from federal health care programs, this scheme victimized beneficiaries and violated the public's trust during a national emergency. The two co-conspirators pleaded guilty to conspiring with a clinical laboratory to commit Medicare fraud, and wire fraud. The company owner who paid kickbacks and bribes received the longest sentence of more than 6 years in prison and was ordered to pay almost $3 million in restitution.
 **Spoofing.** Case that uses deliberately falsified contact information (phone number, email, and website) to mislead and appear to be from a legitimate source.	**Participants:** A foreign national was involved in a spoofing scam to obtain COVID-19 related medical equipment. **Fraud scheme:** During the COVID-19 pandemic, the foreign national impersonated procurement officials of eight U.S. states and local governments and three educational institutions to fraudulently obtain medical equipment, such as defibrillators. He used a web hosting company to spoof state procurement email addresses and sought quotes for medical, laboratory, and computer equipment from targeted suppliers. The targeted suppliers were known to do business with the entities the foreign national was impersonating. The foreign national used the payment terms of "net 30 days", which is a standard term for government and educational entities that requires payment for the goods within 30 days of delivery. He exploited this industry standard to fraudulently obtain equipment without providing any advance payment information or deposit prior to delivery of the equipment. **Impacts:** Through this impersonation, the foreign national obtained and attempted to obtain millions of dollars of medical equipment, laboratory products, computer equipment and hardware, and other merchandise. This type of medical equipment, like defibrillators, were in dire need during the COVID-19 pandemic because the high demand and stress on supply chains caused shortages and reduced accessibility to life-saving equipment. The foreign national pleaded guilty to wire fraud and was sentenced to more than 4 years in prison and ordered to pay more than $300,000 in restitution.

Source: GAO Antifraud Resource and analysis of court documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-106353

Note: Although the examples are categorized by a particular mechanism, the same mechanisms may be present in other fraud scheme examples as well.

Pandemic Oversight Entity, Interagency Task Forces, and Federal Resources Have Been Established to Combat COVID-19 Fraud

The Pandemic Response Accountability Committee's Ongoing Efforts to Address COVID-19 Fraud

The Pandemic Response Accountability Committee (PRAC) was created to help ensure pandemic response spending was administered efficiently and effectively, and COVID-19 relief and recovery funds were awarded appropriately.[21] The PRAC is composed of 21 federal inspectors general. To carry out its mission and address the subsequent fraud occurring in these programs, the PRAC has several ongoing reporting efforts and has developed data analytics tools to detect potential fraud.

Oversight and lessons learned reporting. The PRAC has issued six semiannual reports to Congress about the status of its work. The most recent report, released in June 2023, included updates on investigations, reports, and alerts that focus on fraud, waste, and abuse in the use of the federal pandemic funds.[22] Specifically, the report outlined information on the PRAC's initiatives related to holding wrongdoers accountable through the Fraud Task Force and mitigating major risks that cut across program boundaries through their data analytics efforts.

The PRAC also issued an updated lessons learned report in June 2022 to help identify changes to make pandemic spending more effective.[23] This work highlighted the major lessons the PRAC and its state partners have found in their oversight of pandemic relief and recovery programs. The report identifies 10 key areas for agencies to focus on. The areas related to mitigating fraud are: validating self-certifying information before

[21]The PRAC was established by the CARES Act to conduct oversight of the federal government's pandemic response and recovery effort.

[22]Pandemic Response Accountability Committee, *Semiannual Report to Congress, October 1, 2022 - March 31, 2023* (Washington, D.C.: June 6, 2023).

[23]Pandemic Response Accountability Committee, *Lessons Learned in Oversight of Pandemic Relief Fund*s (Washington, D.C.: June 8, 2022).

payments are sent, using existing federal data sources to determine benefits eligibility, ensuring watchdogs have access to data to find fraud, improving agency collaboration to oversee pandemic relief programs, and accurate reporting to track pandemic relief spending.

Pandemic Analytics Center of Excellence. The PRAC created the Pandemic Analytics Center of Excellence (PACE), which helps agencies find the highest risk areas to investigate by combining oversight data in one place with a suite of analytic tools, with the purpose to be shared and used to find fraud. According to the PRAC, the PACE promotes best practices, provides services to OIGs who lack data analytics capabilities, provides leading edge tools and training to OIG professionals, and promotes overall data literacy throughout the oversight community. As of June 2023, the PRAC reported that the PACE has supported over 500 investigations into more than 6,000 subjects, with an estimated potential fraud loss of $500 million.[24]

However, the PACE is focused on pandemic programs only and the funding for the PACE is currently set to expire in 2025. Ongoing challenges with fraud and improper payments highlight the value of these analytical capabilities, not only for emergency spending but to tackle these challenges across the federal government where they have been a growing concern in recent years.

In March 2022, we recommended that Congress consider establishing a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud.[25] Without permanent government-wide analytics capabilities to assist the oversight community, some OIGs will have limited resources to apply to nonemergency programs to ensure robust financial stewardship. Additionally, the OIG community will lack a comprehensive tool with the power to bring together information from across the whole of government to better prepare for applying fundamental financial and fraud risk management practices to future emergency funding. The status for this matter remains open and not addressed.

[24]Pandemic Response Accountability Committee, *How the PRAC Fights Fraud* (Washington, D.C.: Aug. 23, 2023).

[25]GAO-22-105715.

Interagency Task Forces Aimed at Combatting COVID-19 Fraud

DOJ and the PRAC have developed several interagency task forces to address and combat COVID-19 fraud. The examples of federal efforts presented in this report illustrate the different types of government-wide efforts undertaken since the beginning of the pandemic, and are not exhaustive of all federal efforts to address COVID-19 fraud.

COVID-19 Fraud Enforcement Task Force. DOJ established the COVID-19 Fraud Enforcement Task Force in May 2021 to investigate and prosecute individuals and organizations involved in COVID-19 related fraud. The task force includes representatives from various federal agencies, including the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS). According to DOJ, the goal of the COVID-19 Fraud Enforcement Task Force is to bolster efforts to investigate and prosecute the most culpable domestic and international criminal actors and assist agencies with administering relief programs to prevent fraud. DOJ also notes that the task force does so by augmenting and incorporating existing coordination mechanisms, identifying resources and techniques to uncover fraudulent actors and their schemes, and sharing and harnessing information and insights gained from prior enforcement efforts.

The COVID-19 Fraud Enforcement Task Force has investigated several large cases, including those with complex schemes defrauding COVID-19 relief programs. For example, in August 2023 the COVID-19 Fraud Enforcement Task Force announced a 3-month cross-country fraud enforcement sweep conducted in collaboration with other teams and offices within DOJ. As part of this effort, the COVID-19 Fraud Enforcement Task Force reported taking law enforcement actions against fraudsters responsible for approximately $836 million in fraud. According to a DOJ press release, this included filing criminal charges against 371 defendants. It also included 119 defendants pleading guilty or being convicted at trial with over $57 million in court-ordered restitution imposed. In addition to these actions, there were 117 civil actions with over $10.4 million in judgments. DOJ and law enforcement secured over $231.4 million in criminal and civil forfeiture. These enforcement actions targeted a wide range of criminal activity–from violent criminals to transnational crime groups to fraud on the Internal Revenue Service (IRS)–and illustrate a collective federal commitment to combat COVID-19 related fraud.

National Unemployment Insurance Fraud Task Force. DOJ established the National Unemployment Insurance Fraud Task Force (NUIFTF) in response to the unprecedented scope of UI fraud during the

COVID-19 pandemic. Specifically, it was established to investigate numerous fraud schemes targeting state workforce agency UI programs across the country. The NUIFTF is a prosecutor-led multi-agency task force with representatives from the FBI, DOL OIG, IRS-Criminal Investigation, Homeland Security Investigations, Social Security Administration OIG, and other agencies. In addition to fraud investigations, the NUIFTF has also released public warnings, such as one in March 2021 highlighting that criminals are creating websites mimicking unemployment benefit websites—including state workforce agency websites—to steal personal information and file for UI benefits during the COVID-19 pandemic.

PRAC Fraud Task Force. The PRAC and its OIG partners launched the PRAC Fraud Task Force in January 2021 to help law enforcement pursue investigations and criminal enforcement related to pandemic relief fraud. The PRAC Fraud Task Force coordinates investigations, exchanges information about fraud schemes, and shares resources that support investigations across the federal government. The PRAC reported that the work of the task force has resulted in hundreds of criminal convictions, jail sentences, and the recovery of more than $1 billion.

Identity Fraud Reduction & Redress Working Group. The PRAC formed the Identity Fraud Reduction & Redress (IFFR) Working Group in July 2021 to prevent and address identity fraud in COVID-19 pandemic response programs. According to the PRAC, the IFFR focused on effective identity verification and victim identification, and related fraud reduction and fraud assistance. The IFFR is a joint effort of multiple OIGs from the National Reconnaissance Office, SBA, Treasury Inspector General for Tax Administration, Department of Veterans Affairs, HHS, and DOL. In June 2022, the IFFR released its first report summarizing various OIG partners' work to identify agency actions to reduce fraud and help victims.[26] Specifically, in the report, the IFFR Working Group noted that sharing relevant identity verification data and providing timely

[26]Pandemic Response Accountability Committee, *Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs* (June 13, 2022). The report outlined the following insights on potential improvements to reduce identity fraud in pandemic response programs: conduct data matching and data linking to verify identity and eligibility for government programs, establish controls or processes that check for duplicate applications or benefits, collaborate and coordinate with states and other entities affiliated with government benefit programs, develop processes to track and analyze fraud complaints to uncover patterns or trends, strengthen communication surrounding breaches, and find opportunities to rely on more robust forms or methods of identification.

assistance to identity fraud victims as impactful ways to help the victims of identity fraud recover.

COVID-19 Fraud-Related Resources Developed for Government, Businesses, and Individuals

Federal agencies have developed fraud-related resources for government, individuals, and businesses. Agencies have used hotline portals; provided resources on COVID-19 related fraud online; and have sent out warning letters and issued reports to support other agencies, businesses, and individuals. Congress has also passed additional laws to address COVID-19 pandemic-related fraud.

Agency hotlines. Existing hotline portals maintained by the Federal Trade Commission (FTC), DOJ (National Center for Disaster Fraud), GAO (FraudNet), and agency OIGs and a new hotline portal created by the PRAC are available for anyone to file a complaint on known or suspected fraud, waste, abuse, mismanagement, or violations of laws and regulations involving funds or programs covered within the CARES Act. Allegations are typically forwarded to the appropriate OIG or agency as well as other federal, state, and local oversight entities.

From March 2020 through June 2023, our hotline—known as FraudNet—received about 4,128 complaints related to the CARES Act, about 2,605 of which involve SBA's PPP and COVID-19 EIDL program, DOL's UI programs, and Treasury's and IRS' economic impact payments (EIP).[27] Additionally, as of June 6, 2023, the FTC has received 910,323 overall COVID-19 reports, about 417,224 of which were related to fraud. The FTC also reported that fraud loss totaled $1.1 billion.

Online fraud-related resources and reports. The FTC has developed COVID-19 fraud prevention resources on its website. This includes

[27]The remainder of the complaints relate to a variety of other programs and issues, including other federal COVID-19 relief programs such as the Restaurant Revitalization Fund Grant program and Higher Education Emergency Relief fund; COVID-19 related mortgage fraud; grants; and testing and vaccines. While not all of the complaints received involve allegations of potential fraud, many of them do.

information on how to identity and report COVID-19 related scams and tips on how to protect personal and financial information.[28]

Individual agency OIGs have issued reports on findings, actions, and recommendations related to fraud during the COVID-19 pandemic. For example, in October 2020 the DOL OIG released a report that provided information from an audit on the actions taken by DOL's Employment and Training Administration and state workforce agencies to deter and detect fraud relating to the self-certification process of one of the temporary UI programs, the Pandemic Unemployment Assistance program.[29] As another example, in September 2022 the SBA OIG released a report that evaluated SBA's controls to flag or prevent potentially fraudulent COVID-19 EIDL applications submitted from foreign Internet Protocol addresses, of which the agency processed more than 233,000 applications and disbursed 41,638 COVID-19 EIDL loans for $1.3 billion.[30]

Warning letters. FTC sends warning letters, sometimes jointly with the Food and Drug Administration, to companies allegedly selling unapproved products that may violate federal law by making deceptive or scientifically unsupported claims about their ability to treat or cure COVID-19. The purpose of FTC letters is to warn companies that their conduct is likely unlawful and that they can face serious legal consequences, such as a federal lawsuit, if they do not immediately stop. FTC's website stated that companies that receive warning letters typically take steps to come into compliance with the law and have found the warning letters are a rapid and effective means to address the problem. From March 2020 through June 2023, FTC has sent 536 warning letters to companies.

[28]Examples of online COVID-19 fraud-related resources created by federal agencies include: DOJ, *Coronavirus Response,* accessed Sept. 6, 2023, https://www.justice.gov/coronavirus; FTC, *Coronavirus (COVID-19) Pandemic: The FTC in Action,* accessed Sept. 6, 2023, https://www.ftc.gov/news-events/features/coronavirus; PRAC, *General & Fraud FAQs*, accessed on Sept. 6, 2023, https://www.pandemicoversight.gov/faq-resources/general-and-fraud; SBA, *Preventing fraud and identity theft*, accessed Sept. 6, 2023, https://www.sba.gov/funding-programs/loans/covid-19-relief-options/preventing-fraud-identity-theft.

[29]DOL OIG-Office of Audit, *COVID-19: States Cite Vulnerabilities in Detecting Fraud While Complying with the CARES Act UI Program Self-Certification Requirement,* 19-21-001-03-315 (Washington, D.C.: Oct. 21, 2020).

[30]SBA OIG, *COVID-19 Economic Injury Disaster Loan Applications Submitted from Foreign IP Addresses*, 22-17 (Washington, D.C.: Sept. 12, 2022).

Legislative efforts, proposed legislation, and agency rules. In August 2022 the President signed into law two acts by Congress that extended the statute of limitations for criminal and civil enforcement for all forms of PPP and COVID-19 EIDL fraud from 5 years to 10 years.[31] Enactment of these laws allows investigators more time to pursue those who defrauded programs intended to assist small business owners and their employees during a national crisis. The new ten-year statute of limitations is now consistent with the charge of bank fraud, which the PRAC notes has been charged in most cases of alleged PPP fraud because most loans were issued by traditional banks. For loans not issued by banks, however cases could only be prosecuted as wire fraud, which has a statute of limitations of 5 years. With the new laws in place, law enforcement will now have an additional 5 years to pursue fraud charges in small business relief programs, regardless of the type of lender.

In December 2020, Congress passed the COVID-19 Consumer Protection Act of 2020. This Act made it unlawful for any person or corporation to engage in a deceptive act or practice affecting the treatment, cure, prevention, mitigation, or diagnosis of COVID-19 or a government benefit related to COVID-19.[32] People who violate this Act may be subject to civil penalties, injunctive relief, and other remedies available under the FTC Act. The COVID-19 Consumer Protection Act of 2020 provides additional enforcement authority for the FTC regarding COVID-19 related claims and potentially deters deceptive COVID-19 related scams.

The FTC also published a notice of proposed rulemaking in October 2022 to fight government and business impersonation scams.[33] The proposed rule would prohibit the impersonation of government, businesses, or their

[31]PPP and Bank Fraud Harmonization Act of 2022, Pub. L. No. 117-166, 136 Stat. 1365 and COVID-19 EIDL Fraud Statute of Limitations Act of 2022, Pub. L. No. 117-165, 136 Stat. 1363.

[32]The COVID-19 Consumer Protection Act, which became law in December 2020 as part of the Consolidated Appropriations Act, 2021, gives the FTC authority to seek civil penalties on the first offense for scams and deceptive practices related to the COVID-19 pandemic. Pub. L. No. 116-260, div. FF, tit. XIV, § 1401, 134 Stat. 1182, 3275-3276 (2020).

[33]Notice of Proposed Rulemaking, Trade Regulation Rule on Impersonation of Government and Businesses, 87 Fed. Reg. 62,741 (Oct. 17, 2022).

officials and allow the FTC to recover money from or seek civil penalties against scammers who violate the rule and harm consumers.[34]

In March 2023, the Administration released a new anti-fraud proposal consisting of 17 components intended to enhance the response to fraud against COVID-19 relief programs and apply lessons learned during the pandemic to prevent fraud. The plan includes administrative policy changes, proposals for new legislation, and a total of $1.6 billion in potential new funding. The actions in the proposal are divided into three broader categories—(1) support for fraud investigations and prosecutions, (2) fraud and identity theft prevention, and (3) help for identity theft victims. Additionally, this proposal calls upon the Congress to also increase the statute of limitations for fraud involving pandemic UI programs to 10 years.

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

If you or your staff have any questions about this report, please contact me 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 report. GAO staff who made key contributions to this report are listed in appendix I.

Rebecca Shea
Director, Forensic Audits and Investigative Service

[34]The FTC noted that fraud reports of these impersonation scams rose during the COVID-19 pandemic, and it received more than 2.5 million reports from consumers nationwide from the beginning of 2017 through the middle of 2022, and those consumers reported losing more than $2 billion to these scams.

List of Committees

The Honorable Patty Murray
Chair
Susan Collins
Vice Chair
Committee on Appropriations
United States Senate

The Honorable Ron Wyden
Chairman
The Honorable Mike Crapo
Ranking Member
Committee on Finance
United States Senate

The Honorable Bernie Sanders
Chairman
The Honorable Bill Cassidy, M.D.
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Kay Granger
Chairwoman
The Honorable Rosa L. DeLauro
Ranking Member
Committee on Appropriations
House of Representatives

The Honorable Cathy McMorris Rodgers
Chair
The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Mark E. Green, M.D.
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable James Comer
Chairman
The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Jason Smith
Chairman
The Honorable Richard Neal
Ranking Member
Committee on Ways and Means
House of Representatives

Appendix I: GAO Contact and Staff Acknowledgments

GAO Contact

Rebecca Shea at (202) 512-6722 or SheaR@gao.gov

Staff Acknowledgments

In addition to the contact name above, Gabrielle Fagan (Assistant Director), Scott Clayton (Analyst-in-Charge), Carla Craddock, and Krinjal Mathur made key contributions to this report. Also contributing to the report were Colin Fallon, Amber Gray, Brooke Linsenbardt, Maria McMullen, Daniel Silva, and Sabrina Streagle.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

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.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548

Please Print on Recycled Paper.