

# Fraud Risk in Federal Programs: Continuing Threat from Organized Groups Since COVID-19

GAO-25-107508

Q&amp;A

Report to Congressional Committees

July 10, 2025

Accessible Version

## Why This Matters

Organized groups of individuals working together have defrauded public assistance programs, as was evident during the COVID-19 pandemic. Aided by technology, organized fraud groups have targeted programs at a larger volume and with greater speed than individual fraudsters. Using various fraud schemes, technology, and key information—such as stolen personally identifiable information (PII)—organized fraud groups, both domestic and transnational, continue to pose a threat to public programs.

In April 2025, we reported on fraud schemes and risks affecting federally funded assistance programs during the pandemic. This includes fraud committed both by individual opportunists and organized groups. According to our analysis of Department of Justice (DOJ) public statements and court documentation from March 2020 through December 2024, 46 percent of the 1,875 defendants convicted of pandemic fraud-related offenses with final charges recorded had conspiracy charges, suggesting involvement of an organized fraud group.<sup>1</sup> Although the full extent of pandemic relief fraud is not known, estimates from some of the largest programs—Paycheck Protection Program (PPP), COVID-19 Economic Injury Disaster Loan Program (COVID-19 EIDL), and regular and temporary Unemployment Insurance (UI) programs—put losses around \$300 billion.<sup>2</sup> Some of these losses are associated with organized groups. For example, from January 2018 through May 2021, a hospice owner and a conspirator filed fraudulent claims and paid kickbacks to steal over \$9 million from Medicare. The group carried out additional schemes to obtain fraudulent funds from three pandemic relief programs—the Provider Relief Fund, PPP, and COVID-19 EIDL.

The CARES Act includes a provision for us to monitor and oversee the federal government's efforts to prepare for, respond to, and recover from the COVID-19 pandemic.<sup>3</sup> This report provides information on organized fraud risks to public programs, including pandemic-relief programs, and agencies' roles in preventing and detecting such fraud.

## Key Takeaways

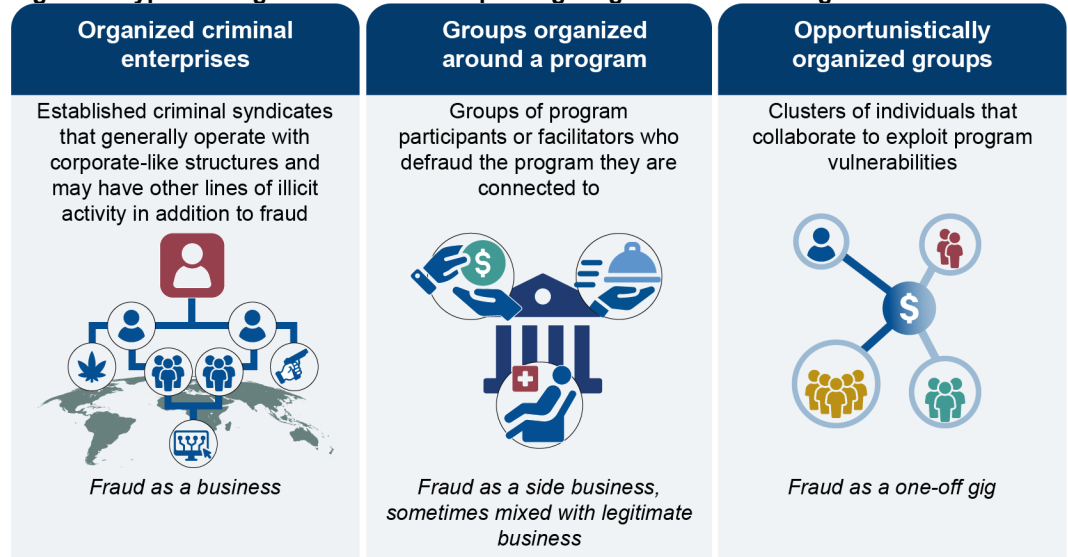
- Organized fraud groups vary in size, structure, and participants and have defrauded programs on a large scale using technology, program knowledge, and other means. These groups harm people, programs, and society in financial and nonfinancial ways that deplete program funds and cause physical and psychological harm.
- Program managers, oversight and payment integrity entities, and law enforcement across the government have roles in preventing, detecting, and responding to organized fraud and use a range of data analytic tools to do so.

- Evolving fraud tactics, data and systems silos, and the need to balance program delivery with fraud controls are some of the challenges to overcome when preventing and detecting organized fraud. However, comprehensive fraud risk management, education, analytics improvements, and collaboration can enhance efforts to prevent and detect organized fraud.
- To enhance fraud risk management, we made 173 recommendations to over 40 agency or program offices from July 2015 through August 2023. Agencies had taken actions to address 78 of these recommendations but had yet to fully address 95 of them, as of August 2023.

## How are fraud groups organized?

Organized fraud groups vary in size, structure, and participants. They generally fall into three types, based on our analysis of fraud cases and information from state, federal, and foreign officials. The three types are (1) organized criminal enterprises, (2) groups organized around a program, and (3) opportunistically organized groups. (See fig. 1) These groups are not mutually exclusive, and a given group may have features of two or more types. Cases involving organized fraud groups range in size from two fraudsters to hundreds. Group structures may be simple, such as a mastermind assisted by someone who produces and sells fraudulent program documentation. Their structures may also be complex, involving multiple cells within the group, each responsible for different tasks to carry out the fraud.

**Figure 1: Types of Organized Fraud Groups Targeting Government Programs**



Sources: GAO analysis of Department of Justice case information and responses from state, federal, and foreign officials (data); Icons-studio, Oleh, stock.adobe.com (icons). | GAO-25-107508

Participants in organized fraud groups may include domestic and foreign individuals (as shown in fig. 2 below). These participants may also be entities internal or external to the program.

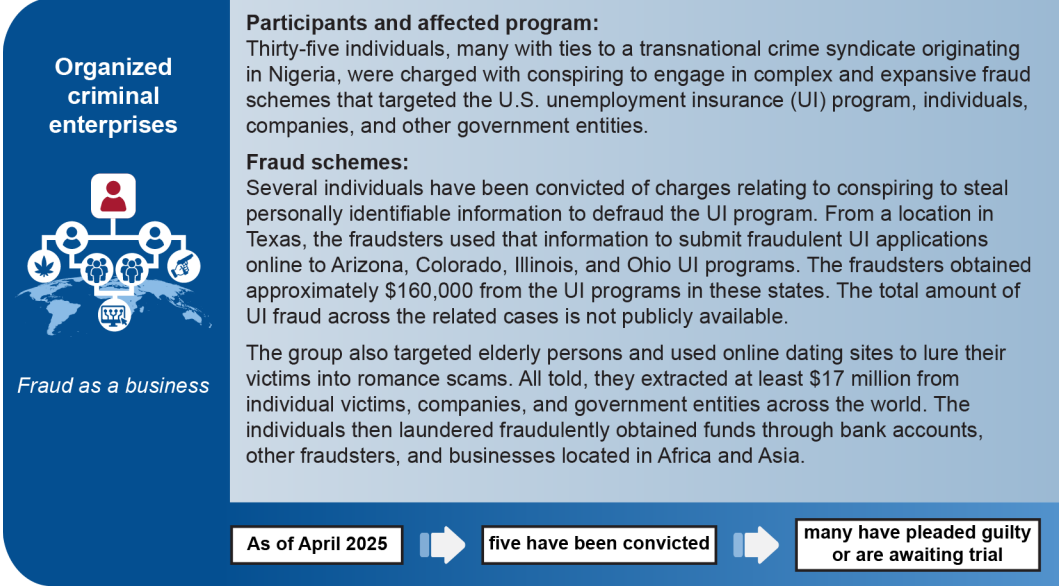
- Fraudsters internal to a program may receive program benefits, deliver benefits through the program, or administer the program, as shown in figure 3 below.
- Fraudsters external to a program are not connected to the program but have exploited program vulnerabilities, as shown in figure 4 below.

**Organized criminal enterprises.** These groups involve established criminal syndicates that may have other lines of illicit activity in addition to fraud. They are generally large and operate with corporate-like structures where individuals or cells act in specialized roles. For example, one cell may focus on procuring

stolen identities; another on electronically preparing and submitting fraudulent documents; and yet another on moving, laundering, and disbursing proceeds. Fraudsters participating in organized criminal enterprises are often external to the program and operate across geographic and legal jurisdictions. For example, these groups have included large transnational criminal enterprises, such as those based in China, Italy, Mexico, Nigeria, Romania, and Russia. Nation-states such as the North Korean government also pose a significant threat.<sup>4</sup>

Figure 2 provides an example of a fraud scheme perpetrated by an organized criminal enterprise against a public assistance program and lays out the fraud scheme participants, the targeted program, and amount of fraudulently obtained funds.

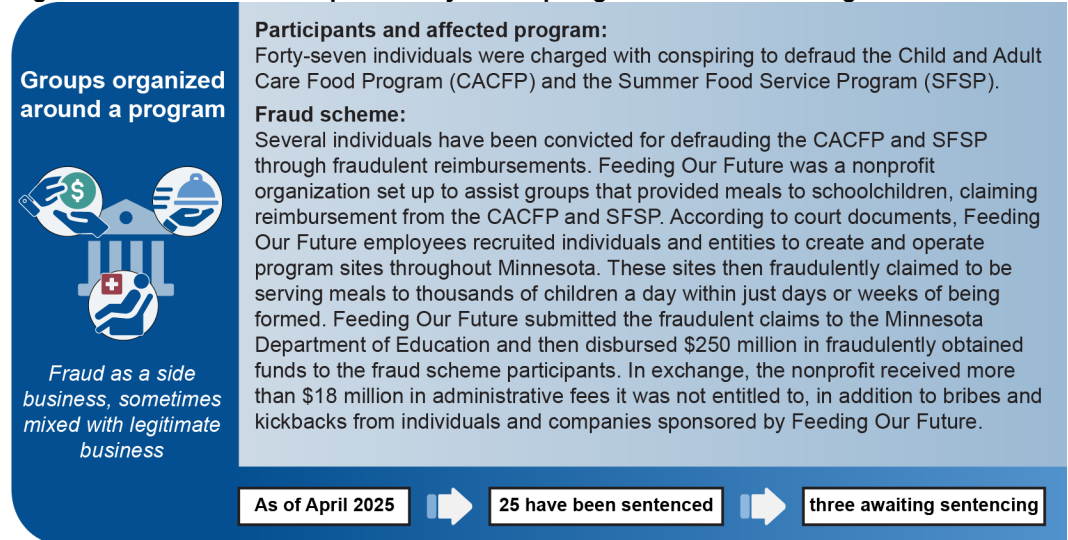
**Figure 2: Fraud Scheme Perpetrated by an Organized Criminal Enterprise**



Sources: GAO analysis of Department of Justice case information (data); Icons-studio, Oleh, stock.adobe.com (icons). | GAO-25-107508

**Groups organized around a program.** Groups organized around a program involve program participants and facilitators who conspire to defraud the program they are connected to. See figure 3. Program participants are individuals or groups who receive public assistance benefits as well as others who are internal to a program, such as those who deliver the benefits, including program administrators, contractors, and grantees, among others. Program facilitators are external individuals or groups in the private sector, for example, tax preparers or attorneys, who may use their program knowledge to conspire with those applying for and receiving benefits by providing fraudulent documentation. These groups vary in size and structure and may involve legitimate businesses. Using program knowledge and connections is a trademark of these groups, often relying on corrupt actions of participants delivering the program.

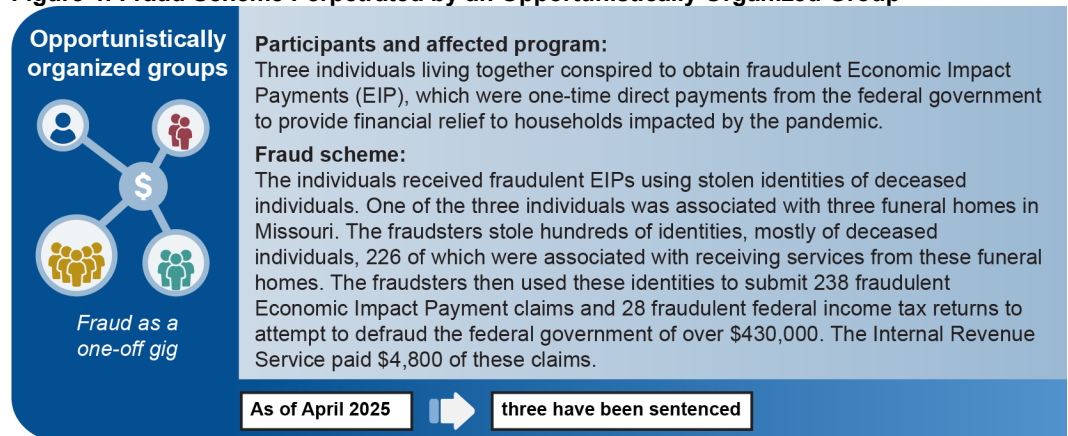
**Figure 3: Fraud Scheme Perpetrated by a Group Organized Around a Program**



Sources: GAO analysis of Department of Justice case information (data); Icons-studio, Oleh, stock.adobe.com (icons). | GAO-25-107508

**Opportunistically organized groups.** These groups involve clusters of individuals who come together as opportunities for fraud arise. Opportunistically organized groups are generally smaller in size and simpler in structure than other types of organized fraud groups. Fraudsters in these groups are external to the program and are recruited from established communities, including online communities. For example, this type of group may form when an individual learns about a fraud scheme to exploit a public assistance program and then recruits friends or family members to participate in the scheme for a kickback fee. See figure 4 for an example of a fraud scheme perpetrated by an opportunistically organized group.

**Figure 4: Fraud Scheme Perpetrated by an Opportunistically Organized Group**



Sources: GAO analysis of Department of Justice case information (data); Icons-studio, Oleh, stock.adobe.com (icons). | GAO-25-107508

For more information about the cases summarized in figures 2, 3, and 4, see appendix I.

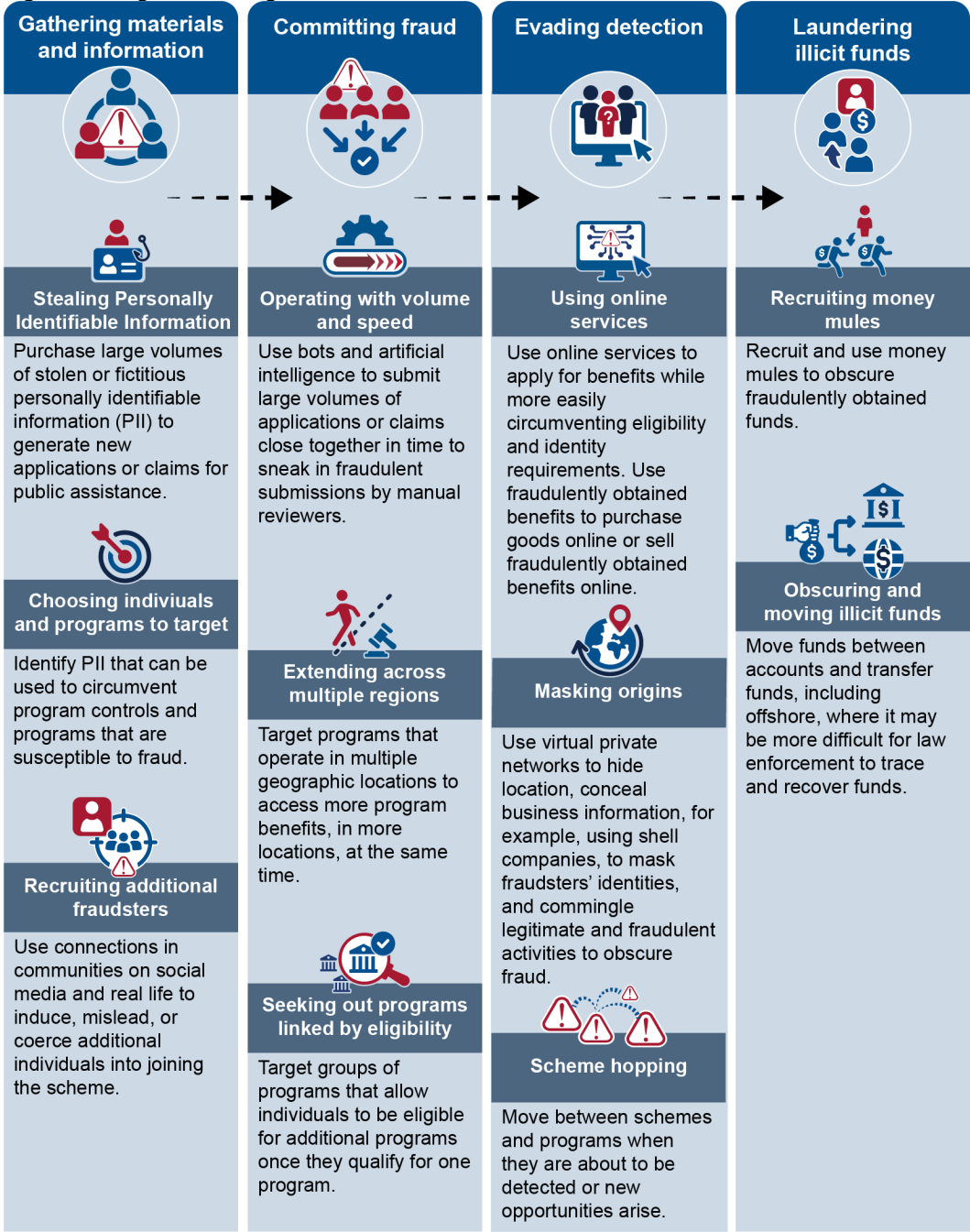
## How have organized groups defrauded public assistance programs?

Organized fraud groups have used technology, program knowledge, and other means to commit fraud on a large scale against a single program as well as multiple programs simultaneously. These groups have used and reused stolen or fictitious PII and forged documentation to misrepresent or falsify eligibility for public assistance programs, file fraudulent applications or claims, and obtain

benefits.<sup>5</sup> Organized groups have committed fraud on a large scale by taking advantage of group participants’ specialized skillsets in carrying out different functions in the scheme.

The stages of an organized fraud scheme include methods commonly used by the three fraud group types, such as gathering materials and information, defrauding programs on a large scale across multiple regions, evading detection, and laundering fraudulently obtained funds, as shown in figure 5.

Figure 5: Stages of an Organized Public Assistance Fraud Scheme



Sources: GAO analysis of responses from state, federal, and foreign officials (data); Icons-Studio/stock.adobe.com (graphics). | GAO-25-107508

**Gathering information and materials.** Organized groups begin a scheme by gathering information and materials, such as PII, information about program controls, and forged documents, to fraudulently obtain public benefits.



PII may be purchased or obtained by targeting groups of individuals. Organized groups may purchase large volumes of stolen or synthetic identities on the dark web.<sup>6</sup> Stolen PII can come from data breaches, hacking, or phishing.<sup>7</sup> These groups may also target individuals whose PII would allow them to circumvent program controls. For example, deceased or homeless individuals' PII may be less likely to be flagged by antifraud controls because these identities may not have been reported as stolen or synthetic.

These groups gather information about, and target programs that allow, individuals to qualify for benefits in many programs once they demonstrate eligibility in one of them.<sup>8</sup> According to officials we spoke with from one state, for example, fraudsters may enroll in Medicaid to more easily establish their financial eligibility for the Supplemental Nutrition Assistance Program (SNAP), which has been easier and more profitable to defraud due to the fraudsters' ability to obtain diverted cash benefits from Electronic Benefit Transfer (EBT) cards.

Organized groups also use social engineering methods and technologies, such as social media and the dark web, to pull additional fraudsters into their schemes.<sup>9</sup> In some cases, they deceive potential recruits about the true nature of their scheme or coerce them into participating in the fraud. In other cases, individuals join the scheme knowingly and willingly for the potential financial gain.

**Committing fraud.** Organized groups operate with volume and speed across multiple regions and programs to fraudulently obtain public benefits. They target public assistance programs at a larger volume and with greater speed than individual fraudsters. For example, for agencies that need to manually review applications, these groups will use bots and artificial intelligence (AI) to submit large volumes of applications within minutes, often reusing information and documentation across multiple applications.<sup>10</sup> Doing so can decrease the time a reviewer has to inspect each document for fraud. These groups also target programs that operate in multiple states or that are linked to other programs by eligibility to access more program benefits, in more states, at the same time.

**Evading detection.** To evade detection, organized groups take advantage of online services to apply for benefits, fraudulently obtain goods, and sell fraudulently obtained goods. Accelerated by the pandemic, these groups have taken advantage of the shift from in-person to online application and claims processes to more easily circumvent eligibility and identity requirements.

Such groups have also fraudulently purchased goods online in large quantities to resell. In October 2024, DOJ indicted one group for allegedly stealing over \$2.4 million in SNAP benefits and using those stolen benefits to purchase large quantities of sports drinks and baby formula from websites associated with grocery stores, later reselling the goods on the black market. These groups have also evaded eligibility requirements by coercing beneficiaries into selling their benefits, often at a loss, and then trafficking the illegally purchased benefits loaded onto SNAP EBT cards to third parties who use the benefits to fraudulently purchase goods.<sup>11</sup>

Organized groups also use various techniques to mask their location. For example, they have spoofed their internet protocol (IP) addresses by using virtual private networks (VPN) to hide the location of their operations.<sup>12</sup> These groups may also conceal business information through opaque ownership structures such as shell, shelf, and fake companies, and shifting business ownership to conceal the identities of fraud scheme participants.<sup>13</sup> Organized groups may also commingle legitimate and fraudulent business activity to evade detection. In the case summarized in figure 3, for example, the organized group created dozens of

shell companies to enroll in the targeted program and to receive and launder the fraudulent proceeds.

Organized groups quickly adapt to new or additional schemes and programs, hopping between schemes and programs when their current fraud scheme is detected or when they are incentivized by additional financial gain.

**Laundering illicit funds.** Organized groups recruit and use individuals known as money mules to move fraudulently obtained funds through money laundering and other techniques to obscure their illicit origins.<sup>14</sup> They may recruit money mules to facilitate the movement of illegally obtained funds through multiple accounts, to add complexity to the money trail, evade monetary reporting requirements, and enhance the anonymity of their groups.

In addition to money laundering, organized groups employ layered financial transactions, use prepaid debit cards, and leverage digital assets to efficiently move funds to accounts where it is more difficult for law enforcement to trace and recover funds.<sup>15</sup> These groups have used money mules as well as “structuring”—breaking up fraudulently obtained funds into several smaller sums for deposit—to avoid detection across many accounts.

How does organized fraud harm people, programs, and society?

Organized fraud harms people, programs, and society in many financial and nonfinancial ways that are worsened when carried out on a large scale. (See fig. 6) The potential for large-scale harm applies not only to the number of people whose benefits are stolen but also to the number of programs harmed. According to one federal law enforcement agency, organized fraud may reach virtually every public program benefit that exists, thereby harming society as a whole.

Figure 6: Examples of How Organized Fraud Harms People, Programs, and Society

|                                                                                     | Financial harm                                                                                                                                                                                                                                         | Nonfinancial harm                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Harm to people</b>                                                               |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                              |
|  | <ul style="list-style-type: none"><li>Stolen benefits, for example, leaving low-income families unable to purchase groceries</li></ul>                                                                                                                 | <ul style="list-style-type: none"><li>Physical, for example, if unnecessary medical tests are performed on a person</li><li>Psychological, for example, as an effect of identity theft</li></ul>                                                                                             |
| <b>Harm to programs</b>                                                             |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                              |
|  | <ul style="list-style-type: none"><li>Cost to pay out fraudulent benefits or replace stolen benefits</li><li>Funds expended to detect and investigate organized fraud</li><li>Reduced ability to invest in resources to prevent future fraud</li></ul> | <ul style="list-style-type: none"><li>Delays in providing assistance</li><li>Diminished reputation and loss of public trust</li></ul>                                                                                                                                                        |
| <b>Harm to society</b>                                                              |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                              |
|  | <ul style="list-style-type: none"><li>Public funds taken out-of-state or out-of-country instead of being spent on the local economy</li><li>Higher cost of programs</li></ul>                                                                          | <ul style="list-style-type: none"><li>Limited food access in the community, for example, when a store can no longer participate in a program due to fraud</li><li>National security, for example, when relief funds are diverted to fund criminal activity, such as drugs and guns</li></ul> |

Sources: GAO analysis of Department of Justice case information and responses from federal and state officials (data); Icons-studio/stock.adobe.com (icons). | GAO-25-107508

**Financial harm to people, programs, and society.** Examples of such harm include the following:

- Stolen benefits cause financial harm to people. This occurred in the case of an organized fraud group accused of stealing over \$181 million between June

2022 and February 2024 from people receiving SNAP and Temporary Assistance for Needy Families benefits. That group did so by using card skimming devices to steal account information and fraudulently withdrawing cash or otherwise diverting funds from victims' accounts. When this type of activity happens, a person may be at the store trying to buy groceries only to find that their EBT card has been depleted.

- A person may also suffer financially if they are unemployed and unable to access UI benefits because a fraudster has already claimed the benefits using their identity.<sup>16</sup>
- Programs experience financial harm when they need to replace stolen benefits, requiring additional taxpayer funds to maintain program delivery, according to state and federal officials.<sup>17</sup>
- Society is also financially harmed when public funds are lost to fraud and withdrawn from the state or country, such as when pandemic funds were fraudulently obtained and diverted to other countries around the world.

**Nonfinancial harm to people.** Organized fraud also causes significant nonfinancial harm to people. For example, state officials told us that people may be physically harmed when unnecessary medical tests are performed on them so that fraudsters can bill Medicaid for those tests. Additionally, they said that people may also be physically harmed if they are denied necessary medical services because of an earlier fraudulent billing for those services.

Psychological harm is a concern when PII is stolen to perpetrate fraud, such as when an organized fraud group stole hundreds of identities to further their UI and Economic Impact Payment fraud schemes from January 2020 to October 2020. As we have previously reported, the emotional trauma associated with identity theft may be as devastating as many of the most violent offenses and contributes to anxiety, among other symptoms.<sup>18</sup> Identity theft victims may also be harmed again in future crimes using their stolen information.

**Nonfinancial harm to programs and society.** Organized fraud can cause nonfinancial harm to programs and society. Nonfinancial harm to programs can include reduced efficiency in aiding legitimate beneficiaries and harm to program reputation when the public loses trust in the program's ability to carry out its mission, according to state and federal officials. When one program's reputation is harmed, it may also lead the public to lose trust in all programs. Society may also be harmed by organized fraud, for example, when the only SNAP retailer in a community is disqualified from accepting SNAP benefits due to fraud, resulting in a lack of access to food for the community.

On a larger scale, national security can be threatened when organized fraud disrupts government information systems, potentially exposing sensitive information to unauthorized disclosure, alteration, and destruction. Additionally, communities and the nation's security are placed at risk when organized fraud groups use relief funds to further other criminal activity, such as activity involving drugs or guns.

---

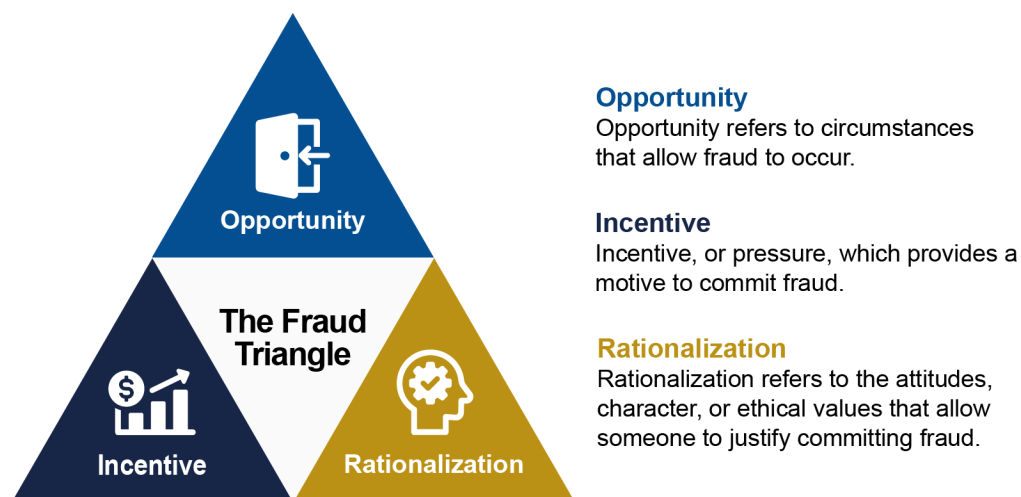
### How did organized fraud groups exploit the pandemic environment?

Organized fraud groups exploited the pandemic environment's increased opportunity, incentive, and rationalization for fraud against public programs. As we have previously reported, while fraud risk may be greatest when all three risk factors of the fraud triangle—opportunity, incentive, rationalization—are present, one or more of these factors may indicate a fraud risk.<sup>19</sup> (See fig. 7) The emergency environment and the need to distribute funds quickly resulted in an escalation and expansion of organized fraud groups targeting public programs



according to state, federal, and foreign officials we heard from, and our prior reporting.

**Figure 7: Three Risk Factors of the Fraud Triangle**



Sources: GAO figure adapted from the Department of the Treasury's *Program Integrity: The Antifraud Playbook*; Icons-Studio/stock.adobe.com (icons).  
| GAO-25-107508

**Opportunity.** Opportunity refers to circumstances that allow fraud to occur. Opportunity for fraud increased during the COVID-19 pandemic because of the infusion of funds—over \$4.6 trillion in the U.S.—provided to help the nation recover from the pandemic. For example, according to the Small Business Administration, by October 2020, the agency had disbursed an amount that was more than three times the disaster loans that it made in all years combined since the agency's creation in 1953.

Also, fewer barriers existed to accessing pandemic relief funds. For example, some programs relied on self-certification or shifted from in-person to online application processes. This shift made it easier for organized fraud groups to circumvent eligibility and identity requirements and defraud programs in large volumes and with great speed, according to federal officials we received responses from.

Aided by advancing technologies, fraudsters seized on this shift to more virtual-based processes to gather information to defraud public programs. For example, they spoofed websites mimicking legitimate UI benefit sites to harvest sensitive information. Organized fraud groups also used social media to harvest, steal, and sell information to use in schemes against public programs, advertise their services, and share methods to circumvent program controls, according to federal officials.

**Incentive.** Incentive, or pressure, can provide a motive to commit fraud. During the COVID-19 pandemic, organized fraud groups exploited public programs in part because they were high-value, low-risk targets. According to federal and state oversight officials we heard from, public programs are a low-risk target, especially compared with other illicit activity that organized criminal enterprises may be involved in, such as drug trafficking or violent crimes. Because of this environment, groups that may not previously have been in the business of defrauding public programs may have been incentivized to do so during the pandemic.

The pandemic environment contributed to individuals feeling financial pressure, which organized fraud groups could take advantage of to recruit individuals to

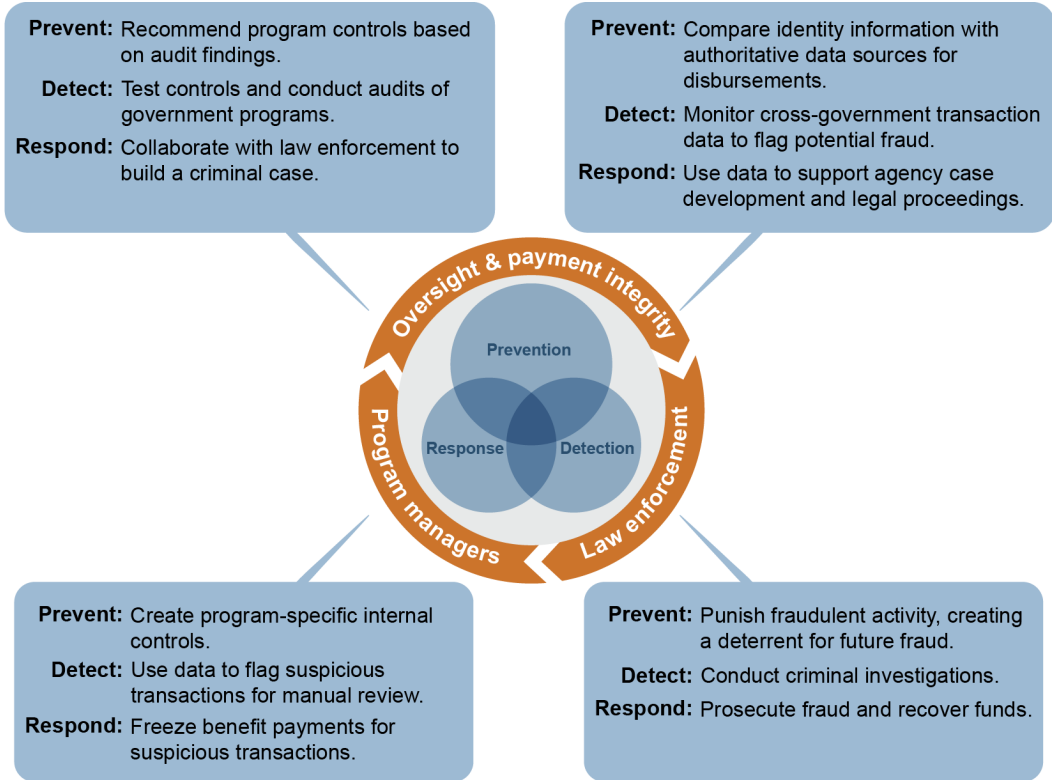
participate in fraudulent schemes. To pursue their targets, fraud groups also took advantage of the added pressure, using more aggressive tactics, such as calling customer service lines or a state representative after being denied a claim, to try to obtain the benefits or put pressure on program officials, a state official told us. Further, federal officials told us that public awareness of successful attempts to defraud public programs incentivized additional attempts. Specifically, they told us that fraudsters have celebrated their successes on social media, leading to more attempts to defraud public programs.

**Rationalization.** Rationalization refers to the attitudes, character, or ethical values that allow someone to justify committing fraud. There has been an increasing propensity for, and acceptance of, fraud, according to state and foreign officials. Instances of fraud can normalize additional fraudulent behavior, leading the public to believe that “fraud happens all the time,” that “everyone is doing it,” and they are simply getting what they are owed. Organized fraud groups, using technology, may more efficiently propagate their justifications for committing fraud and continually reinforce those attitudes within society.

What roles do federal and state agencies play in combatting fraud?

Program managers; oversight and payment integrity entities, such as auditors and comptrollers; and law enforcement at federal and state levels play roles in preventing, detecting, and responding to fraud, including fraud committed by organized groups. According to GAO’s Fraud Risk Framework, fraud prevention, detection, and response activities are interdependent and mutually reinforcing.<sup>20</sup> Figure 8 provides examples of activities to prevent, detect, and respond to fraud affecting government agencies, for each of the entities with a role.

Figure 8: Examples of Activities Government Agencies Use to Prevent, Detect, and Respond to Fraud



Sources: GAO analysis based on responses from federal and state officials and GAO reports. | GAO-25-107508  
Note: These are examples of activities and not comprehensive. For more information about fraud risk management and internal control activities, see GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 2015); and GAO, *Standards for Internal Control in the Federal Government*, [GAO-25-107721](#) (Washington, D.C.: May 2025).

**Program managers.** Program managers are responsible for administering public programs while combatting fraud. Some programs, such as SNAP, Medicaid, and UI, have both federal and state program managers with distinct responsibilities. For example, for Medicaid, federal program managers approve states' plans for administering Medicaid, while states provide day-to-day administration of benefits. If program managers detect potential fraud, they may compile case information about the suspected fraud to support oversight and refer to law enforcement for investigation.

Program managers can also take administrative action against potential fraud. At the federal level, the Centers for Medicare and Medicaid Services (CMS) may suspend payments or require prepayment reviews for providers or suppliers participating in Medicare that have acted suspiciously. For example, CMS officials described a case in which suppliers fraudulently charged for catheters to test CMS's payment process before increasing the volume and dollar amount of their fraudulent claims. Using its fraud prevention data tool, CMS reported stopping over 99 percent of the payments before they went out the door and revoked enrollment of 15 potential bad actors from Medicare, preventing over \$4.2 billion in payments, as of July 6, 2024. CMS officials noted that administrative actions, like payment suspensions, allow them to react quickly to prevent potentially fraudulent activity.

According to program managers we spoke with, their priority is to administer benefits timely and accurately, while also preventing fraud. Some examples we heard from program managers of internal control activities to prevent, detect, and respond to fraud, including fraud committed by organized groups, are to do the following:

- **Prevent:** Require that employees have a separation of duties and are given assignments and cases to review at random,
- **Detect:** Use data analytics to pause applications with suspicious characteristics for manual review, and
- **Respond:** Reset the Personal Identification Number for stolen EBT cards to mitigate theft.

UI officials from one state described using data flags to detect fraudsters that had stolen account passwords of legitimate UI beneficiaries in order to change the bank information and obtain the benefit for themselves. Officials said that in response, they contact beneficiaries to confirm whether they intended to change their bank information.

**Oversight and payment integrity entities.** Oversight entities are independent entities that combat fraud by conducting program audits or making internal control recommendations to program managers.<sup>21</sup> These entities vary by state and program in their authorities and include federal and state offices of inspectors general (OIG), auditors, comptrollers, and Medicaid Fraud Control Units (MFCU). Federal OIGs are responsible for investigations within their affiliated agencies, while state auditors and comptrollers are generally responsible for audits and financial management within their state.

Because oversight entities' authorities can span multiple states or programs, their roles are particularly useful in combatting organized fraud, which often crosses state and program lines, according to oversight officials. In particular, the Pandemic Response Accountability Committee (PRAC) brings together inspectors general from across the federal government and also works closely with state and local oversight partners.<sup>22</sup> The PRAC's unique positioning allows it to identify fraud risks across agency and program lines.<sup>23</sup>

Oversight entities use program audits to detect and respond to fraud and make recommendations to prevent future fraud. In one case, MFCU officials told us they audited for-profit nursing homes and found that the owners siphoned revenue to themselves at the expense of staff positions focused on resident health and safety. The officials recommended that the program implement preventive measures, including specifying minimum staffing levels. Oversight entities may also take steps to recover fraudulently obtained funds.

Payment integrity entities, such as the Department of the Treasury's Bureau of the Fiscal Service are responsible for supporting fraud prevention and detection by ensuring that government disbursements are secure, accurate, and legitimate. The Fiscal Service provides services at no cost to help federally funded programs—including those administered by states—address common payment integrity challenges. These services include payment eligibility verification through the Treasury's Do Not Pay portal and Account Verification Service.<sup>24</sup> According to Treasury officials, the Fiscal Service currently works with over 60 federally funded programs to provide access to these services. The Fiscal Service also monitors and shares cross-government transaction data to detect fraud and provide analytics and reporting support to oversight and law enforcement partners. In fiscal year 2024, its efforts combatting improper payments and fraud yielded \$7.2 billion in prevention and recovery, according to Fiscal Service officials.

**Law enforcement.** Law enforcement agencies are responsible for detecting and responding to fraud by conducting civil and criminal investigations, prosecutions, and recoveries. They also work to dismantle organized fraud groups and prevent the transfer of criminal funds within and outside the U.S. These activities may also prevent fraud, as the possibility of punishment discourages fraudulent behavior. At the federal level, law enforcement agencies include, for example, those within DOJ; the Department of Homeland Security (DHS); and certain OIGs. At the state level, these include the state Attorney General and local police. For example, the investigations and response related to the case summarized in figure 2 involved multiple law enforcement agencies, including those within DOJ, DHS, Treasury, and local police departments.

---

### What role does data analytics play in combatting organized fraud groups?

Federal and state agencies use a range of data analytic tools, from basic techniques like data matching to advanced techniques like network analytics, to prevent and detect threats from organized fraud groups. Data analytic tools can be used to identify indicators of fraudulent activity. According to federal and state officials, fraud indicators are generally the same for groups and individuals. However, federal and state officials stated, organized fraud groups may be distinguished by the following three indicators that may be identified using data analytics:

**Scale.** A large number of actions occurring within a short period of time. For example, groups submit thousands of applications for public benefits within a short period of time that may use similar identifying information.

**Connections.** Relationships between people, entities, or other associated data points. For example, multiple participants connected by the same PII used to obtain information on thousands of SNAP EBT cards.

**Outliers.** Data points outside of what would ordinarily be seen. An organized fraud group might submit, for example, reimbursement claims to Medicaid that are unreasonable based on geography or time.

The range of tools in figure 9—from basic to advanced—can help in preventing and detecting fraudulent activity. Advanced tools can be particularly helpful in identifying indicators of organized fraudulent activity: scale, connections, and outliers.

Figure 9: Range of Data Analytic Tools for Preventing and Detecting Fraud

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                            | Prevent                                                                                                                                                                                                                                                                                                                | Detect |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| <div>Basic</div> <div>↓</div> <div>Advanced</div> | <div>Edit checks</div> <div></div> <div>Compares data entries to requirements, and automatically denies entries that do not meet requirements or flags them for further review.</div>                                                                                                                                                                     | ✓                                                                                                                                                                                                                                                                                                                      |        |
|                                                   | <div>Data matching</div> <div></div> <div>Compares information from one source with information from another source, such as government or third-party databases, to identify any inconsistencies. Can be used to verify key information, including self-reported information and information necessary to determine eligibility.</div>                   | ✓                                                                                                                                                                                                                                                                                                                      | ✓      |
|                                                   | <div>Data mining</div> <div></div> <div>Analyzes data for connections that have not been previously discovered. Can be used to identify suspicious activity or transactions, including anomalies and other outliers, indicating potentially fraudulent activity that warrants further investigation.</div>                                                |                                                                                                                                                                                                                                                                                                                        | ✓      |
|                                                   | <div>Predictive analytics</div> <div></div> <div>Includes a variety of automated systems and tools that can be used to identify particular types of behavior before transactions are completed. Can be used to detect patterns of behavior that individually may not be suspicious, but when conducted together, can indicate fraudulent activity.</div> | ✓                                                                                                                                                                                                                                                                                                                      |        |
|                                                   | <div>Network analytics</div> <div></div> <div>Analyzes data to map relationships between people, entities, or other data points to uncover potentially unknown relationships. Also identifies “key players,” which are influential or central individuals, entities, or other data points in a network.</div>                                           | ✓                                                                                                                                                                                                                                                                                                                      | ✓      |
|                                                   | <div>Legend:</div> <div>✓ Can be used to prevent or detect fraud</div>                                                                                                                                                                                                                                                                                                                                                                     | <div><b>Prevent.</b> Stopping fraud from occurring before processing or approval. For example, flagging an application for follow-up before being approved.</div> <div><b>Detect.</b> Identifying potential fraud after a transaction was processed, such as after an application was approved and payment made.</div> |        |

Sources: GAO analysis of the GAO Fraud Risk Framework, the Chief Financial Officers Council and Bureau of the Fiscal Service Antifraud Playbook, and previous GAO reports (data); Icons-Studio/stock.adobe.com (icons). | GAO-25-107508

Note: More information about how data analytic tools can be used to prevent and detect fraud is available at GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015); and Chief Financial Officers Council and the Bureau of the Fiscal Service, *Program Integrity: The Antifraud Playbook* (Oct. 17, 2018), <https://www.cfo.gov/assets/files/Interactive-Treasury-Playbook.pdf>.

Federal and state officials told us they use these tools to identify indicators of organized fraud groups. PRAC officials, for example, told us that they have used data analytics to identify organized fraud groups and to assist OIGs, including a case where they helped to uncover nearly \$109 million in fraudulent loan applications, leading to guilty pleas in March 2025. Officials also provided the following examples of how data analytic tools can be used to identify fraud indicators.



**Edit checks to identify ineligible and suspicious transactions.** When fraudsters submit applications at or above the income level required for program eligibility, edit checks can be used to reject ineligible applicants or identify applicants for further screening.

**Data matching to identify anomalies.** When fraudsters submit applications using stolen PII or fake identities, information provided in the applications can be matched against information from established databases to verify applicant information.

**Data mining to identify suspicious connections and patterns.** Data mining can be used to identify fraud that involves, for example, billing for medical transportation trips that are unreasonable based on geography or time.

**Predictive analytics to identify outliers and anomalies.** Developing algorithms based on known organized fraud group indicators, such as indicators related to IP addresses and usernames, can help develop a predictive model to identify similar patterns of organized fraudulent activity.

**Network analytics to analyze relationships and identify connections.** A single suspicious address can be used as a starting point to identify hundreds of applicants or recipients with the same address.

Further, data analytic techniques are also used to respond to fraud. For example, during an investigation, law enforcement can map relationships between people, entities, or other information to identify key players in a group or connect individuals to identify an organized fraud group. From July 2015 through August 2023, we made 47 recommendations to federal agencies related to the use of data analytics. Of the 47 recommendations, a little more than half have been implemented as of April 2024. See appendix II.

---

**What are the challenges in preventing and detecting organized fraud?**

Officials from federal and state agencies that we received responses from cited evolving fraud tactics, data and systems silos, and efforts to balance program delivery with fraud controls as challenges to program managers, oversight and payment integrity officials, and law enforcement in preventing and detecting organized fraud. (See fig. 10).

**Figure 10: Challenges Cited by Federal and State Officials to Prevent and Detect Organized Fraud**



Sources: GAO analysis of federal and state agency responses and interviews (data); Icon-studio/stock.adobe.com (icons). | GAO-25-107508

Federal and state officials provided the following insights on these three challenges:

**Evolving fraud tactics.** Federal and state officials told us that the increased use of stolen identities from data breaches, synthetic identities, and widespread availability of advanced technological tools, such as AI and bots, will continue to pose major challenges for officials who are continuously “one step” behind organized fraud groups. Officials from one agency stated that organized groups increasingly rely on obtaining large volumes of PII from data breaches, phishing attacks, and the purchase of stolen records from the dark web. An official from another agency said that organized groups may use AI and bots to facilitate fraud schemes, allowing them to file claims in rapid succession seconds or minutes apart. The widespread availability of these tools can allow individual fraudsters to operate at a level similar to organized fraud groups.

**Data and systems silos.** Data and systems silos are created by different system architectures and legal requirements. IT system architecture can create data silos fostering an environment where fraudsters can purposely target more than one agency, according to federal and state officials. There are many different data systems, and the systems are not interoperable, according to one official. According to other officials, even when data can be obtained, data need to be cleaned to be usable and, by the time that is done, the data are outdated. These challenges can be compounded by a lack of advanced analytical tools to aid in the identification of emerging fraud schemes and modern case management systems that allow for information sharing, said officials from another agency.

Legal requirements aimed at protecting privacy and safeguarding personal records can limit information and data sharing for the purposes of preventing and detecting organized fraud. Officials from one government-wide federal oversight agency reported needing almost 70 different agreements to access the data necessary to fulfill its oversight responsibilities. Additionally, a state official told us that each program is restricted to sharing data within the program. There are also limits to interagency information sharing. For example, according to one state agency administering a federally funded state program, they are restricted by state and federal laws from sharing information among state programs, such as information on individuals and what state services they use in total. This can limit the ability to connect fraudsters to potential fraud across states and state programs. Obtaining critical data, such as tax records to verify an applicant's identity or program eligibility, while also safeguarding the data, is also time and resource intensive, according to federal officials.<sup>25</sup>

**Balancing program delivery with fraud control activities.** Multiple state program officials we interviewed discussed the challenge of balancing efficient program delivery with fraud control activities. State UI program managers discussed the challenge of needing to meet federal program requirements for timely benefit payments while also implementing fraud controls, such as identity verification. Additionally, according to a state program official, fraud impacted staff's ability to help legitimate program applicants, increasing wait times in that state.

According to GAO's Fraud Risk Framework, although pressures to deliver benefits quickly may appear at odds with fraud controls—which can slow program delivery to ensure that benefits are provided to eligible recipients in the right amount—the purpose of proactively managing fraud risks is to facilitate, not hinder, the program's mission.

---

### What kinds of actions promote prevention and detection of organized fraud?

Comprehensive fraud risk management, education, analytics, and collaboration promote organized fraud prevention and detection. Federal officials we received responses from noted that it is not possible to eliminate all risk associated with public assistance programs, but that fraud risk can be managed through a multilayered approach, using various controls and mitigation tactics. Leveraging these approaches is particularly important, given the continuing threat from organized groups, which have learned to target public programs throughout the COVID-19 pandemic.

To enhance fraud risk management, we made 173 recommendations to over 40 agency or program offices from July 2015 through August 2023. Agencies had taken actions to address 78 of these recommendations, but had yet to fully address 95 of them, as of August 2023. See appendix II for further information on our prior recommendations related to fraud risk management.

**Comprehensive fraud risk management.** As we have found in our prior work, comprehensive fraud risk management involves being prepared to manage fraud risks when the environment changes, such as during a future emergency.<sup>26</sup> Agencies were unprepared to combat the new fraud environment of the COVID-19 pandemic.<sup>27</sup> Following the leading practices in GAO's Fraud Risk Framework, for example, to regularly conduct fraud risk assessments, helps to prepare for future emergencies.<sup>28</sup> Federal, state, and foreign officials we heard from agreed that it is important to continually adapt and respond so that they are prepared for the next major fraud event.

Conducting fraud risk assessments at the program development stage, and throughout program administration, is an action that entities have used to help prevent and detect organized fraud. For example, program managers and oversight entities, such as OIGs and the PRAC, started holding “Gold Standard” meetings to discuss fraud controls before launching new programs. These meetings began in 2021 as a “lesson learned” from early pandemic relief implementation. Similarly, the United Kingdom (UK) Public Sector Fraud Authority (PSFA) said that it supports UK public entities in understanding their fraud risks and in developing and implementing preventive controls at the earliest stage of policy development.<sup>29</sup>

**Education.** Federal, state, and foreign officials we received responses from noted that increasing program managers’ awareness of potential fraud schemes through education can enable them to better prevent and detect fraud. For example, Internal Revenue Service officials noted that to stay adaptive to new fraud methods, they use capacity-building efforts, such as training staff to use sophisticated analytical tools, holding data analytics workshops, and working with public sector experts and academic institutions.

**Analytics.** Government programs can continue to promote organized fraud prevention and detection using analytic tools and data sharing. Department of Labor (DOL) OIG officials noted that fraud data analytics are particularly important for uncovering cross-state, large-scale organized fraud schemes. Multiple federal agencies offer data hubs for state agencies to cross-check whether a beneficiary has applied for or received benefits in another state.<sup>30</sup> State UI officials described using the DOL-funded Integrity Data Hub to identify claims from suspicious bank accounts, Social Security Numbers, and IP addresses for manual review.

PRAC officials noted that fraud is best dealt with when information is centralized. For example, the PRAC’s centralized data analytics center—Pandemic Analytics Center of Excellence (PACE)—has helped detect “multidipping,” where a group obtains benefits across multiple programs. As of January 2025, the PACE has supported 48 OIG and federal law enforcement partners in more than 1,000 pandemic-related investigations involving over 23,000 subjects and more than \$2.4 billion in estimated fraud loss. Similarly, the UK’s PSFA’s National Fraud Initiative collects and analyzes data from over 1,100 public and private entities to identify inconsistencies that may indicate fraud. Treasury’s cross-government analytics support offered by the Fiscal Service is yet another example. Multiple domestic program managers noted that having data from other federal and state agencies would promote fraud prevention and detection. UI officials from one state said that having access to tax return data to match to a person’s UI attestation in advance of distributing funds could help prevent fraud. For example, officials from that state reported that in November 2020, they were able to run a one-time match, which found that 380,000 people were granted UI benefits without having a recent tax return in the state.

**Collaboration.** In addition to facilitating data sharing, interagency and inter-governmental collaboration can help prevent, detect, and respond to organized fraud.

*Interagency collaboration:* Combatting organized fraud can require the coordinated efforts of multiple agencies.<sup>31</sup> For example, the COVID-19 Fraud Enforcement Task Force (CFETF) brought together oversight entities and law enforcement officials from different federal agencies to investigate and prosecute fraud committed against pandemic programs, including organized fraud. CFETF established five multiagency task forces that include federal

inspectors general and law enforcement officials, with the stated goal of combatting the most impactful criminal pandemic fraud cases, often involving multiple CARES Act programs, foreign actors, violent perpetrators, or large loss amounts.<sup>32</sup> Additionally, as the federal government's central disbursing entity, Treasury's Fiscal Service collaborates with numerous federal agencies to support fraud prevention and detection.

*Inter-governmental collaboration:* Because federal and state entities may have related responsibilities but different access to information, coordination between levels of government is helpful in antifraud efforts.<sup>33</sup> Both law enforcement and oversight officials we spoke with reported that it can be difficult to determine which entity, whether federal, state, or local, might pursue a fraud case. To address this challenge, DOJ's Organized Crime Drug Enforcement Task Force officials—whose work includes combatting organized fraud threats—described its Fusion Center that works on case coordination and deconfliction by sharing information across investigating agencies. Further, state program managers we spoke with noted that their federal counterparts could play a useful role in sharing best practices and lessons learned from other state program managers.

---

## Agency Comments

We provided a draft of this report to DHS, DOJ, and Treasury for review and comment. We incorporated technical comments from DHS, DOJ, DOL, and Treasury as appropriate.

---

## How GAO Did This Study

To answer these questions, we conducted a literature review; reviewed relevant fraud cases and other documentation; and interviewed and obtained written responses from selected federal, state, and foreign entities.

Specifically, we conducted a literature review of relevant documentation covering the past 10 years, including GAO and other government publications, scholarly articles, and news reports related to organized fraud. To describe characteristics of organized fraud and provide examples of organized fraud cases, we also reviewed DOJ press releases published in the last 10 years and related Public Access to Court Electronic Records documents.

For inclusion in the scope of this review, we selected federal programs based on our prior work involving pandemic-relief programs, program budget, and relevant information regarding program fraud prevalence, for example, from GAO reports and DOJ press releases. In selecting the public assistance programs, we considered criteria, such as the size of the program's budget and whether the program was adjusted, for example, to reduce program controls or expand benefit coverage, during the COVID-19 pandemic. We define public assistance programs as those that provide either cash assistance or in-kind benefits, such as a good or service, from any governmental entity, to include social welfare and social insurance programs. Selected programs include over 20 public assistance programs that are federally administered, for example, Economic Impact Payments and Medicare, and those that are state administered (Medicaid, SNAP, and UI).

We selected federal entities that either (1) oversaw the programs in scope or (2) had a law enforcement or oversight role related to organized fraud. The eight federal agencies we selected based on the programs in scope are the Departments of Agriculture, Education, Health and Human Services, Homeland Security, Labor, and Treasury; and the Small Business and Social Security Administrations. The 12 agencies we selected based on their law enforcement or oversight roles were the Departments of Justice and State, the Office of



Management and Budget, Pandemic Response Accountability Committee, and OIGs for the eight federal agencies that oversaw the selected programs.

We selected six states that administer Medicaid, SNAP, and UI programs, and which could provide various perspectives on program integrity functions and activities. For example, we identified states in which state auditors, inspectors general, and antifraud entities have a program integrity role. We also reviewed information about the number of reported fraud investigations related to those programs. Based on this review, we initially selected four states: Florida, Michigan, New York, and Washington. We selected an additional two states—Tennessee and Wisconsin—using the same criteria to supplement information on the SNAP program after we were unable to obtain responses from SNAP program administrators for two of the initially selected states. For each selected program, we interviewed officials and requested written responses to questions about their perspectives on organized fraud and roles and responsibilities related to program integrity and oversight.

To gather international perspectives on public sector fraud committed by organized groups, we reviewed literature and interviewed counter-fraud officials from selected countries. Specifically, we interviewed counter-fraud officials from Australia, Canada, and the United Kingdom, with whom GAO collaborates as part of the International Public Sector Fraud Forum.<sup>34</sup> We also interviewed counter-fraud officials from the European Union and INTERPOL Washington, a component of the DOJ which serves as a liaison between the nation's domestic law enforcement agencies and the International Criminal Police Organization, commonly known as INTERPOL.

Lastly, we interviewed officials representing national associations, specifically, the United Council on Welfare Fraud; the National Association of State Auditors, Comptrollers and Treasurers; state officials recommended by the Association of Inspectors General; and the National Association of Medicaid Fraud Control Units.

The characteristics of organized fraud that we describe in this report are not intended to be an exhaustive list. Similarly, examples of roles, data analytic tools, challenges, and actions to promote organized fraud prevention and detection described in this report are not intended to present a comprehensive, detailed analysis of all such roles, tools, challenges, and actions that may exist with regard to managing organized fraud risk in public programs.

We conducted this performance audit from April 2024 to July 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## List of Addressees

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

The Honorable Mike Crapo  
Chairman

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

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

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

The Honorable Tom Cole  
Chairman  
The Honorable Rosa L. DeLauro  
Ranking Member  
Committee on Appropriations  
House of Representatives

The Honorable Brett Guthrie  
Chairman  
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 Robert Garcia  
Ranking Member  
Committee on Oversight and Government Reform  
House of Representatives

The Honorable Jason Smith  
Chairman  
The Honorable Richard Neal

Ranking Member  
Committee on Ways and Means  
House of Representatives

We are sending copies of this report to the appropriate congressional committees; the Secretary of the Department of Homeland Security, the Attorney General of the United States, the Secretary of the Treasury; and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

---

## GAO Contact Information

For more information, contact: Rebecca Shea, Director, Forensic Audits and Investigative Service, [SheaR@gao.gov](mailto:SheaR@gao.gov).

Public Affairs: Sarah Kaczmarek, Managing Director, [Media@gao.gov](mailto:Media@gao.gov).

Congressional Relations: A. Nicole Clowers, Managing Director, [CongRel@gao.gov](mailto:CongRel@gao.gov).

**Staff Acknowledgments:** Toni Gillich, Irina Carnevale (Assistant Directors), Yue Pui Chin (Analyst in Charge), John Mac Emery, Colin Fallon, Sarah Florino, Nicole Mackowski, Joseph Rini, and Claire Rueth.

Connect with GAO on [Facebook](#), [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).  
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).

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

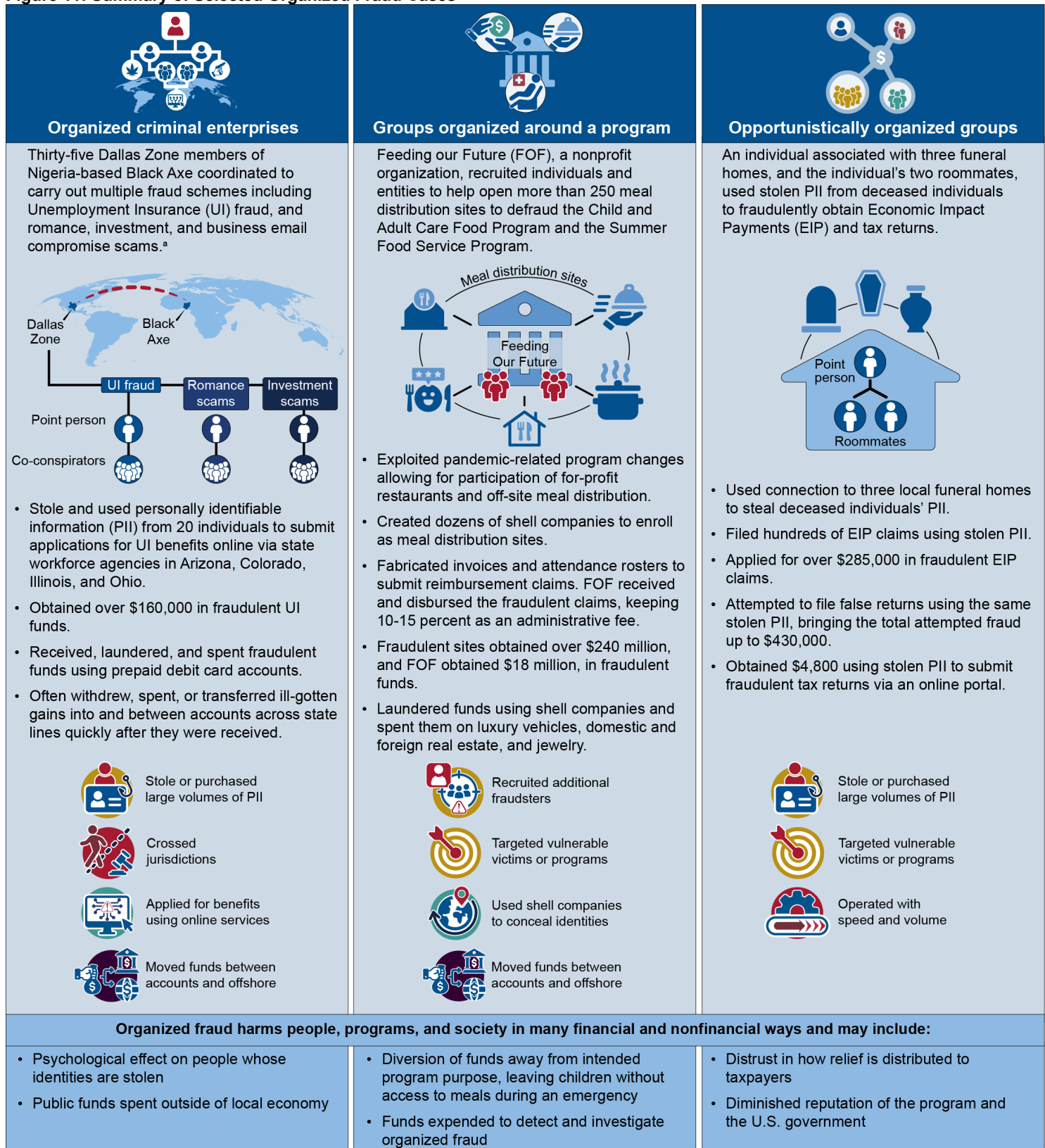
This is a work of the U.S. government but may include copyrighted material. For details, see <https://www.gao.gov/copyright>.

---

## **Appendix I: Summary of Selected Organized Fraud Cases**

Figure 11 summarizes examples of fraud schemes perpetrated by three types of organized fraud groups—organized criminal enterprises, groups organized around a program, and opportunistically organized groups. The summaries include descriptions of the organized groups, the programs they targeted, how they carried out the fraud schemes, and examples of the potential harm they caused.

**Figure 11: Summary of Selected Organized Fraud Cases**



Sources: GAO analysis of Department of Justice case information (data); Icons-Studio, Yusiki, stock.adobe.com (graphics). | GAO-25-107508

<sup>a</sup>Black Axe is a transnational crime syndicate originating in Nigeria. The syndicate has leadership at the international, national, and local level and is generally broken down into city-specific zones. International leadership consists of a President and High Council of Elders; national leadership consists of a National Body; and local leadership consists of a Zonal Executive Council, Zonal Elder Council, and Zone Leader. The Zone Leader leads members within the zone, some of whom serve in specialized roles. For example, a Chief Ihaza acts as a treasurer; a Chief Eye acts as a secretary; and a Chief Butcher acts as the security officer, with there being some additional roles in some zones.



## Appendix II: GAO Recommendations to Enhance Fraud Risk Management

Since the issuance of GAO's Fraud Risk Framework in 2015, we have made numerous recommendations to enhance fraud risk management across federal programs. These include recommendations that federal agencies and programs align their activities with leading practices in fraud risk management, such as by assessing fraud risks and using data analytics. From July 2015 through August 2023, we made 173 recommendations to over 40 agency or program offices related to fraud risk management. As of August 2023, agencies had taken actions to address 78 of these recommendations but had yet to fully address the remaining 95.<sup>35</sup>

From July 2015 through August 2023, we made 47 recommendations to federal agencies related to the use of data analytics, such as using data matching to verify self-reported information. Using data analytics to manage fraud risks is one of the leading practices in fraud risk management and can facilitate prevention and detection of organized activity. Of the 47 recommendations, a little more than half have been implemented, as of April 2024.<sup>36</sup>

Federal agencies have seen benefits by mitigating fraud risks and implementing data analytics while continuing to take steps to make data and tools available for fraud data analytics. For example:

At the Small Business Administration (SBA):

- In June 2020, we recommended that SBA implement plans to respond to risks in the Paycheck Protection Program (PPP), help ensure program integrity, and address potential fraud.<sup>37</sup> In response, SBA developed a loan review process in December 2020. As of the end of fiscal year 2023, we estimated that SBA's use of additional safeguards in the PPP and other COVID-19 programs resulted in more than \$12 billion in savings.
- In May 2023, we reported on fraud risks, including from organized groups, in SBA pandemic relief programs. We recommended that SBA ensure it (1) has mechanisms in place and utilizes them to facilitate cross-program data analytics and (2) identifies external sources of data that can facilitate the verification of applicant information and the detection of potential fraud across its programs.<sup>38</sup> SBA agreed with these recommendations and has taken steps to perform cross-program data analytics and to pursue verification tools and data sharing with the Department of the Treasury. However, as of May 2025, these recommendations remained open, pending SBA's documentation of its policy and plan, among other actions.<sup>39</sup>

At the Federal Aviation Administration (FAA):

- In March 2020, we reported on fraud and abuse risks in aircraft registrations, including from organized groups. We recommended that FAA ensure that information on aircraft owners and other key information is recorded in a format that facilitates data analytics.<sup>40</sup> In June 2024, as part of its IT modernization, FAA made that information available in searchable PDF format, which facilitates data analytics.
- In the same report, we also recommended that FAA use data collected as part of IT modernization—such as sanctions data and postal addresses—to identify and analyze patterns of activity indicative of fraud or abuse, including from organized groups, to support monitoring and risk-based oversight. FAA agreed with the recommendation. As of December

2024, FAA was still implementing its Civil Aviation Registry Electronic Services system, which would provide greater flexibility to query system transactions to track specific data and trends associated with aircraft registration.

We have also identified actions that Congress can take to further improve the federal government's capabilities to manage fraud risks. In March 2022, we recommended 10 matters for congressional consideration, including the following three matters that would help mitigate the risks of fraud, including from organized groups.<sup>41</sup> All 10 remained open as of May 2025.

- Congress should establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud.
- Congress should reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports.
- 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.

---

## Endnotes

---

<sup>1</sup>While allegations in an indictment are accusations that have not been proven, we have used the inclusion of conspiracy charges in cases that ended with a conviction on any charges as a flag for organized group activity.

<sup>2</sup>GAO, *COVID Relief: Consequences of Fraud and Lessons for Prevention*, [GAO-25-107746](#) (Washington, D.C.: Apr. 9, 2025). The UI system includes UI programs that were established prior to the COVID-19 pandemic, which we refer to as "regular" UI programs, and programs established in response to the COVID-19 pandemic, which we refer to as "temporary" UI programs: Pandemic Unemployment Assistance, Federal Pandemic Unemployment Compensation, Pandemic Emergency Unemployment Compensation, and Mixed Earner Unemployment Compensation.

<sup>3</sup>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>.

<sup>4</sup>Nation-state actors, such as China, Iran, North Korea, and Russia, are well-resourced and engage in sophisticated malicious cyber activity that is targeted and aimed at prolonged system intrusion. Nation-states may use more sophisticated fraud schemes, have entire government units dedicated to defrauding the U.S., and can maintain greater operational stealth compared to many other organized criminal enterprises, according to a federal official.

<sup>5</sup>PII is information that can be used to distinguish or trace the identify of an individual.

<sup>6</sup>A synthetic identity is a combination of real and fabricated personally identifiable information where the implied identity is not associated with a real person.

<sup>7</sup>Phishing is the fraudulent practice of sending emails or other messages purporting to be from a legitimate company or official government office to induce individuals to reveal personal information.

<sup>8</sup>Policies that allow an individual to qualify for benefits in many programs once they demonstrate eligibility in just one program are typically known as broad-based categorical eligibility policies.

<sup>9</sup>Social engineering is a form of deception that uses human psychology to target and manipulate individuals and make them more susceptible to fraud.

<sup>10</sup>A bot, or internet robot, is a computer software that operates over networks, such as the internet, and is made to automate certain tasks to simulate human activity.

---

<sup>11</sup>For additional information on trafficking and recipient eligibility fraud related to SNAP, see GAO, *Supplemental Nutrition Assistance Program: Observations on Employment and Training Programs and Efforts to Address Program Integrity Issues*, [GAO-18-504T](#) (Washington, D.C.: May 9, 2018). For additional information on skimming related to SNAP, see U.S. Department of Agriculture, Food and Nutrition Service, *Supplemental Nutrition Assistance Program (SNAP) Electronic Benefit Transfer (EBT) Theft* (Nov. 26, 2024).

<sup>12</sup>A VPN establishes an encrypted connection between a computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that masks the IP address of the computer. Spoofing is a mechanism that uses deliberately falsified information to appear to be from a legitimate source. Fraudsters can spoof their IP address to make their IP address appear as a legitimate source.

<sup>13</sup>Shell companies are corporations or limited liability companies that have no physical presence beyond a mailing address, generate little-to-no independent economic value, and help conceal the company's true ownership while providing the true owners with complete control over the organization. Shelf companies are formed and then placed aside for years to give the appearance of business longevity and legitimacy, as the length of time that a shelf company has been in existence adds legitimacy to the entity. Shelf companies are a form of shell company until they are used for real economic activities.

<sup>14</sup>A money mule is an individual that transfers illegally acquired money—either wittingly or unwittingly—on behalf of, or at the direction of, another.

<sup>15</sup>Money laundering generally is the process of converting proceeds from illicit activities into funds and assets in the financial system that appear to have come from legitimate sources. Money mules have been associates of organized groups and have consisted of both knowing and unwitting participants.

<sup>16</sup>According to the Department of Labor (DOL), the agency took steps to help address this issue. For example, DOL issued guidance to states to promote, among other things, identity verification. DOL also developed an unemployment fraud reporting website to help people understand unemployment identity fraud and to provide resources to help those experiencing such fraud.

<sup>17</sup>For SNAP, there is no longer authority at the federal level to replace stolen SNAP EBT benefits after December 20, 2024.

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

<sup>19</sup>[GAO-25-107746](#).

<sup>20</sup>GAO, *A Framework for Managing Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

<sup>21</sup>Some oversight entities may also have law enforcement authorities. For example, the Inspector General Act of 1978, as amended, and the Legislative Branch Inspectors General Independence Act of 2019 generally authorize criminal investigators in the offices of certain inspectors general to exercise law enforcement powers, including carrying a firearm while conducting official duties and seeking and executing federal warrants for arrest.

<sup>22</sup>In March 2020, Congress created the Pandemic Response Accountability Committee (PRAC) as part of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act). PRAC's mission is to promote transparency and use data to detect fraud, waste, abuse, and mismanagement. The PRAC and its data analytics center are scheduled to sunset on September 30, 2025, unless Congress takes action. GAO has recommended that Congress establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud. 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).

<sup>23</sup>PRAC's Blueprint for Enhancing Program Integrity highlights strategies for federal and state program managers to develop, implement, and maintain strong internal controls, even during emergencies. Pandemic Response Accountability Committee, *Blueprint for Enhanced Program Integrity Chapter 1: Best Practices for Strengthening Federal Programs* (May 2024).

---

<sup>24</sup>Payment eligibility verification is an examination of payment data such as whether the payment is being made to a proper account, whether the name of the accountholder aligns with the intended payee, and other financial integrity data elements. Payment eligibility verification does not independently assess program participation eligibility. The initial determination of whether an intended payee is eligible for participation in a program is determined by the agency administering that program.

<sup>25</sup>As discussed above, the Fiscal Service provides services at no cost to help federally funded programs—including those administered by states—address common payment integrity challenges. These services include payment eligibility verification through the Treasury’s Do Not Pay portal and Account Verification Service.

<sup>26</sup>[GAO-15-593SP](#); and GAO, *Fraud Risk Management: Key Areas for Federal Agency and Congressional Action*, [GAO-23-106567](#) (Washington, D.C.: Apr. 13, 2023).

<sup>27</sup>GAO, *Emergency Relief Funds: Significant Improvements Are Needed to Address Fraud and Improper Payments*, [GAO-23-106556](#) (Washington, D.C.: Feb. 1, 2023).

<sup>28</sup>[GAO-15-593SP](#).

<sup>29</sup>The UK Public Sector Fraud Authority is the UK government’s center of expertise on the management of public sector fraud whose mission includes developing capability in the public sector to find, prevent, and respond to fraud.

<sup>30</sup>The UI Integrity Data Hub, which is funded by DOL and administered by the National Association of State Workforce Agencies, shares UI data across states and is free for use by state workforce agencies. The U.S. Department of Health and Human Services created the Public Assistance Reporting Information System (PARIS). PARIS is a data matching service that checks to see if a recipient has received benefits in two or more states.

<sup>31</sup>GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, [GAO-23-105520](#) (Washington, D.C.: May 24, 2023).

<sup>32</sup>CFETF has resulted in over 3,500 defendants criminally charged, over 400 civil settlements and judgments, and over \$1.4 billion in fraudulently obtained CARES Act funds seized or forfeited, according to its April 2024 report. Department of Justice, *COVID-19 Fraud Enforcement Task Force 2024 Report* (Washington, D.C.: April 2024).

<sup>33</sup>PRAC provides guidance highlighting lessons learned from federal, state, and local collaboration in pandemic relief program implementation and oversight. Pandemic Response Accountability Committee, *Blueprint for Enhanced Program Integrity Chapter 4: Whole-of-Government Approach* (April 2025).

<sup>34</sup>The forum was established in 2017 by government officials from Australia, Canada, New Zealand, the United Kingdom, and the United States. The goal of the forum is to use shared knowledge to reduce the risk and harm of fraud and corruption in the public sector across the world.

<sup>35</sup>GAO, *Fraud Risk Management: Agencies Should Continue Efforts to Implement Leading Practices*, [GAO-24-106565](#) (Washington, D.C.: Nov. 1, 2023).

<sup>36</sup>GAO, *Fraud and Improper Payments: Data Quality and a Skilled Workforce Are Essential for Unlocking the Benefits of Artificial Intelligence*, [GAO-25-108412](#) (Washington, D.C.: Apr. 9, 2025).

<sup>37</sup>GAO, *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts*, [GAO-20-625](#) (Washington, D.C.: June 25, 2020).

<sup>38</sup>[GAO-23-105331](#).

<sup>39</sup>GAO, *Priority Open Recommendations: Small Business Administration*, [GAO-25-108048](#) (Washington, D.C.: May 1, 2025).

<sup>40</sup>GAO, *Aviation: FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration*, [GAO-20-164](#) (Washington, D.C.: Mar. 25, 2020).

<sup>41</sup>[GAO-22-105715](#).