United States Government Accountability Office

Report to Congressional Requesters

April 2025

CONSUMER PROTECTION

Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams

GAO-25-107088

GAO Highlights

Highlights of GAO-25-107088, a report to congressional requesters

April 2025

CONSUMER PROTECTION

Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams

Why GAO Did This Study

Scams, a method of committing fraud, involve the use of deception or manipulation intended to achieve financial gain. Scams often cause individual victims to lose large sums—in some cases their entire life savings.

GAO was asked to review federal agencies' and businesses' efforts to counter scams. This report examines, among other things, the extent to which (1) a comprehensive, government-wide strategy guides agency efforts; (2) selected federal agencies compile scam-related complaint data and agencies' ability to estimate the total number of scams and related dollar losses; and (3) selected agencies measure the effectiveness of consumer education activities.

GAO analyzed publicly available information, agency documents, and agency consumer complaint data. GAO interviewed agency officials and representatives of relevant industries and advocacy groups.

What GAO Recommends

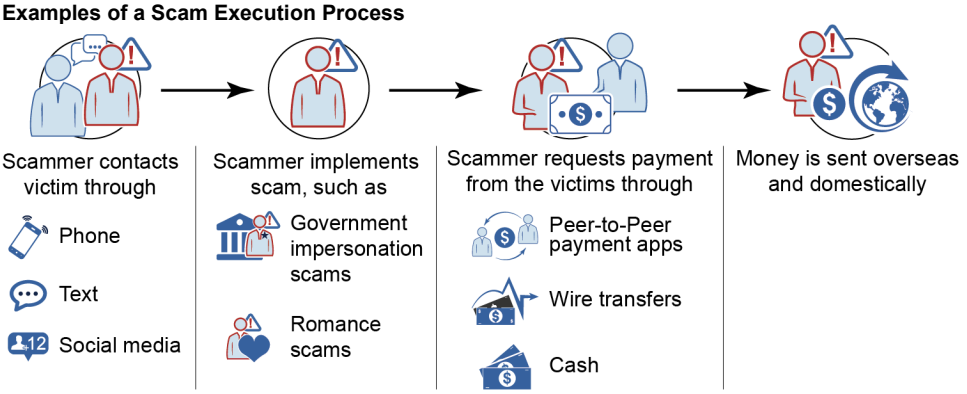
GAO is making 16 recommendations to various agencies to develop a government-wide strategy to counter scams, a national scam estimate, a common definition of scams, and evaluate the outcomes of consumer education efforts. The FBI disagreed with three recommendations related to the development of a national estimate, a definition of scams, and evaluating the outcomes of its consumer education efforts. GAO maintains the recommendations are valid, as discussed in the report. FTC neither agreed nor disagreed with the five recommendations made to it.

View GAO-25-107088. For more information, contact Seto J. Bagdoyan at bagdoyans@gao.gov and Howard Arp at arpj@gao.gov.

What GAO Found

Scams occur in a variety of forms, have evolved with technology, and are a growing risk to consumers. Commonly, scams involve a scammer contacting the victim, engaging the victim with a particular type of scam, and requesting a payment for a false purpose.

Examples of a Scam Execution Process



Sources: GAO analysis of publicly available information on scams, including from the Federal Trade Commission and Federal Bureau of Investigation; Icons-Studio, sdecoret/stock.adobe.com, GAO (icons). | GAO-25-107088

Note: Other types of contact methods, scams, and payment methods exist.

The 13 federal agencies GAO spoke with engage in a range of efforts to counter scams. However, none were aware of a government-wide strategy to guide those efforts. Existing strategies did not focus on countering scams and did not apply across agencies. The Federal Bureau of Investigation (FBI) is developing a cyber-enabled fraud strategy. The overlap in issues relating to scams and cyber-enabled fraud could provide FBI with the expertise to develop a government-wide strategy. Developing a government-wide strategy would better position agencies to coordinate and strategically target their efforts to counter scams.

The Consumer Financial Protection Bureau (CFPB), FBI, and Federal Trade Commission (FTC) receive, compile, and report on consumer complaints pertaining to issues including internet-related crime and scams. Data limitations, such as issues with how data are collected, do not allow agencies to calculate the exact number of scam complaints, but each agency can estimate the number it receives. For example, the FBI estimated that in 2023 it received approximately 589,400 scam-related complaints, resulting in losses of $10.55 billion. In addition, no government-wide estimate of the total number of scams and dollar losses exists. Improved data collection and estimates would better support federal efforts to understand the extent of this type of crime and develop ways to counter it.

CFPB, FBI, and FTC provide a variety of education resources for consumers. However, they do not measure the effectiveness of their education efforts on the consumers that receive them. Doing so would help the agencies understand how their education efforts are affecting consumers' ability to recognize and protect themselves from scams and how the agencies might adjust their education materials to best help consumers.

Contents

Table

Figures

Abbreviations

BBB	Better Business Bureau
CFPB	Consumer Financial Protection Bureau
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
FCS	Financial Crimes Section
HSI	Homeland Security Investigations
IC3	Internet Crime Complaint Center
OCC	Office of the Comptroller of the Currency
MSB	money services business
PIN	Personal Identification Number
P2P	Peer-to-Peer
Sentinel	Consumer Sentinel Network

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

April 8, 2025

The Honorable Elizabeth Warren
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Kirsten Gillibrand
Ranking Member
Special Committee on Aging
United States Senate

Scams have been around for many years, have evolved with technology, and are a growing risk to consumers in the United States and around the world. Scams are one method of committing fraud that involve the use of deception or manipulation intended to achieve financial gain.[1] In perpetrating various scams, scammers deceive victims into making a payment or providing information to make a payment to benefit the scammer. These payments are often made via, but not limited to, Peer-to-Peer (P2P) payment apps, gift cards, and wire transfers.[2] In addition to inflicting emotional distress, scams have caused individual victims to lose tens of thousands of dollars, and, in some cases, their entire life savings. Although there is no government-wide estimate of the total amount lost to scams, as discussed later in this report, experts and available data indicate that scams may be costing Americans billions of dollars annually.

[1]For this report, we are using the term "scams" as defined in the Federal Reserve Scam Classifier Model. The model defines scams as the use of deception or manipulation intended to achieve financial gain. Federal Reserve, *Scam Classifier Model* (June 2024), https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/. ScamClassifier℠ is a service mark of the Federal Reserve Banks. GAO defines fraud as obtaining something of value through willful misrepresentation. As discussed later, this report highlights specific types of scams that include impersonation scams and investment scams, among others. These scams are included in the Scam Classifier Model but are not an exhaustive list of all current and other types of scams that may evolve in the future.

[2]P2P payment apps allow consumers to send and receive money from mobile devices through a linked bank account. A gift card is a plastic card or other payment code or device that is purchased on a prepaid basis; issued at a specific amount; and redeemable at a single merchant or an affiliated group of merchants that share the same name, mark, or logo. A wire transfer is a way to send money electronically to a domestic or an international recipient.

Criminal organizations throughout the world operate using networks of scammers. According to the United Nations, organized crime groups that facilitate certain scams continue to expand their operations and increase the sophistication of scams.[3] In an example highlighting the scope and reach of this issue, a 2023 international police operation against online financial crime, including scams, resulted in over 3,000 arrests and the seizure of $300 million worth of assets across 34 countries, including the United States.[4] Likewise, in the United States, the Department of Justice (DOJ) has identified the involvement of transnational criminal organizations that have taken hundreds of millions of dollars from Americans through scams.

Multiple federal agencies seek to prevent and respond to scams through efforts that include educating consumers, receiving complaints, investigating cases, and bringing law enforcement actions. We were asked to review the efforts of federal agencies and businesses to counter scams. This report

1. describes federal agencies' activities to prevent and respond to scams and evaluates the extent to which there is a comprehensive, government-wide strategy to guide their efforts;
2. evaluates the extent to which federal agencies compile scam-related consumer-complaint data and are able to estimate the total number of scams and related financial losses;
3. describes federal agencies' efforts to educate consumers about scams and evaluates the extent to which they measure their effectiveness;
4. describes selected private businesses' efforts to counter scams; and
5. describes actions by federal agencies and selected private businesses to respond to consumer complaints related to scams.

[3]United Nations Office on Drugs and Crime, *Casinos, cyber fraud, and trafficking in persons for forced Criminality in Southeast Asia* (September 2023), https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.

[4]Interpol, *USD 300 million seized and 3,500 suspects arrested in international financial crime operation* (Dec. 19, 2023), https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation.

To describe federal agencies' activities to prevent and respond to scams, we reviewed documentation and interviewed officials from 13 agencies, including the

- Consumer Financial Protection Bureau (CFPB),
- Federal Bureau of Investigation (FBI) and the Executive Office for United States Attorneys within DOJ,
- Federal Trade Commission (FTC),
- Federal Reserve (Board of Governors of the Federal Reserve System and Federal Reserve Payment Services), and
- the Financial Crimes Enforcement Network (FinCEN) within the Department of the Treasury.[5]

We identified these agencies by reviewing publicly available information describing their work related to scams.

To evaluate the extent to which a comprehensive, government-wide strategy exists across federal agencies to prevent and respond to scams, we asked officials from each of the 13 agencies if they were aware of any such strategy. We also reviewed existing U.S. strategies, such as those related to cyberthreats and fraud and money laundering, to determine whether any of these strategies may serve as a comprehensive, government-wide strategy to counter scams. Further, we reviewed strategies, developed by foreign countries, specifically intended to counter scams. We reviewed these strategies to understand what types of information had been included in the strategies. We identified these strategies through a review of publicly available information and attendance at the Global Anti-Scam Alliance summit in 2023.[6] We also interviewed the Consumer Federation of America, the Retail Gift Card Association, and a financial institution to discuss federal government coordination and strategies.[7]

[5]See app. I for the list of the 13 agencies that were part of this review. App. II contains descriptions of the 13 agencies' missions.

[6]The Global Anti-Scam Alliance is an international knowledge-sharing organization composed of government, law enforcement, consumer protection groups, and the private sector.

[7]These industry experts and consumer organizations were selected based on our review of publicly available information regarding scams and referrals made by other organizations.

To evaluate the extent to which federal agencies compile scam-related consumer complaint data, we obtained information from three federal agencies that told us they receive and report on consumer complaints related to scams: CFPB, FBI, and FTC. We obtained documents, interviewed officials, and reviewed their publicly available data, including reports specifically addressing scams.

To evaluate the extent to which federal agencies use scam-related consumer complaint data to estimate the full extent of scams and dollar losses, we held additional discussions with officials at CFPB, FBI, and FTC. We met with these agencies because they produce publicly available annual reports that contain data on scams and associated losses derived from the consumer complaint data they receive. Further, we reviewed our previous work related to the importance of knowing and understanding the scope of fraud in managing fraud risk.[8]

To describe federal agencies' efforts to educate consumers about scams and evaluate the extent to which they measure the effectiveness of such efforts, we reviewed documentation from the 13 agencies discussed above. We had additional discussions with officials, specifically from CFPB, FBI, and FTC, to better understand the extent to which they measure the effectiveness of their consumer education activities. We focused on these three agencies because they provide consumer education materials directly to a broad range of consumers. We also reviewed our previous work related to program outcomes that can help federal agencies effectively manage and assess the results of their training efforts.[9]

To describe the efforts of selected private businesses to counter scams, we met with seven businesses. We met with two P2P payment app service providers, two gift card issuers, one money services business (MSB), and two financial institutions.[10] We selected these businesses based on various criteria, such as the ownership structure of the business

[8]GAO, *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments*, GAO-24-105833 (Washington D.C.: Apr. 16, 2024).

[9]GAO, *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts,* GAO-23-105460 (Washington, D.C.: July 12, 2023).

[10]An MSB is generally an institution engaging as a business in the transfer of funds as a money transmitter or offering check cashing; foreign currency exchange services; or selling money orders, travelers' checks or prepaid access (formerly stored value) products.

and efforts to counter scams. The information obtained from these interviews is illustrative and cannot be generalized to other businesses.

As part of this objective, we selected and visited, unannounced, a nongeneralizable sample of 68 locations of eight different gift card retailers across eight states and the District of Columbia to observe gift card scam warning signs that may be voluntarily posted at gift card displays.[11] These retailers included grocery stores, hardware stores, department stores, and pharmacies. The results of our site visits are specific to the retailer location visited and cannot be projected to all gift card retailers.

To describe actions taken by federal agencies and selected businesses to respond to consumer complaints related to scams, we interviewed officials from CFPB, FBI, and FTC. We focused on these agencies because they receive complaints directly from consumers and produce reports based on these data. We also interviewed the seven selected businesses about their actions to respond to consumer complaints.

We conducted covert scenarios to obtain information on the experiences of consumers of varying demographics, including older adults, who report scams to selected federal agencies and businesses.[12] As part of implementing our covert scenarios, we filed complaints to agencies and businesses stating that we were deceived into making a payment as part of a scam. We executed different scenarios where we were the victims of different types of scams, such as government impersonation and investment scams, among others. We also selected a nongeneralizable sample of P2P payment apps, gift card issuing companies, and MSBs as scam payment methods used for our covert scenarios. We submitted consumer complaints to CFPB, FBI, and FTC, as well as to a nongeneralizable selection of four gift card issuers and a nonbank wire transfer company.[13] We did this to determine what initial action the

[11]Federal law does not require gift card retailers to post fraud warning signs in retail stores. Some states, however, have enacted laws and regulations that may require certain signage. We did not assess for compliance with state laws.

[12]This report refers to persons 60 and older when using the term “older adults.” This definition is consistent with the requirements in Section 2(1) of the Elder Abuse Prevention and Prosecution Act, which references Section 2011 of the Social Security Act (42 U.S.C. 1397j(5)) (defining “elder” as an individual age 60 or older).

[13]The P2P payment app businesses blocked our attempted transactions, citing suspicious activity on the accounts. Therefore, we did not submit scam complaints to P2P payment app businesses or P2P-related complaints to federal agencies.

agencies and selected businesses take when an individual informs them that they have been the victim of a scam.[14] The results of our covert scenarios are for illustrative purposes and cannot be projected to the outcomes of other consumer complaints or responses by agencies and entities.

See appendix I for a detailed description of our scope and methodology.

We conducted this performance audit from October 2023 to April 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. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Background

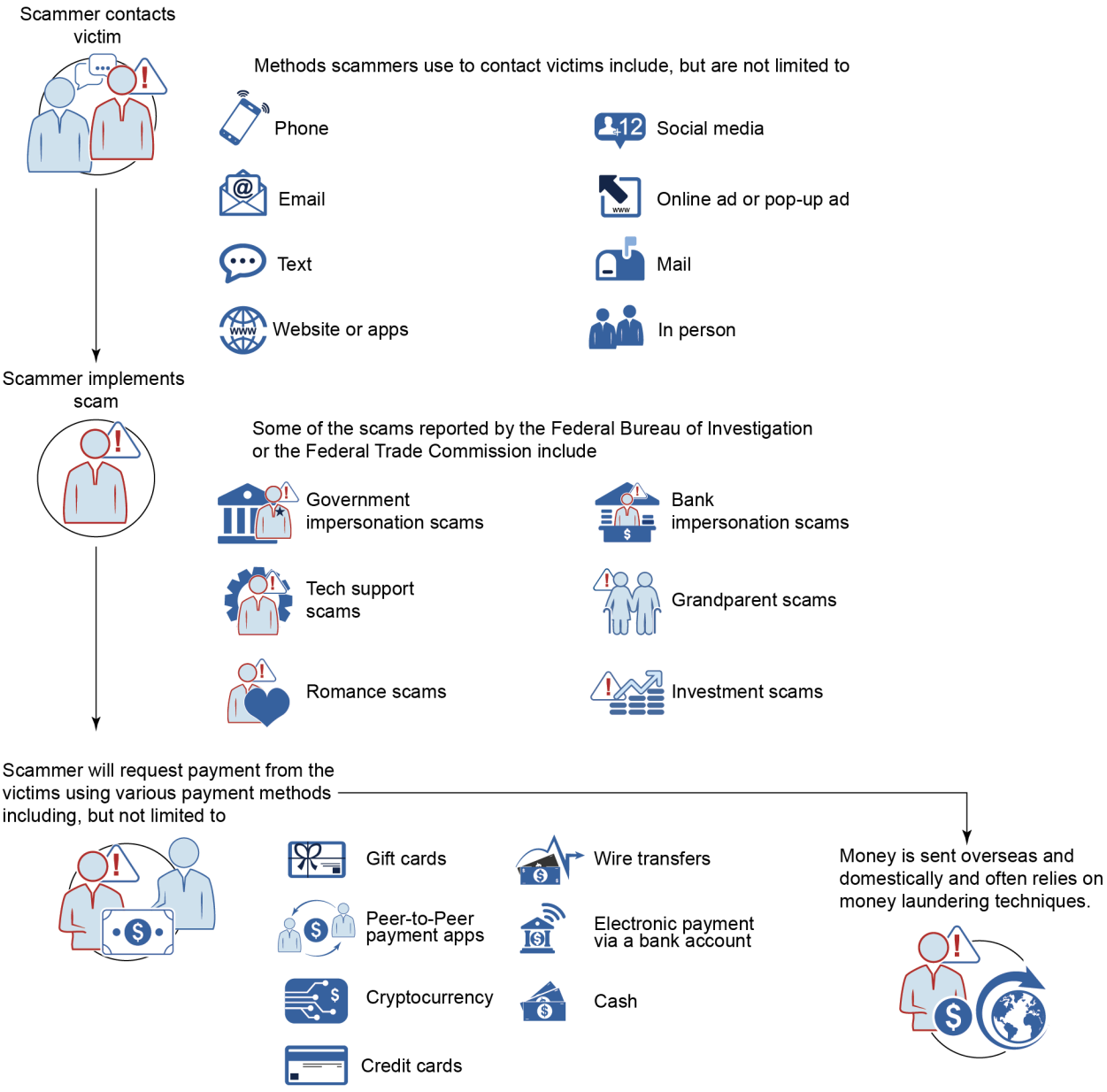
Characteristics of Scams, Victims, and Scammers

Scams involving the use of information technology have been around for decades. In an early common scheme, text messages were sent to consumers requesting that funds be sent to someone purporting to be a family member. By 2008, tech support scams, as discussed below, began to appear and have proliferated since that time. According to our analysis of publicly available information, scams currently occur in a wide variety of forms. In many instances, scams involve a scammer contacting the victim, through means such as text message or social media; engaging the victim with a particular scam; and requesting a payment, such as a wire transfer, for a false purpose. Figure 1 illustrates how many scams may be conducted.

[14]We reviewed what initial step these businesses undertook when scams were reported. We did not investigate how these businesses implement error resolution responsibilities under applicable law.

Figure 1: Common Examples of the Scam Execution Process

Scams can be carried out by individuals and bad actors, including criminal networks operating both outside the United States and domestically.



Sources: GAO analysis of publicly available information on scams, including from the Federal Trade Commission and Federal Bureau of Investigation; Icons-Studio, sdecoret/stock.adobe.com, GAO (icons). | GAO-25-107088

Victim information. Scammers may obtain victim information, including their name and address, through various sources. These include fake solicitations to the victim via autodialing software (robocalls and robotexts), data breaches, marketing lead lists, social media, open-source information, and information-sharing by scamming networks.[15] In some cases, the scam may seem more believable because the scammer already has some of the victim's personal information.

A 2024 DOJ study found there was no statistically significant difference between the percentage of persons aged 60 or older and persons aged 59 or younger who experienced fraud in 2017.[16] However, older adults are more likely to experience greater losses and are less likely to report scams. According to FTC, older adults, or persons aged 60 and older are less likely to report losing money to fraud compared with younger adults aged 18 to 59. FTC's most recent fraud survey, published in October 2019, also found that what it called the "rate of victimization" for the various categories of frauds included in the survey was generally lower for those 65 and older than for younger consumers. However, older adults report greater individual median losses than younger adults.[17] As discussed later in this report, in response to laws enacted by Congress, FTC has initiatives designed specifically to help older adults avoid scams. Additional resources or specialized personnel are sometimes employed by agencies or businesses to respond to older victims, but the resolution process generally remains the same as for other victims.[18]

Contact methods. Depending on the type of scam, the contact method may include phone calls, social media, in-person, email, or text. When

[15]Robocalls are calls made with an autodialer or that contain a message made with a prerecorded or artificial voice. Robotexts are text messages sent to a mobile phone, using an autodialer.

[16]Department of Justice, National Institute of Justice, *Examining Financial Fraud Against Older Adults* (Mar. 20, 2024), https://www.ojp.gov/library/publications/examining-financial-fraud-against-older-adults. The National Institute of Justice is the research, development and evaluation agency of the U.S. Department of Justice.

[17]Federal Trade Commission, *Protecting Older Consumers 2023-2024* (Oct. 18, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf.

[18]There are financial elder abuse-type laws issued by states that provide for specialized procedures for responding to suspected financial abuse of older adults. We did not review the states' financial elder abuse laws because it was outside the scope of our work.

phone calls are used, scammers may spoof caller identification information to hide their identity. Specifically, a consumer's caller identification may incorrectly indicate a call is coming from a government agency or other legitimate entity.

Scam implementation. Scammers may use a script to appear legitimate and create a sense of urgency to pressure or scare individuals into sending money immediately. Alternatively, some scams, such as romance scams, can take months to build a trusting relationship before the scammer asks for money.

In July 2024, we reported on fraudulently induced payments.[19] We noted that the use of artificial intelligence and deepfake technology lend credibility to scams by enabling criminals to hide their identities, and we described how some scammers use artificial intelligence to make scams harder for the victims to detect. This technology can be exploited by scammers to alter voices, images, and video to impersonate family, friends, or business officials.

Scam types. Scammers are constantly finding new ways to scam victims. CFPB, FBI, and FTC have identified numerous types of scams. Figure 2 provides a nonexhaustive listing of scam types.

[19]GAO, *Payment Scams: Information on Financial Industry Efforts*, GAO-24-107107 (Washington, D.C.: July 25, 2024).

Figure 2: Examples of Scam Types

Types of scams

 Government/business impersonation	Government/business impersonation scams occur when the scammer fraudulently identifies as a government or business official to manipulate or steal from the victim.
 Tech support	Tech support scams occur when the scammer poses as technical or customer support/service. For example, the tech support scammer may trick an individual with a pop-up window that appears on the individual's computer that might look like an error message from the operating system. The pop-up window will direct the individual to call the tech support team. The scammer, pretending to be a tech support team member, will request money to provide assistance.
 Grandparents	Grandparent scams involve a scammer impersonating a family member, usually a grandchild, of an older adult or someone who says the family member is in trouble. The scammer claims that money is immediately needed to assist the family member.
 Romance	Romance scams occur when a scammer adopts a fake online identity to gain a victim's affection (romantic or platonic) and trust and then uses the illusion of a romantic or close relationship to manipulate or steal from the victim.
 Investment	Investment scams involve a scammer offering low- or no-risk investments, guaranteed returns, overly consistent returns, complex strategies, or unregistered securities to manipulate or steal from the victim.
 Business compromise	Business email compromise scams involve a scammer targeting a business or individual and taking over an official account or using email spoofing to attempt to redirect payments to an illicit account controlled by the fraudster to steal from the victim.
 Lottery/sweepstakes/ inheritance	Lottery/sweepstakes/inheritance scams occur when an individual is contacted about winning a lottery or sweepstakes they never entered or to collect on an inheritance from an unknown relative.

Sources: GAO Antifraud Resource and analysis of Consumer Financial Protection Bureau, Federal Bureau of Investigation, and Federal Trade Commission information; Icons-Studio/stock.adobe.com, bsd studio/stock.adobe.com, sdecoret/stock.adobe.com, GAO (icons). | GAO-25-107088

Payment methods. The scammer may obtain funds from the victim by requesting payment through methods such as P2P payment apps; electronic payment via a bank account, wire transfer, check, cash, cryptocurrency, precious metals; or providing gift card numbers and Personal Identification Numbers (PIN).[20] Below are characteristics of some frequently used payment methods employed by scammers to obtain funds from victims, as cited by FTC reports.

- P2P payment apps allow consumers to quickly send and receive money. Depending on the payment provider, a P2P payment can be initiated from a consumer's online bank account portal, or a mobile app. According to FTC, scammers rely on P2P payment apps because transfers happen quickly and, once the individual sends the money, it is difficult to get it back.
- Gift cards hold specific cash value that can be used for payments for goods and services. Scammers can request that individuals purchase a gift card and ask for the gift card number and PIN. Scammers deceive their victims by telling them, for example, that the gift card number is to pay the government for taxes or fines, pay for tech support, or for some other fictitious reason. The gift card number and PIN allow the scammers to access the funds that their victim has loaded onto the card.
- A wire transfer occurs where, typically, funds are sent electronically from one person or entity to another. A wire transfer can be initiated through a financial institution or through a nonfinancial institution provider, such as an MSB. The transfer can be domestic or international.

In our July 2024 report, we discussed how fraudulently induced payments occur when a person with payment authority is manipulated or deceived into making a payment for the benefit of the scammer.[21] We found that financial institutions are generally not required under federal law to reimburse consumers for losses stemming from a fraudulently induced payment because the payment was authorized by a person with payment authority on the account (i.e., the owner of the account or other authorized person). Financial institutions and P2P payment companies

[20]The scams we focus on above generally involve victims initiating a payment to the scammer themselves or voluntarily providing a scammer with bank account, gift card, or other credentials. A PIN is a type of password that may be used by stored value card holders, among others, to gain access to their funds or transaction and balance information.

[21]GAO-24-107107.

provide consumer education and staff training to help identify and avoid potential scams. Additionally, some institutions and payment apps have put in place measures to slow down payments to provide the consumer an opportunity to verify the legitimacy of the payment. Industry representatives we interviewed for our 2024 report recommended a multisector approach, to include telecommunications and social media companies, as well as law enforcement, to address fraudulently induced payments.

Scammers. Scams can be carried out by individuals and bad actors, including criminal networks operating both outside the United States and domestically. Multiple domestic law enforcement investigations have identified criminals operating from international call centers working to scam Americans. For example, scammers in foreign-based call centers have called Americans and falsely identified themselves as federal law enforcement officers or other government officials to request that victims send money to avoid arrest or other economic consequences. The funds that criminals obtain from these scams may be linked to other illicit activities, such as human trafficking and drug trafficking.

According to the United Nations Office on Drugs and Crime, transnational organized crime groups have built large organizations to perpetrate sophisticated scams.[22] Specifically, transnational criminals have trafficked hundreds of thousands of victims and forced many of them to work in "scam compounds" and conduct scams through the internet. These criminals also conduct mass recruitment of professionals with information technology expertise and pay them a salary. Some of the scam operations have developed training manuals and scripts that individuals are made to follow to commit the scams, according to the United Nations Office of the High Commissioner.[23]

Consumer Complaints About Scams

Multiple federal agencies receive complaints, some of which involve scams, directly from consumers. Different agencies may have authority

[22]United Nations Office on Drugs and Crime, *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia* (September 2023), https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.

[23]United Nations, Office of the High Commissioner, *Online Scam Operations and Trafficking Into Forced Criminality in Southeast Asia: Recommendations for A Human Rights Response* (2023), https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf.

over different matters impacting the public. Federal agencies receive complaints through their websites and may also receive complaints through phone, fax, or mail.

We identified eight federal agencies (of the 13 total agencies in our review) that receive complaints from consumers about scams:[24]

- **CFPB.** Receives consumer complaints about financial products or services, including money transfers, cryptocurrency, and prepaid cards. The CFPB complaint process is discussed in greater detail later in the report.
- **FBI.** Within FBI, the Internet Crime Complaint Center (IC3) receives consumer complaints related to internet crime, including identity theft, data breaches, and scams.[25] FBI officials told us that in addition to submitting complaints to IC3, consumers can file complaints to FBI field offices. The IC3 complaint process is discussed in greater detail later in the report.
- **Federal Deposit Insurance Corporation (FDIC).** Receives consumer complaints about financial institutions that it regulates. Consumer complaints made to the agency could include issues related to scams. Consumers can provide information on the specific financial institution where the victim's money is held and a narrative with additional information.
- **Federal Reserve.** Receives complaints about financial institutions and forwards them to the appropriate federal regulator or to the

[24]When receiving complaints, federal agencies may refer consumers to other agencies. Also, according to FinCEN officials, the agency does not receive scam complaints directly from consumers. Rather, FinCEN receives Suspicious Activity Reports from financial institutions that might signal criminal activity, which could include scams. FinCEN uses Suspicious Activity Reports and other reports to provide financial intelligence about illicit finance. FinCEN may also receive referrals from federal law enforcement agencies to support investigations or to assist in interdicting, freezing, or recovering funds. This list is not comprehensive. Other federal agencies may receive complaints about scams, such as the Social Security Administration and the U.S. Department of Veterans Affairs, when scams are generally related to their programs or benefits.

[25]FBI defines internet crime as any illegal activity involving one or more components of the internet, such as websites, chat rooms, and email. Internet crime involves the use of the internet to communicate false or fraudulent representations to consumers. According to FBI, these crimes may include, but are not limited to, advance-fee schemes, business email compromise, computer hacking, confidence/romance scams, employment/business opportunity scams, government impersonation scams, identity theft, investment scams, lottery/sweepstakes/inheritance scams, nondelivery of goods or services, and tech support scams.

appropriate Reserve Bank.[26] Federal Reserve officials stated that consumers can submit complaints about scams involving financial institutions where the victim's money is held. According to the Federal Reserve, internet fraud complaints are referred to IC3, consumer fraud complaints are referred to FTC, and mail fraud complaints are referred to the U.S. Postal Inspection Service.[27]

- **FTC.** Receives consumer complaints about fraud or scams, and bad business practices, including those in the financial services area.[28] FTC receives reports directly from the public via its website and through its call center and from various contributors. Its consumer complaint process is discussed in greater detail later in the report.
- **Homeland Security Investigations (HSI).** Receives tips from the public through a hotline. Officials stated that tips are sent to specific Department of Homeland Security units based on the nature of the tip or the information provided. The tip hotline allows individuals to report information on any of HSI's investigative areas, such as financial crime, cybercrime, human trafficking, and narcotics smuggling, and is not specific to scams. In addition, tips and complaints can be reported to local HSI Field Offices. HSI works with task forces, which consist of state, local, federal, and private sector partners in identifying and combatting fraud.
- **Office of the Comptroller of the Currency (OCC).** Receives consumer complaints about financial institutions that it regulates. According to OCC officials, complaints made to the agency could include issues related to scams involving financial institutions where the victim's money is held. Consumers can provide information on a specific financial institution that is the subject of the complaint and a narrative with additional information. OCC stated that the agency is unable to process complaints where the complainant is not a customer of the financial institution that is the subject of the complaint.
- **Secret Service**. Individuals can report crimes to a local Secret Service field office. However, Secret Service officials told us they do

[26]The 12 Federal Reserve Banks are one of the three parts of the Federal Reserve System. The 12 regional Reserve Banks are the operating arms of the Federal Reserve and work as a system to conduct the nation's monetary policy and ensure a stable financial system.

[27]The U.S. Postal Inspection Service enforces federal statutes related to crimes that involve the postal system, its employees, and its customers. Areas within its scope include identity theft, mail fraud, cybercrime, and fraud prevention and education.

[28]When collecting consumer complaints, FTC does not distinguish between fraud and scams.

not have a formal system in place to specifically receive scam complaints like FBI and FTC. The Secret Service's investigative areas include financial crimes, cybercrimes, and counterfeit currency investigations and are not specific to scams. The Secret Service has field office-based Cyber Fraud Task Forces, whose mission is to prevent, detect, and mitigate cyber-enabled financial crimes. According to the Secret Service, these task forces work with state and local law enforcement agencies and financial institutions to combat cybercrime and scams.

When receiving complaints, federal agencies may refer consumers to state and local agencies and businesses.[29] For example, according to FTC, it advises most consumers reporting financial losses to report the problem to the company operating the payment system involved so that the consumer can get a refund, if possible, and to make sure the company knows about the fraudulent transaction on its system and can act accordingly. In addition, according to FTC, depending on the type of report, it may also tell consumers they can contact their state attorney general or local consumer protection agency. Other agencies that take consumer complaints may refer these complaints to one of the eight agencies above.

In addition to filing complaints with federal agencies, older adults can receive assistance reporting scams and other financial crimes from DOJ's National Elder Fraud Hotline. Further, individuals can report scams to nonprofit consumer organizations, such as AARP and the Better Business Bureau (BBB), that may share information with federal agencies.

Multiple Agencies Engage in Activities to Counter Scams, but No Comprehensive, Government-wide Strategy Guides Their Efforts

At least 13 federal agencies engage in a range of activities related to countering scams perpetrated against victims. In this regard, each agency has its own mandate and authority, with each largely pursuing independent activities related to countering scams.

Several agencies formally and informally coordinate their efforts with other agencies and consumer and other associations, including when providing consumer education or by sharing consumer-complaint information. However, these efforts are not coordinated across all the agencies we identified on a formal, government-wide basis. Further, there is no single, comprehensive, government-wide strategy for guiding efforts to counter scams.

[29]Individuals can also report scams directly to state and local agencies.

Selected federal agencies and industry groups offered their views about the need for such a strategy, while some foreign countries, such as the United Kingdom, have developed and implemented strategies to counter scams. The absence of a comprehensive, government-wide strategy poses a risk for potential fragmentation of effort among agencies and overlap of their activities to counter scams, which risks diminishing their efficiency and effectiveness.

Multiple Agencies Engage in Activities to Prevent and Respond to Scams

Officials from the 13 federal agencies we spoke with indicated they were engaged in a range of activities related to countering scams. These activities cover a spectrum of roles intended to prevent, detect, and respond to scams.

We asked officials from these agencies whether their agency engaged in any of 11 different activities specifically related to countering scams. Each agency stated they engaged in some form of preventative activities, such as consumer education or outreach (for example, publishing consumer alerts and articles related to fraud and scams). About half of the agencies stated they engaged in information-gathering activities, such as recording or reporting on scam complaints. Similarly, most of the agencies stated that they take some form of action to respond to or investigate scams. Investigation activities range from reviewing consumer complaints to supporting legal action by the agency to assisting other law enforcement entities with information gathering and research. Figure 3 below shows the activities agencies told us they take to counter scams.

Figure 3: Federal Agency Activities to Counter Scams

	Education	Advocacy	Outreach	Coordination	Recording	Reporting	Research	Regulation	Enforcement	Investigation	Prosecution
Consumer Financial Protection Bureau	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Department of Health and Human Services	✓	—	✓	—	—	—	—	—	—	—	—
Department of State	✓	—	✓	✓	—	—	—	—	—	—	—
Federal Bureau of Investigation[a]	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	—
Federal Deposit Insurance Corporation	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	—
Federal Reserve Board	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	—
Federal Trade Commission	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Financial Crimes Enforcement Network[b]	✓	✓	✓	✓	✓	✓[d]	✓	✓	✓	✓	—
Homeland Security Investigations[c]	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	—
National Credit Union Administration	✓	—	—	—	—	—	✓	—	✓	—	—
Office of the Comptroller of Currency[b]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—
Office of the United States Attorneys[a]	✓	✓	✓	✓	—	—	—	—	✓	✓	✓
U.S. Secret Service[c]	✓	—	✓	✓	✓	—	—	—	✓	✓	—

Legend: ✓ = Yes; — = No

Source: GAO compilation and analysis of agency interview responses. | GAO-25-107088

Note: Activity definitions

Education: Agency provides education materials or programing regarding scams to consumers and businesses.

Advocacy: Agency provides information to policymakers or performs advocacy in policy areas affected by scams.

Outreach: Agency conducts outreach or distributes notifications regarding scams to consumers and businesses (e.g., warnings/advisories).

Coordination: Agency collaborates with other agencies to address scam issues.

Recording: Agency receives and records complaints regarding scams.

Reporting: Agency regularly collects and reports on scams or provides statistics for related issues/scams.

Research: Agency conducts research and produces reports regarding scams.

Regulation: Agency promulgates regulations that affect scam issues.

Enforcement: Agency enforces laws or regulations that affect scam issues.

Investigation: Agency leads, or assists with, the investigations of complaints/scams.

Prosecution: Agency undertakes criminal or civil prosecutions of scams.

[a]Component of the Department of Justice

[b]Component of the Department of the Treasury

[c]Component of the Department of Homeland Security

[d]According to Financial Crimes Enforcement Network (FinCEN) officials, the agency does not receive scam complaints directly from consumers. Rather, FinCEN receives Suspicious Activity Reports from financial institutions that might signal criminal activity, which could include scams.

Some Agencies Coordinate Activities to Counter Scams

Although at least 13 federal agencies engage in activities related to countering scams perpetrated against victims, each agency has its own mandate and authority, with each largely carrying out activities related to countering scams independently. However, in some instances, agencies coordinate efforts, such as by providing consumer education or by sharing consumer complaint information. Some of these efforts are implemented through official bodies intended to address crimes against older adults.

In an example of coordination, FTC maintains the Consumer Sentinel Network (Sentinel). Sentinel, a collaborative effort involving 46 contributors including FBI, is a consumer-complaint reporting database made accessible to law enforcement agencies. (We discuss Sentinel later in this report.) Similarly, Treasury's FinCEN supports law enforcement investigations by providing financial intelligence and, at times, investigation support. CFPB officials noted that some federal agencies engage in informal discussions and complaint sharing to monitor and identify emerging trends and issues.

Legislation has been enacted to improve formal coordination in countering scams. Specifically, in 2022, Congress enacted the Stop Senior Scams Act, requiring the establishment of an older-adult scam prevention advisory group. The group consists of representatives from across federal government and law enforcement agencies; consumer

advocacy organizations; and the gift card, MSB, retail, and telecommunications industries, among others.[30] With a focus on older adults, the advisory group is to collect information on materials that industry uses to educate employees on identifying and stopping scams. The group is then to identify any inadequacies or deficiencies with those materials and create models, best practices, or guidance documents to help address deficiencies.

In response to the Stop Senior Scams Act, in 2022, FTC established the Scams Against Older Adults Advisory Group. The advisory group focused on four main areas, and each area was led by a separate committee: (1) expanding consumer education and outreach efforts, (2) improving industry training on scam prevention, (3) identifying innovative or high-tech methods to detect and stop scams, and (4) reviewing research related to scam prevention messaging and making recommendations for future research.

Since its establishment, the full Scams Against Older Adults Advisory Group held two meetings, one in September 2022 and a second in April 2024. According to FTC, the committees met regularly from December 2022 to early 2025. They also issued deliverables, such as (1) a reference sheet on principles to better reach people with messages that help them spot and avoid fraud; (2) a document outlining principles for effective industry training on scam prevention; (3) a report summarizing what research has shown to be effective in scam prevention messaging, challenges to that messaging, and where additional research is needed; and (4) a document identifying state laws that allow banks or brokerages to hold or freeze a transaction when fraud is suspected, which may help prevent a scammer from obtaining consumer funds.[31]

Further, according to FTC officials, other multiagency government-wide initiatives exist to address insidious and pervasive scams. Specifically, FTC participates in government-wide collaboration to address fraud, including through the Global Anti-Fraud Enforcement Network, the Elder

[30]Pub.L.No. 117-103, Div. Q, Title 1, Subtitle A,136 Stat. 809 (2022).

[31]The advisory group's work products are available to the public at ftc.gov/olderadults. Additional information about the advisory group's work is described in the FTC's annual older adults report. Federal Trade Commission, *Protecting Older Consumers 2023-2024.*

Justice Coordinating Council, and the COVID-19 Fraud Enforcement Task Force.[32]

According to FBI, it counters scams through coordinated activity with foreign, federal, state, and local law enforcement through joint investigations, tasks forces, and the public and private sectors through working groups. FBI officials noted that there are initiatives to counter elder abuse, neglect, and financial exploitation, including scams, and that scams are being investigated by other federal agencies, such as HSI. The initiatives to counter elder fraud, including scams, include DOJ's Elder Justice Initiative. This initiative is a program that works to counter elder abuse, neglect, and financial exploitation, including scams. Additionally, the DOJ Consumer Protection Branch leads a cross-agency domestic elder justice working group, and the Transnational Elder Fraud Strike Force investigates and prosecutes individuals and organizations engaging in foreign-based scams that disproportionately affect American seniors.[33] Further, FBI participates in international law enforcement working groups addressing scams. According to FBI, it has dedicated personnel in the identified epicenters of romance scams and confidence and tech support scams. These personnel lead coordination efforts with local law enforcement and specifically address elder fraud from abroad—intelligence collection, and coordinated operational activity to disrupt, dismantle, and deter the syndicates, and recover victim funds.

According to HSI, the agency is committed in the fight against fraud and has engaged in multi-initiative workforce groups in developing a national strategy. Along with FBI and other law enforcement partners, HSI works with private sector partners, such as financial institutions, and regulatory agencies, such as the Commodity Futures Trading Commission,

[32]The Global Anti-Fraud Enforcement Network is an organization that aims to identify the threats posed by international fraud schemes and to collaborate to pursue the offenders and disrupt their activities. The Elder Justice Coordinating Council was established by the Elder Justice Act in 2010 to coordinate activities related to elder abuse, neglect, and exploitation across the federal government. The Attorney General established the COVID-19 Fraud Enforcement Task Force to coordinate responses related to identifying, investigating, and punishing COVID-19 fraud.

[33]According to FBI, the Strike Force is comprised of attorneys and analysts from the Department of Justice's Consumer Protection Branch and 20 U.S. Attorney's Offices. The FBI, U.S. Postal Inspection Service, and HSI provide dedicated resources for identifying the most harmful elder fraud schemes and bringing perpetrators to justice. Special Agents from the Internal Revenue Service, U.S. Secret Service, Defense Criminal Investigative Service, Social Security Administration Office of Inspector General, and Treasury Inspector General for Tax Administration also conduct Strike Force investigations.

international partners, and DOJ in combatting scams, to include romance scams, cryptocurrency scams, elder fraud, and other types of scams.

There Is No Comprehensive, Government-wide Strategy to Guide Agency Activities to Specifically Counter Scams

Officials with the 13 federal agencies we spoke to noted that they were not aware of a single, comprehensive, government-wide strategy to guide federal efforts to counter scams. Our own review of existing strategies did not identify any that are specifically focused on countering scams. A national strategy is a type of interagency coordination mechanism—typically, a document or initiative—that provides a broad framework for addressing issues that cut across federal agencies and other levels of government and sectors.[34] Three agencies and the White House have strategies that address various aspects of scams but do not provide government-wide direction.

We identified four strategies—developed by Treasury, FBI, FTC, and the White House—that focus on illicit financing, cyber-enabled fraud, unfair and deceptive acts or practices, and transnational organized crime, respectively. Our review of the four strategies found that, although each addresses activities related to scams, the strategies do not focus on scams. We also found that none of the strategies functions as a single, comprehensive, government-wide strategy to counter scams nor were any of them intended to.

- **U.S. Department of the Treasury 2024 National Strategy for Combating Terrorist and Other Illicit Financing.** In 2024, the U.S. Department of the Treasury published a national strategy for countering terrorist and other illicit financing, which includes fraud. The strategy identifies efforts to strengthen tools and authorities against illicit finance and outlines specific actions some agencies will

[34]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

take to support these priorities.[35] Unlike the 2022 national strategy, the 2024 strategy explicitly identifies the misuse of money orders, prepaid cards, and P2P payments in its discussion of illicit finance vulnerabilities. However, it does not include a discussion of efforts to counter scams government-wide because the focus of the strategy is illicit financing in general.

- **FBI cyber strategy.** In September 2020, FBI published a 2-page cyber strategy that presents the agency's cyber vision and mission to raise risk awareness and impose consequences on cyber adversaries through authorities, capabilities, and partnerships.[36] The cyber strategy does not discuss efforts to counter scams at a government-wide level. According to FBI officials, the agency's Cyber Division focuses on criminal and nation-state cyber intrusions and also noted that scams were not included as cases to be addressed under the strategy.

According to FBI officials, the agency considers scams to be a financial crime; the primary responsibility for addressing this activity falls under the FBI Criminal Investigative Division, Financial Crimes Section (FCS). However, because scams are often cyber-enabled, crossover exists within the 2020 Cyber Strategy, specifically the descriptions of capabilities and partnerships. The strategy also highlights the asset recovery team, discussed later in this report, which can assist victims that meet certain criteria in recovering financial losses related to cybercrime, which may

[35]U.S. Department of the Treasury, *2024 National Strategy for Combating Terrorist and Other Illicit Financing* (May 2024), https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf. The 2024 strategy addresses the key risks discussed in the National Money Laundering, Terrorist Financing, and Proliferation Financing risk assessments. The Department of the Treasury's 2024 National Money Laundering Risk Assessment references scams, such as investment scams, as a threat. The 2024 National Money Laundering Risk Assessment examines the current money laundering environment and identifies the ways in which criminal and other actors seek to launder funds. U.S. Department of the Treasury, *2024 National Money Laundering Risk Assessment* (February 2024), https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf; *2024 National Terrorist Financing Risk Assessment* (February 2024), https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf; and *2024 National Proliferation Financing Risk Assessment* (February 2024), https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf. Illicit finance refers to the movement of money across borders that is illegal in its source (e.g. corruption, smuggling), its transfer (e.g., tax evasion), or its use (e.g., terrorist financing).

[36]Federal Bureau of Investigation, *FBI Cyber Strategy,* https://www.ic3.gov/PSA/2020/PSA201008.pdf.

include scams. Further, the strategy states that no single agency or government can counter cyber threats alone.

- **FTC Strategic Plan for Fiscal Years 2022-2026.** FTC officials cited Goal 1 of its Strategic Plan for 2022-2026 as its strategy to counter scams.[37] Goal 1 addresses unfair and deceptive acts or practices, which include scams. Under Goal 1, the plan describes several objectives, including
  - identifying, investigating, taking actions against, and deterring unfair or deceptive acts or practices that harm the public;
  - connecting with individuals, communities, and businesses to provide practical knowledge, guidance, and tools and to learn about key challenges and opportunities for future FTC engagement; and
  - collaborating with domestic and international partners to enhance consumer protection.

As described in the plan, FTC stated it provides access to analytical tools through Sentinel to enable law enforcement agencies to target investigations, identify witnesses, and uncover details about scam operations, such as payment methods, contact methods, and sales pitches. However, while the plan does specifically address efforts to counter scams, its focus is limited to the FTC's efforts. As such, it does not serve as a single, comprehensive, government-wide strategy to counter scams.

- **White House Strategy to Combat Transnational Organized Crime.** In December 2023, the White House released an update to its 2011 strategy to respond to the shifting strategic environment of transnational organized crime.[38] The strategy targets the dispersions of illicit finance pathways by encouraging law enforcement to increase its use of FinCEN reporting to inform investigations. Additionally, it seeks to counter cyber-enabled fraud capabilities by engaging with the private sector to craft educational messaging to counter fraud schemes. While this strategy has objectives related to elements of scams, the strategy focuses on organizations that engage in

[37]Federal Trade Commission, *Strategic Plan for Fiscal Years 2022-2026 (February 2025 Update)*, https://www.ftc.gov/system/files/ftc_gov/pdf/fy-2022-2026-ftc-strategic-plan-2025-update.pdf.

[38]White House, *2023 White House Strategy to Combat Transnational Organized Crime* (December 2023).

transnational crime, with the bulk of its strategic objectives addressing issues, such as intelligence sharing and border security, to counter other aspects of transnational organized crime.

In July 2024, FBI informed us that its FCS is developing a "cyber-enabled fraud strategy" to identify, target, and disrupt the most prolific transnational criminal enterprises defrauding U.S. citizens. FBI noted that the FCS has established resources to contribute to mitigating the cyber-enabled fraud threat across agencies and has working relationships with strategic partners to leverage the cyber-enabled fraud program, such as FinCEN, FTC, CFPB, and several DOJ components. FBI did not have a timeline for when the strategy will be finalized and implemented. Even when completed, the strategy may not serve as a comprehensive, government-wide strategy because, as an FBI-focused strategy, it may not address the roles, responsibilities, and authorities of other agencies or contain all the characteristics of a national strategy.

According to FBI, in December 2024, the FBI's Criminal Investigative Division established the Cyber-Enabled Fraud & Money Laundering Unit to prioritize and resource FBI cyber-enabled fraud investigations. The Cyber-Enabled Fraud & Money Laundering Unit defines cyber-enabled fraud as traditional fraudulent activities that are facilitated or enhanced by digital technology, the internet, and electronic communications such as cryptocurrency scams, romance scams, tech fraud scams, and other scam typologies. The strategic goal of the Cyber-Enabled Fraud & Money Laundering Unit is to disrupt and dismantle cyber-enabled fraud actors and the ecosystem that supports them by leveraging strategic partnerships with the U.S. Intelligence Community, private sector, and international law enforcement. Public outreach and education are also part of the Cyber-Enabled Fraud & Money Laundering Unit strategy to counter the cyber-enabled fraud threat.

Selected Federal Agencies' Perspectives on a Comprehensive, Government-wide Strategy to Counter Scams Differ

FTC and Treasury officials shared their view with us on a single, comprehensive, government-wide strategy to counter scams.

- According to FTC officials, no single agency has the jurisdiction and authorities to tackle the diversity of fraud and scams in the marketplace government-wide. They stated that a government-wide strategy could help overcome those jurisdictional barriers, if significant resources could be applied to tackle multifaceted and evolving scams. FTC added that any comprehensive, government-wide strategy must include a focus on criminal and civil law enforcement.

- Treasury officials noted that many law enforcement and other agencies have overlapping mandates when it comes to fraud and scams, and a fully coordinated law enforcement strategy may in practice be difficult to coordinate and implement between agencies. Further, Treasury officials noted that to have a government-wide strategy to coordinate efforts to counter scams would involve several key agencies, such as CFPB, FBI, FTC, and Treasury.

We also asked CFPB and FBI for their views on a government-wide strategy to counter scams. Neither offered specific views on such a strategy. FBI officials, however, noted that cyber-enabled fraud is a worldwide problem warranting a unified, global response. FBI officials stated that FBI coordinates efforts and activities to counter scams affecting all consumers to the extent possible within available funding and resources. However, FBI officials recognized that there is no formalized mechanism to deconflict (i.e., coordinate between agencies in areas where overlapping investigations occur to avoid compromising those investigations), collaborate, coordinate, leverage assets, and share respective resources among investigations.[39]

Some Industry and Consumer Organizations Have Advocated for a Government-wide Strategy to Counter Scams

Some industry representatives and consumer organizations have advocated for a government-wide strategy to counter scams. For example:

- In its November 30, 2023, meeting, the Federal Advisory Council to the Federal Reserve Board stated in its minutes that a government-wide approach is needed to counter fraud and scams.[40]
- In testimony before the Senate Homeland Security and Governmental Affairs Committee's Permanent Subcommittee on Investigations in May 2024, the American Bankers Association stated that a national

[39]FTC officials explained that deconflicting tools exist within the Sentinel database, for example, alerting other law enforcement users of active investigations. FBI added that while it acknowledges that FTC's Sentinel database includes tools that alert users of active investigations, this functionality falls short of a deconfliction tool. Rather than proactively preventing overlapping investigations, it provides an opportunity for agencies to recognize existing cases.

[40]The Federal Advisory Council, which was created by the Federal Reserve Act, is composed of 12 representatives of the banking industry selected by the Federal Reserve Banks.

antiscam strategy needs to be developed.[41] The association said that "fraud and scams are costing consumers billions of dollars each year and current federal activities are disjointed and uncoordinated with no overarching strategy." The association further stated its belief that a "national anti-scam strategy is critically needed to develop and implement a coordinated federal approach focused on stopping consumers from being scammed in the first place and developing solutions to assist consumers once the scam has been perpetrated." Further, the association said, "Focusing on only one aspect or one step in the [scam] process will not stop this surge of scams. Rather, a holistic approach to address all the entities and elements of a scam has the best chance of being successful."

- An official from the Consumer Federation of America we spoke with stated that there is a need for a strategy to help develop a uniform term that defines scams, develop a single estimation of losses associated with scams, and coordinate efforts so federal agencies can work better together and with the banking industry.[42]
- Officials from one of the world's largest financial institutions told us that a national antiscam strategy and a comprehensive federal government approach are needed to counter these criminals and the scams they perpetrate. This strategy requires a whole-of-government response that partners with financial institutions, telecommunications companies, and social media companies to protect consumers. Further, the officials stated that there is a need for a lead agency to help coordinate efforts and prevent fragmentation.
- The Retail Gift Card Association told us that it values and supports legislation that is focused on inter-agency strategies and data sharing in an effort to counter fraud, while ensuring that gift cards remain accessible, anonymous, and convenient to consumers.

[41]The American Bankers Association is an organization that supports bankers and other members of the financial services industry with education, tools, and expert insights. The American Bankers Association also advocates for banks in legislative and regulatory issues.

[42]The Consumer Federation of America is a nonprofit organization founded to advance consumer interests through research, education, and advocacy.

- In July 2024, the Aspen Institute Financial Security Program launched the National Task Force for Fraud and Scam Prevention.[43] According to public information, the task force will bring together stakeholders from the government, law enforcement, and private industry to develop a nationwide strategy aimed at helping prevent fraud and scams. The task force plans to address different aspects of fraud and scams, with a primary focus on prevention. Some of the members that are part of the task force include BBB, American Bankers Association, FinCEN, FBI, FTC, Department of Homeland Security, and Secret Service, among other organizations.

Other Countries Have Developed Strategies and Identified Entities to Counter Scams

Other countries, such as the United Kingdom, Australia, and Singapore, have developed and implemented government-wide strategies and identified specific entities to counter scams, with attributable reductions in the level of scams.

Specifically, in May 2023, the United Kingdom government issued a fraud strategy that provides a plan for how government, law enforcement, regulators, industry, and charities will work together to counter scams.[44] The strategy states that scams continue to be the priority for the Financial Conduct Authority and that it will continue to proactively consider a range of potential policy initiatives to tackle the scale and impacts associated with this type of crime, both for victims and the firms that the authority regulates.[45] Since the launch of the fraud strategy, the United Kingdom saw a decrease of fraud of 13 percent in June 2023, 16 percent in December 2023, and 10 percent in March 2024 year-on-year. However,

[43]The Aspen Institute is a global nonprofit organization whose purpose is to ignite human potential to build understanding and create new possibilities for a better world. The Aspen Institute Financial Security Program aims to illuminate and solve the most critical financial challenges facing American households, making financial security for all a top national priority.

[44]HM Government, *Fraud Strategy: Stopping Scams and Protecting the Public* (May 2023), https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf.

[45]The Financial Conduct Authority regulates the financial services industry in the United Kingdom. Its role includes protecting consumers, keeping the industry stable, and promoting healthy competition between financial service providers.

the United Kingdom saw an increase of fraud of 7 percent in June 2024 and a 19 percent increase of fraud in September 2024 year-on-year.[46]

Similarly, Australia created a National Anti-Scam Centre within its Competition and Consumer Commission that draws on expertise across government, law enforcement, industry, and consumer groups to make Australia a harder target for scammers.[47] Together, the entities collect and share scam data and intelligence, implement scam prevention and disruption initiatives, and provide better awareness alerts and education resources to help consumers identify and avoid scams. The National Anti-Scam Centre supports the work of those agencies. For example, the Anti-Scam Centre provides a central place for consumers to report scams, shares information about scams across the Australian government, and coordinates activities to stop scams.

The Australian government has reported that the National Anti-Scam Centre's efforts have led to a 13.1 percent decline in reported scam losses from 2022 to 2023. The Australian National Anti-Scam Centre reported that overall scam losses in the fourth quarter of 2023 were down by 43 percent compared with the same quarter in the previous year. Further, in November 2023, the Australian government announced the proposed Scams Code Framework. The proposed framework would set clear roles and responsibilities for industry, with an initial focus on banks,

[46]Office for National Statistics, *Crime in England and Wales: year ending September 2024* (Jan. 30, 2025), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2024; *Crime in England and Wales: year ending June 2024* (Oct. 24, 2024), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2024; *Crime in England and Wales: year ending March 2024* (July 24, 2024), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2024; *Crime in England and Wales: year ending December 2023* (Apr. 25, 2024), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2023; *Crime in England and Wales: year ending September 2023* (Jan. 25, 2024), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2023; and *Crime in England and Wales: year ending June 2023* (Oct. 19, 2023), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2023.

[47]Australian Competition and Consumer Commission, *National Anti-Scam Centre in action: Quarterly update January to March 2024*, https://www.nasc.gov.au/system/files/NASC-Quarterly-update-Q3-2024.pdf.

telecommunications providers, and digital platforms, in an effort to fight against scams.

Singapore created the Anti-Scam Command to achieve greater synergy between various scam-fighting units within the Singapore Police Force by integrating scam investigation, incident response, intervention, and enforcement capabilities under a single umbrella.[48] In October 2023, Singapore published a proposal for a Shared Responsibility Framework for sharing responsibility for phishing scam losses among financial institutions, telecoms, and consumers.[49]

The Absence of a Comprehensive, Government-wide Strategy Poses Risk for Fragmentation of Effort and Overlap of Activities

As described earlier in this report, responsibility for countering scams is dispersed among at least 13 federal agencies. Our prior work has shown that in some instances, it may be appropriate or beneficial for multiple agencies to be involved in the same programmatic or policy area due to the complex nature of the issue or magnitude of the federal effort.[50] In other instances, in a situation such as countering scams, having multiple agencies involved in the same programmatic area could create the risk of fragmentation of effort or overlap of multiple activities (such as those described in this report)—especially absent a strategy to coordinate and manage such activities—potentially limiting their effectiveness and impact.[51]

In this regard, the varied aspects of scams, and responses to them, cross the jurisdictions of multiple agencies. Consequently, no one agency can

[48]Public Affairs Department, Singapore Police Force, *"Opening of Anti-Scam Command Office"* (September 2022), https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office.

[49]Phishing is a type of online scam that targets consumers by sending them an email that appears to be from a well-known source, such as a financial institution. It asks the consumer to provide personal identifying information. Then a scammer uses the information to open new accounts or invade the consumer's existing accounts.

[50]See GAO, *Broadband: National Strategy Needed to Guide Federal Efforts to Reduce Digital Divide*, GAO-22-104611 (Washington, D.C.: May 31, 2022); and *Broadband: A National Strategy Needed to Coordinate Fragmented, Overlapping Federal Programs*, GAO-23-106818 (Washington, D.C.: May 10, 2023).

[51]Fragmentation refers to those circumstances in which more than one federal agency (or more than one organization in an agency) is involved in the same broad area of national need, and opportunities exist to improve service. Overlap occurs when multiple agencies have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries. See GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP (Washington, D.C.: Apr. 14, 2015).

counter the problem alone, and no agency is mandated or required to do so, either individually or collectively.[52] As a result, and absent formal guidance or directive, no agency has taken the lead to explore the need for and develop a comprehensive, government-wide strategy to help guide the various activities agencies employ to counter scams and mitigate the risk for potential fragmentation and overlap.

We have reported that strategies to coordinate programs that address crosscutting issues of broad national need can help identify and mitigate negative effects associated with fragmented, overlapping, and potentially duplicative federal programs.[53] While interagency coordination can help agencies and those they support, broad and challenging goals—in this instance, countering scams—may require a national strategy.

Our prior work has identified desirable characteristics of national strategies, including clear organizational roles, goals, objectives, and performance measures to gauge and monitor results. Defining organizational roles involves identifying entities—for example, specific federal agencies and offices and any other sectors, such as states and private industry—and their respective responsibilities. Goals address what the strategy is trying to achieve, objectives help lay out the steps needed to achieve those results, and performance measures provide accountability for achieving results. Additionally, a strategy should identify necessary resources and any legislative, regulatory, or administrative changes to assist with implementation of the strategy. Further, strategies are most effective when they are regularly updated and monitored.[54]

A single, comprehensive, government-wide strategy to combat scams would facilitate the alignment and coordination of the range of federal agency activities to counter scams and help prevent consumers from becoming victims. In this regard, as discussed earlier, the implementation of similar strategies in the United Kingdom and Australia illustrates their potential impact. Namely, according to these governments, their strategies have helped reduce fraud and scam losses. Some industry and

[52]Other nongovernment entities may also have a role in countering scams. In July 2024, we found that financial institutions and industry representatives believed telecommunication and social media companies could play a greater role in reducing scams by making it more difficult for scammers to communicate with potential victims. GAO-24-107107.

[53]GAO-22-104611 and GAO-23-106818.

[54]GAO-04-408T.

agency officials pointed out that a national strategy to combat scams would be foundational to developing and implementing a coordinated federal approach because no single agency has the jurisdiction, authorities, and resources to tackle the diversity of fraud and scams. A government-wide strategy could help overcome those jurisdictional barriers.

Assigning a federal agency to lead the development of a government-wide strategy to organize and prioritize combating scam efforts could help ensure that related activities are not duplicative or fragmented, do not unnecessarily overlap, and have a greater impact. According to FBI, it is best positioned to lead efforts to mitigate scams due to its expertise regarding cyber-enabled fraud and the collaborative capabilities of its FCS with stakeholders internal and external to FBI.

According to FBI, the FCS has established resources to immediately contribute to mitigating scam threats across agencies via financial crime response and support teams, relationships with national commissions and networks that counter financial and cyber-crimes networks, and dedicated legal attachés located abroad. The FCS also can leverage strong working relationships with strategic partners combating scams, such as other DOJ components, IC3, FinCEN, CFPB, and FTC.

As previously discussed, FBI/FCS is developing a cyber-enabled fraud strategy to identify, target, and disrupt prolific transnational criminal enterprises defrauding Americans. The overlap in issues relating to scams and cyber-enabled fraud could provide FBI/FCS with the expertise to develop a comprehensive, government-wide strategy for the federal government that includes clear organizational roles, goals, objectives, and performance measures across federal agencies to gauge and monitor results. A comprehensive, government-wide strategy could help facilitate and target efforts to combat scams and help prevent consumers from becoming victims.

Federal Agencies Compile Scam-Related Complaint Data, but Limitations Exist in Estimating the Extent of Scams and Related Financial Losses

CFPB, FBI, and FTC collect and report on consumer complaints both directly and, in some cases, from other agencies, as discussed below. Data limitations prevent agencies from determining the exact number of all scam complaints and dollar losses. CFPB, FBI, and FTC can provide limited estimates of the number of complaints and related dollar losses specifically related to scams. Additionally, there is no single, government-wide estimate of the total number of scams and dollar losses that factors in unreported incidents. Similarly, federal agencies have not produced a common, government-wide term for, or definition of, scams.

Agencies Collect and Report on Consumer Complaints, but the Data Collected Have Limitations

Of the eight federal agencies that receive scam-related consumer complaints, three agencies (CFPB, FBI, and FTC) publish annual reports summarizing consumer complaint data. However, the data these reports are based on have limitations.

CFPB

Complaint Collection

When consumers submit complaints to CFPB, they are asked to select one of 11 consumer financial products or services (such as credit reporting, credit card, or prepaid card) with which they have a problem, the issue that best describes the problem, and the company to which they want to direct their complaint. Consumers can further select from a list of issue categories, such as “Fraud or Scam.” The categories vary, depending on the consumer financial product or service selected. Consumers can describe the details of their complaint and their desired resolution, using open narrative fields. Consumers are instructed to describe what happened and to include dates, amounts, and actions taken by the consumer or the company.

CFPB sends the consumer complaints it receives to companies named by complainants for review and response. It also uses information from consumer complaints and company responses to monitor risk in financial markets, assess risk at companies, and prioritize agency action.

Complaint Reporting

CFPB publishes annual reports that include information on the number of consumer complaints it received, by financial product or service. These reports also detail the percentage of complaints that were closed with and without monetary relief from the companies subject to the complaints. These reports do not state the financial loss amount reported by consumers or the total number of complaints and associated dollar losses that were only related to scams.

Data Limitations

The way CFPB complaint data are collected limits their utility in reporting an aggregate count of the total number of complaints CFPB received related to scams. Specifically, if consumers submit complaints under the "Fraud or Scam" issue category, no further categories are available to select, for example, whether a complaint was about a specific scam, such as romance or tech support.

Additionally, consumers do not always have the "Fraud or Scam" option available to select. Specifically, CFPB does not have a predetermined data field that allows consumers to select a scam type, such as impersonation scam, for every financial product or service that consumers can submit a complaint about. For example, an impersonation-related data field is available for consumers who submit a complaint specifically about telecommunications debt (a debt collector trying to collect for a telecom bill, such as an internet, cable, or phone bill) but not for other categories, such as credit card debt and complaints about a checking or savings account. CFPB also does not request dollar loss amounts from consumers in a predefined field. CFPB officials stated that the agency uses narrative information entered by consumers to determine whether a complaint was specifically related to a scam, to the extent such information is provided, and analyzes narrative information as part of its ongoing monitoring activities.

According to CFPB, the agency's complaint function is designed to collect complaints regarding consumer financial products and services. CFPB officials stated that due to variability and the evolution of market and related issues, the agency provides an open narrative field so that consumers can explain the issue in their own words. They noted that the complaint function was intentionally designed to not duplicate the FTC's fraud reporting website.

According to CFPB officials, a change to the CFPB complaint form to permit consumers to identify a specific type of fraud or scam would require significant system, reporting, and data publication and sharing changes, among other things. Additionally, such a change would require CFPB to conduct a feasibility assessment to evaluate proposed changes and conduct user testing to ensure that any changes capture the information sought and are clear to complainants and that issues or biases are identified prior to implementation.

The FBI's IC3

Complaint Collection

All complainants to IC3 are requested to provide name and contact information and details of the transaction they are submitting a complaint about. Consumers are specifically requested to provide information on any financial loss, payment method used, and recipient of any funds in separate data fields. Consumers can describe additional details about their complaint, using an open narrative field, and are instructed to provide a description of the incident and how the consumer was victimized. Instructions for the narrative field inform consumers to provide information not captured elsewhere on the complaint form.

Consumer complaints received by IC3 are analyzed and disseminated to federal, state, local, or international law enforcement or regulatory agencies for public awareness and criminal, civil, or administrative action, as appropriate.

Complaint Reporting

IC3 publishes annual internet crime reports that provide consumer complaint statistics. The reports state the total number of internet crime complaints and reported associated losses made by consumers to IC3. In 2023, IC3 reported approximately 880,000 internet crime complaints and $12.5 billion in associated potential losses. The reports also include the number of complaints and reported associated dollar losses related to some specific scams taken from consumer complaint narratives. For example, these reports categorize complaints by crime type that include scam-related crimes (such as government impersonation) and non-scam-related crimes (such as harassment and stalking). These reports do not include a single total of the number of complaints and associated dollar losses that were only related to scams.

IC3 also issues an annual report on fraud affecting older adults that provides information on scam complaints submitted by consumers who

indicated in their complaints that they were at least 60 years old. DOJ officials acknowledged that these reports also do not include a total of the number of complaints and associated dollar losses that were only related to scams.

Data Limitations

The way IC3 complaint data are collected limits their utility in reporting an aggregate count of the total number of complaints related to scams. IC3 does not collect information from consumers about scams in predefined fields. Specifically, FBI does not provide fraud or scam subcategories, such as imposter scams, that consumers can select from when making complaints. Because IC3 does not request information from consumers about the type of internet crime they encountered in a predetermined data field, it relies on consumers to include this information in an open narrative field. According to FBI officials, analysts review IC3 complaints to determine the crime type and actual dollar losses based on the information provided by the consumer.

FBI officials explained that IC3 had previously provided consumers an opportunity to select the specific type of internet crime they were reporting. At that time, officials stated that consumers predominantly selected an incorrect crime type, which could result in complaints being forwarded to the wrong place for investigation. FBI officials stated that programming could be implemented to add a scam-type data field in the complaint form, but the scope of the addition would be driven by time and cost factors, and an analyst review would still be required to ensure the validity of the provided information.

FTC

Complaint Collection

When consumers submit complaints to FTC, they are asked to select from a list of fraud schemes and other consumer issues. Consumers are specifically requested to provide information on any financial loss and payment method used and how they were contacted, in separate data fields. Consumers can also choose to provide information about their age by selecting an age range. Consumers can describe additional details about their complaint, using an open narrative field, and are instructed to state what happened in the consumer's own words with specific details they remember.

The agency's Sentinel database also receives consumer complaints directly from its 46 data contributors that include federal and state

agencies; private companies; and nonprofit organizations, such as the BBB.[55] According to FTC, over 50 additional entities, including government and business, inform consumers that they can file complaints through the FTC's website. Three of the eight federal agencies we identified that receive consumer scam complaints—FTC, CFPB, and FBI—contribute complaint reports to Sentinel.[56] According to FTC, for complaints classified as fraud, the largest Sentinel contributors in calendar year 2024 were FTC, BBB, and FBI, which together made up over 75 percent of complaints received.[57]

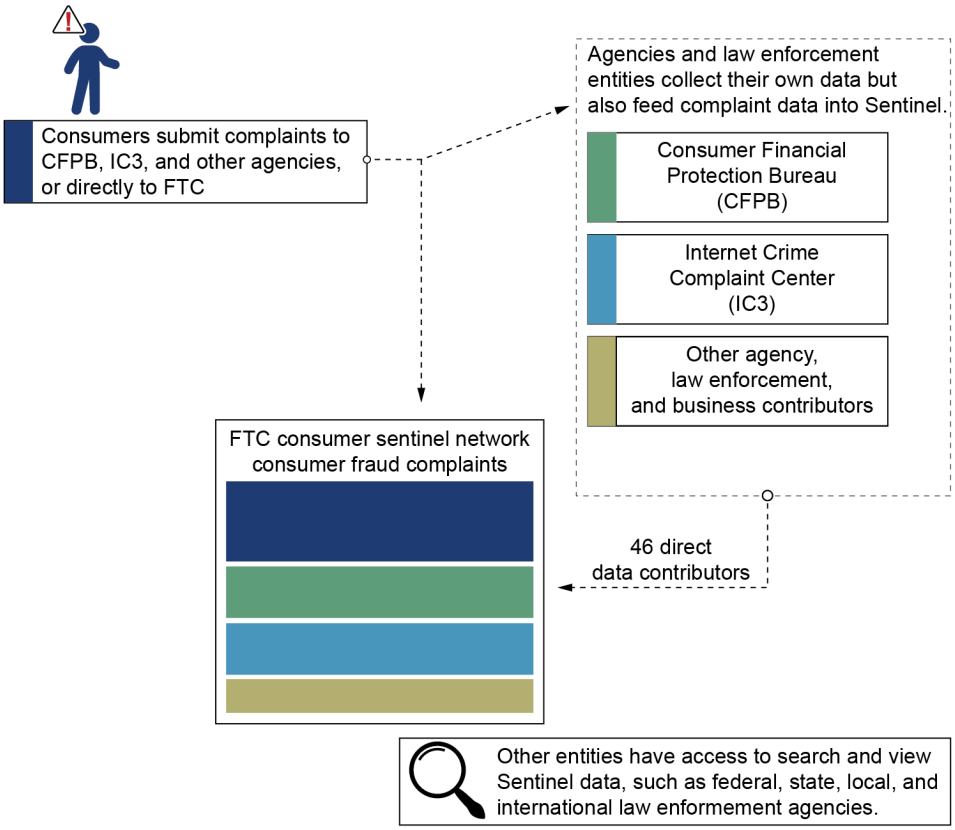
FTC uses consumer complaints for investigations in connection with law enforcement efforts, to spot trends on the issues consumers are reporting, and to educate the public. According to FTC officials, these data are also used for other initiatives, including workshops in which developing issues are addressed. FTC provides access to consumer complaint information to members of law enforcement organizations that have entered into a confidentiality and data security agreement with the agency. Figure 4 below shows how consumer complaints are maintained by FTC and subsequently made available to Sentinel members.

[55]According to FTC officials, the agency has a means for identifying and grouping duplicate complaints in Sentinel, allowing law enforcement to see that a consumer reported to multiple agencies. Other federal or state entities who do not contribute to Sentinel may also receive consumer complaints related to scams.

[56]The agencies that contribute to Sentinel include CFPB, FTC, and FBI. The agencies that do not contribute to Sentinel include FDIC, HSI, OCC, the Federal Reserve Board, and the Secret Service.

[57]FTC, BBB, and FBI accounted for approximately 47, 22, and 8 percent, respectively, of Sentinel fraud complaint data reported for 2024, according to FTC.

Figure 4: Consumer Sentinel Network Overview



Sources: Federal Trade Commission (FTC) (information); Icons-Studio, sdecoret/stock.adobe.com, GAO (icons). | GAO-25-107088

Complaint Reporting

FTC publishes annual reports detailing consumer complaint data maintained in Sentinel. These reports include the total annual number of complaints and dollar losses in Sentinel involving fraud including, but not limited to, scams. In 2024, Sentinel received 2.6 million consumer fraud complaints and overall fraud losses of over $12.5 billion.[58] The reports categorize fraud complaint information by schemes that include types of scams, such as imposter scams. The reports do not state a single total of the number of complaints and associated dollar losses that are specific to scams. FTC officials stated that in general, they could not quantify the

[58]Federal Trade Commission, *Consumer Sentinel Network Data Book 2024* (March 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

number of all scam complaints because the agency's complaint form does not specifically ask consumers if they were scam victims.

Data Limitations

The entities that contribute to Sentinel do not always request fully consistent complaint information from consumers. This potentially limits the FTC's ability to categorize and summarize contributor information and report on the complaint data FTC receives. The total number of fraud complaints in Sentinel and associated dollar losses could be understated because not all contributors request that consumers provide the dollar amount lost as part of a scam or provide specific information about the type of scam they encountered in predefined data fields.

FTC maps CFPB complaints by type that come into Sentinel, but because CFPB collects the dollar amount lost in a narrative data field and does not have a separate data field for the dollar amount lost, that information is not captured separately. This limits the ability to use fraud reports received from CFPB to calculate a single measure of consumer scam complaints and losses. According to FTC, in 2024, while CFPB was the largest contributor of Sentinel complaint data, it was a source of just 1 percent of fraud complaints. FTC officials noted that FTC assigns contributors' data that do not match the FTC's categories to the appropriate category in Sentinel, where possible.

FBI officials also told us that not all IC3 scam complaints are contributed to Sentinel. For example, complaints that are filed with IC3 on behalf of a business with the business name included, or that are referred to a field office, are not provided to Sentinel. FBI officials stated that IC3 complaints filed on behalf of a business include reports about business database intrusions, ransomware attacks, and intellectual property rights and that providing this information to FTC could jeopardize trust in FBI. FBI noted that it shares some of the information it collects with other government agencies in service of its intelligence mission and to contribute to the federal government's strategic understanding of cyber threats; however, FBI does not share cyber victim information with other government agencies. Excluding complaints that are filed on behalf of a business from Sentinel could also exclude some complaints related to scams.

According to FTC, it has not been seen as necessary for Sentinel contributors to change the data fields collected to match its data fields or to provide consistent data fields, as there are cost considerations for

contributors in doing so, and each agency has unique data collection needs. Additionally, contributor databases may predate their decision to become a Sentinel contributor. FTC officials stated that the agency would always welcome more data that could be appropriately formatted into Sentinel data fields and works with its data contributors to improve how data are contributed. Although over 75 percent of 2024 Sentinel fraud data were provided by FTC and two other contributors, FTC officials told us that FTC works with Sentinel contributors to align the data they submit with the fields in Sentinel. These officials stated that the agency has a group that reviews the categories to determine which ones remain relevant over time and which ones need to be retired. They also monitor the information submitted by their contributors to ensure it still aligns with the correct fields. Every year, the volume of information FTC receives continues to increase, so it has started using tools, such as machine learning, to read complaint narratives to ensure the category of the complaint is correct, according to FTC officials.

While such efforts to strengthen the data are helpful, the agencies experience a variety of data limitations, as discussed above. Such limitations affect their ability to report on the types and extent of scams, target preventative efforts, and measure progress in scam prevention.

Agencies Can Estimate the Number of Scam Complaints and Associated Losses

CFPB, FBI, and FTC can calculate an estimate of complaints they receive that are related to scams but not the exact number of scam complaints. However, these agencies do not publicly report these estimates and each of these estimates has limitations.

While CFPB does not publish a count of scam complaints received, agency officials told us that CFPB had developed a model that conducts a text analysis of consumer complaint narratives that can identify complaints likely—but not definitively—related to scams over the P2P platforms only. Based on the CFPB's modeling, the agency estimates that in 2023, it received 3,210 complaints potentially regarding scams over P2P platforms. CFPB officials stated that they did not have a loss estimate for scam-related complaints because they do not require consumers to include dollar losses when filing a complaint.

FBI officials stated that they could quantify the number of complaints FBI receives about scams wherein the victim specified a dollar loss. Although the officials noted that FBI does not include, in its annual reports, a line item for total scam complaints received and associated dollar losses, it compiled the total at our request. According to FBI officials, in 2023, IC3 estimated that it received over 589,355 complaints related to scams, with

losses of $10.55 billion. FBI officials told us that they could consider adding an estimate of scams, and related financial losses, in future annual reports.

FTC officials also told us that they could estimate the number of calendar year 2023 scam complaints and associated financial losses that involved consumers sending payment to a scammer.[59] They said such an estimate could be based on three Sentinel complaint categories that often describe these scenarios and provided an estimate at our request. According to FTC officials, imposter scams (including business, government, and romance imposters), sweepstakes and lottery, and investment-related fraud categories often describe scams involving a consumer making a fraudulently induced bank transfer to a scammer.[60] Based on these three categories in Sentinel, FTC estimates that consumers reported over 280,000 incidents that frequently involved fraudulently induced bank transfer to a scammer in 2023, with reported financial losses totaling over $7.8 billion.

Since CFPB, FBI, and FTC use different, incomplete and, in limited cases, duplicative data and different methodologies to make their estimates of the scam complaints they receive, the estimates cannot be aggregated to make a broader estimate of the total number of scam complaints.

Underreporting of Scams and Lack of a Common Definition Complicate Calculating a Government-wide Estimate of Scams

The underreporting of scams and the lack of a common scam definition complicate calculating a government-wide estimate of scams. According to DOJ and FTC, most consumer fraud goes unreported. For example, in 2015, DOJ estimated that 15 percent of the nation's fraud victims report their crimes to law enforcement.[61] Consequently, the numbers of instances and loss amounts provided in the annual reports discussed above are likely underestimates. Similarly, a study cited by FTC reported that about 5 percent of people who experienced mass-market consumer

[59]FTC does publish the exact number of fraud complaints received. FTC officials told us that the agency uses the terms fraud and scam interchangeably and does not distinguish between them in the manner proposed in this report.

[60]Bank transfers was the most commonly cited payment method in the complaints. A fraudulently induced payment occurs when a person with payment authority is manipulated or deceived into making a payment for the benefit of the scammer.

[61]United States Attorney's Office, Western District of Washington, *Financial Fraud Crime Victims*, https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud.

fraud complained to a BBB or a government agency.[62] According to FTC officials, the agency has estimated the amount of consumer fraud losses—not specific to just scams—taking into account underreporting, but officials stated more research was needed to accurately extrapolate a single estimate of scams based on consumer complaint data.[63]

FBI and FTC officials cited challenges to providing an overall estimate of the number of scams and associated dollar losses impacting the public. According to FTC officials, it would be difficult for CFPB, FBI, and FTC to work together to estimate the overall number of consumers affected by scams and their losses because consumer underreporting rates are unknown and could vary by loss amount. FBI officials stated that losses reported by FTC and CFPB could be inflated or underestimated, depending on whether they adjust consumer-reported losses. According to FBI officials, many complainants may provide a higher loss to garner faster attention, or inadvertently enter an inflated loss amount.

Moreover, other data sources suggest that the total number of scams affecting the public could be larger than indicated by complaint data. Specifically, in 2024, FinCEN published a report analyzing identity-related suspicious activity involving impersonation, which includes scams, that estimated a higher number than the scam complaint totals provided by

[62]The BBB accepts complaints about scams, misleading advertisements, identity theft, and other marketplace issues involving any business. Mass-market consumer fraud refers generally to any fraud scheme that uses one or more mass-communication methods, such as the internet, telephones, mail, or in-person meetings, to fraudulently solicit or transact with numerous prospective victims, or to transfer fraud proceeds to financial institutions or others connected with the scheme. Keith B. Anderson, *To Whom Do Victims of Mass-Market Consumer Fraud Complain?* (May 24, 2021), available at SSRN: https://ssrn.com/abstract=3852323, or http://dx.doi.org/10.2139/ssrn.3852323. This report examined the likelihood that victims of mass-market consumer frauds complained about their experience to someone more than just family and friends. For the analysis, data from surveys sponsored by FTC on mass-market consumer fraud in 2005, 2011, and 2017 were used. The report stated that less than 3 percent of victims complained to a government entity. Somewhat more than half of these—1.5 percent of victims—complained to a local authority, such as the local police. Less than 1 percent complained to a state attorney general or other state authority or to a federal agency. Over 2 percent reported having complained to a BBB. Together, 4.8 percent of victims complained to a BBB or to a government agency.

[63]FTC estimates that overall consumer loss from fraud, adjusting for underreporting, was as high as $158.3 billion. Federal Trade Commission, *Protecting Older Consumers 2023-2024* (Oct. 2024).

FBI and FTC.[64] Even though there are duplicate filings in the data, this report can provide insights on the scale of this suspicious activity. Based on the Bank Secrecy Act data filed with FinCEN in 2021, FinCEN identified a total of $566 billion in suspicious activity. Of this amount, $200 billion was related to impersonation-related suspicious activity, such as romance scams, person-in-need scams, tech and customer support scams, employment scams, and financial institution and government imposter scams.

We have previously reported on the importance of knowing and understanding the scope of fraud in managing fraud risk.[65] Fraud estimates, including those specifically addressing scams, can demonstrate the scope of the problem, could help improve oversight prioritization, and could help determine the return on investment from activities to mitigate fraud.

Additionally, *Standards of Internal Control in the Federal Government* state that management should use quality information to achieve its objectives.[66] Specifically, these standards note that management identifies information requirements as part of an iterative process, obtains relevant data from reliable sources in a timely manner, and evaluates the reliability of the information obtained. Further, management processes the data into quality information and uses such information to make informed decisions and evaluate an entity's performance in achieving key

[64]Financial Crimes Enforcement Network, *Financial Trend Analysis Identity-Related Suspicious Activity: 2021 Threats and Trends* (January 2024). This was the latest analysis available pertaining to impersonation-related suspicious activity. This Financial Trend Analysis focuses on pattern and trend information identified in Bank Secrecy Act data linked to identity-related suspicious activity reported in 2021. FinCEN issues this report pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 that requires periodic publication of Bank Secrecy Act-derived threat pattern and trend information. FinCEN has determined that identity-related suspicious activity is a cybercrime concern. FinCEN's impersonation-related suspicious activity includes various scams where criminals claim to be businesses, charities, financial institutions, government entities, and other individuals to manipulate victims into providing funds, personally identifiable information, or account or system access.

[65]GAO-24-105833. GAO's work focused on fraud impacting federal programs and operations. This work discusses the importance of understanding the scope of fraud in preventing wrongdoing and directing proper resources to stop fraud from occurring. Scams are a type of fraud perpetrated against consumers. Like with fraud impacting federal programs and operations, understanding the scope of scams could help with efforts to counter it.

[66]GAO-14-704G. Quality information is accessible, current, and complete, among other characteristics.

objectives and addressing risks. Likewise, management considers the accessibility of information and makes revisions when necessary, so that the information is accessible. In this regard, management communicates quality information to external parties through appropriate methods so that such parties can help the entity achieve its objectives. Also, a desirable characteristic of a national strategy is the inclusion of performance measures. If significant limitations on performance measures exist, other parts of the strategy might address plans to obtain better data or measurements. Having specific information on scams impacting consumers could provide Congress, federal agencies, and the public with a better understanding of the scope of this type of crime. This would include an estimate of the number of victims and the total costs of scams. Developing a government-wide estimate could assist agency efforts to assess trends in this type of crime and better understand whether antiscam efforts are having an effect.

FBI officials stated that it would take significant coordination and review to produce and report on a single, government-wide scam estimate, as each agency captures fraud and scam crime types differently. Calculating an estimate of the total number of scams and associated dollar losses affecting consumers is also made more difficult because federal agencies and other stakeholders do not have a commonly defined term to describe this type of crime. Some agencies stated that they use broad terms, such as fraud or cyber-enabled financial crimes, when discussing what we refer to in this report as scams. Federal agencies, law enforcement organizations, and associations representing consumers, businesses, and regulators have used other terms synonymously, such as victim-assisted fraud, push payment fraud, authorized push credit payment, authorized push payment fraud, social engineering fraud, faster payments, and scams. Further, the CFPB, IC3, and FTC annual complaint reports we reviewed did not have a definition of scam or consistent scam types. For example, FTC defines and categorizes imposter scams differently from FBI, and CFPB does not define the different types of imposter scams that are included in the FTC and FBI reports.

It is important to define terms and use definitions consistently, including using common definitions, when measuring the volume and impact of scams over time. Using a common definition for this type of crime would

improve the ability of agencies to compare and aggregate data across agencies, assess trends, and show progress in fraud prevention.[67]

According to the Federal Reserve, accurate quantification of scams is often challenging because of multiple operational scam definitions and a lack of consistency in existing scam-type classification approaches. In spring 2023, the Federal Reserve established a scams definition and classification work group. This work group consisted of payments and fraud experts from different disciplines, including federal agencies and financial institutions, with the goal of providing a more consistent foundation for scams reporting to better understand and mitigate the problem. Federal Reserve Board officials told us that it was important to have a consistent scam definition to help ensure that different agencies are counting the same thing, when quantifying scams.

Federal Reserve's Scams Definition

According to the Federal Reserve: "*The definition of a scam is intended to be used by payments industry stakeholders, such as financial institutions, payment networks, technology solution providers and industry trade organizations. However, the work group's definition can benefit non-payments industry audiences, ranging from law enforcement to social media platforms, allowing all involved to use a more consistent classification method. The scams definition is expected to have multiple uses, including helping to foster more consistent dialogue and understanding of scam trends across organizations. In addition, this dialogue can improve scam detection and mitigation, education and reporting by both consumers and businesses*."

Source: Federal Reserve. I GAO-25-107088

The work group's goal was to craft a definition that can apply both to attempted and successful scams. The definition had to encompass key concepts, such as scam interactions, intent, and financial gain. In September 2023, the work group published an operational definition of scams and, in June 2024, introduced a Scam Classifier Model.[68] The definition defines scams as the use of deception or manipulation intended

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

[68]According to the Scam Classifier Model, the model supports consistent and detailed classification, reporting, analysis, and identification of trends in scams. It uses a series of questions to differentiate and classify scams by categories and types and provides a view of the full impact of scams by including cases that resulted in authorized payments, as well as unauthorized payments from account access. The model also can be used to capture attempted scams. Regulation E of the Electronic Funds Transfer Act defines an authorized payment as a payment made by a consumer that is authorized to make a payment–regardless of how they were induced to authorize such payment, whereas an unauthorized payment occurs when a criminal directly accesses a consumer's bank account without the consumer's knowledge.

to achieve financial gain.[69] Federal Reserve Board officials told us that CFPB, FBI, and FTC were not part of this work group and that the officials did not know what those agencies' views would be on this definition. This definition has not been adopted throughout the government.

FTC officials told us that the agency uses the terms fraud and scam interchangeably and did not distinguish between them. These officials stated that the agency considers both words to be synonymous, as both fraud and scams have elements that involve deception to obtain money or something of value. However, not all fraud or business complaints received by FTC involve individuals who were deceived into giving money to scammers. FTC officials stated when discussing fraud and scams that the agency did not track data to differentiate between a consumer deceived into making a payment or a criminal directly accessing a consumer's bank account without the consumer's knowledge because the harm was the same. Similarly, according to FBI, in general, it considers incidents that involve unauthorized activity as fraud and incidents where a scammer convinces the victim to authorize a transaction or to willingly supply personal information as scams. Sometimes FBI uses the terms interchangeably but this does not have a significant impact on how investigations are conducted.

FTC officials told us that there has been other work undertaken to develop a fraud taxonomy. They cited a framework published in 2015 that involved fraud experts representing government, academic, and nonprofit organizations.[70] The agencies that participated in developing this taxonomy included FBI and FTC, among others. However, FTC does not use this fraud taxonomy framework in its consumer fraud complaint reports. According to FTC officials, the taxonomy categories proposed in the framework do not fully cover the range of scams or fraud reported today. For example, the taxonomy framework does not include up-to-date information on the types of imposter scams.

[69]As previously noted, for this report, we use the term "scams" as defined in the Scam Classifier Model. GAO defines fraud as obtaining something of value through willful misrepresentation. This report highlights specific types of scams that include impersonation scams and investment scams, among others. These scams are included in the Scam Classifier Model but are not an exhaustive list of all current and other types of scams that may evolve in the future.

[70]Stanford Center on Longevity, *Framework For A Taxonomy of Fraud* (July 2015), https://longevity.stanford.edu/financial-fraud-research-center/wp-content/uploads/2016/03/Full-Taxonomy-report.pdf. A taxonomy consists of clear, plain-language categories and subcategories used to describe data.

As mentioned earlier, a desirable characteristic of national strategies includes defining the issue or problem that a particular strategy is intended to address. We have reported that the use of common definitions promotes, among other things, more effective intergovernmental operations and helps avoid duplication of effort.[71] In this regard, the definition by the Federal Reserve offers a baseline around which federal agencies and others could collaborate and arrive at a common understanding of what constitutes a scam. Alternatively, agencies could work together to develop a different agreed-upon definition.

Developing a government-wide definition of scams and improving consumer scam complaint reporting could assist agency efforts to compare data across agencies, develop an overall estimate of the total number of scams, and assess trends. Most importantly, agency efforts to improve data collection and reporting about the types and extent of scams would help government agencies, Congress, and industry target their preventative efforts and measure progress in scam prevention and would inform an effective antiscam strategy.

Federal Agencies Engage in Consumer Education Activities Related to Scams but Do Not Always Measure Their Effectiveness

As mentioned earlier, each of the 13 federal agencies we met with seek to educate consumers, for example, by publishing information about scams, issuing public reports on the topic, or conducting community outreach. Some of these efforts are specifically targeted to reach older adults.[72] The antiscam education provided to consumers varies by agency.

Some agencies routinely publish information about new scams and payment methods used by scammers as information about them becomes known. For example, FTC officials told us they analyze Sentinel data for consumer complaint trends and may tailor their education efforts accordingly. According to these officials, FTC publishes consumer alerts and articles on its website that relate to scams, including information on how to identify and avoid different scams. Such alerts also include

[71]GAO, *Homeland Security: Progress Made; More Direction and Partnership Sought*, GAO-02-490T (Washington, D.C.: Mar. 12, 2002).

[72]Legislation has been passed to help prevent older adults from becoming scam victims. In 2022, Congress passed the Seniors Fraud Prevention Act of 2022, Div. Q, Title 1, Subtitle B of Pub. L. No. 117-103, 136 Stat. 811 (2022). The law requires FTC to disseminate information on fraud targeting older adults, including a description of the most common scams and how to report complaints to FTC. As previously discussed, Congress also passed the Stop Senior Scams Act in 2022.

information specific to gift card, P2P, wire transfer, and other payment methods that scammers may use.

Some agencies also have education campaigns that consist of online content and proactive outreach related to scams. For example:

- CFPB provides resources on protecting older adults from fraud and financial exploitation. These resources are aimed at educating financial institutions, caregivers, and service providers working with families of older adults, and others. According to CFPB officials, these resources have included advisories to financial institutions about trends on fraud involving older adults. CFPB also publishes consumer education material on its website that includes payment scam warning signs and information on common scam types.
- FBI has provided training and outreach to groups such as media outlets; consumer groups; federal, state, and local law enforcement; and other groups on scams and issues related to elder fraud. In addition, FBI has published public service advisories on cyber-enabled fraud topics to educate the public on emerging scam trends. According to DOJ, FBI and other department components participated in over 1,600 outreach and training events from 2022 to 2024. Such events are intended to raise awareness of scams and help prevent scam victimization across all age demographics, with special emphasis on protecting older adults. According to FBI, the majority of its educational, outreach and awareness efforts are conducted in-person, across myriad platforms in a decentralized manner across field offices.
- FDIC and CFPB have jointly developed a Money Smart for Older Adults Program and free guides to raise awareness among older adults and their caregivers on how to prevent scams and other elder financial exploitation.
- FTC stated it conducts in-person and online outreach to groups such as older adults, the public, law enforcement agencies, and other stakeholders focused on protecting members of a wide range of communities from scams. According to FTC officials, FTC conducted over 600 outreach events in 2023. This outreach included approximately 150 events that were specifically intended for older adults or organizations that work with older adults.
- Since 2014, FTC developed and implemented Pass It On, a research-based education campaign that encourages older adults to help raise awareness about fraud by talking to family, friends, and neighbors about avoiding common scams. Pass It On has a dedicated website

with articles on 13 topics, including scams. Pass It On materials are available to the public and to the FTC's partners.

- FinCEN publishes public advisory products (i.e., FinCEN Advisories, FinCEN Alerts, and FinCEN Notices) on scams and fraud related to cryptocurrency investment, elder fraud, and others. FinCEN officials stated that while these products are primarily intended for financial institutions to support their filing obligations under the Bank Secrecy Act, they can also serve to educate the public.

Officials from other agencies we met with, including OCC and the State Department, stated they post information about types of scams on their websites to educate consumers.

CFPB, FBI, and FTC all stated they collect consumer complaints and provide education resources for consumers and measure traffic to their online resources. They do not, however, have mechanisms for evaluating how their activities impact consumer knowledge and behavior.[73]

Specifically, CFPB, FBI, and FTC have not designated performance measures or metrics for their in-person and virtual education activities that target outcomes for participants. This is, in part, because some agencies do not believe it is possible, or their focus is often on linking education efforts to a reduction in overall fraud. Also, officials from the three agencies stated that they do not measure the effect of a given presentation or webinar on individual participants.

In our prior work, we have found that using evidence, such as program outcomes, can help federal agencies effectively manage and assess the results of their efforts. Agencies could use measures of knowledge gained to determine the effectiveness of training. For example, agencies could follow up with participants 6 months or a year after the training to ask if they were contacted by a scammer. Agencies could then ask participants who were contacted by a scammer how they used the information

[73]Our previous work looked at federal financial literacy programs for older adults and people with disabilities and determined how the Financial Literacy and Education Commission, which is comprised of the heads of 24 federal agencies and entities, coordinates financial literacy efforts, and reports program outcomes to Congress and the public. We made two recommendations—specifically, that Treasury and CFPB coordinate with each other and with Commission agencies to encourage the ongoing collection of data on financial literacy program outcomes and include these data in the Commission's annual report to Congress. Treasury and CFPB agreed with GAO's recommendations. Both recommendations have been implemented. GAO, *Financial Literacy: Better Outcome Reporting Could Facilitate Oversight of Programs for Older Adults and People with Disabilities*, GAO-24-106381 (Washington D.C.: Apr. 24, 2024).

provided in the training to identify the scam and what subsequent steps they took.[74] It is important for agencies to ensure that their training efforts incorporate performance measures that can be used to demonstrate contributions that training makes to improving results. In addition, such information would allow agencies to identify aspects of their training program that need improvement.

CFPB stated it provides training about scams to stakeholder organizations who interact with and educate consumers. It also provides consumer education information on its website. Specifically, CFPB offers webinars on its website that discuss consumer protection against scams, among other topics. We found, however, that CFPB has not measured the impact of its stakeholder organizations' training on stakeholder participants that received the training. CFPB noted that it does track attendance of in-person training and views of the webinars it makes available on its website. Additionally, officials told us CFPB gathers information on how often resource pages and guides on their website are visited and conducts consumer satisfaction surveys.

CFPB has developed outcome-related performance metrics for other consumer education efforts. Specifically, CFPB has developed a tool for evaluating education outcomes related to resources used by stakeholder organizations.[75] The Money Smart guide developed by CFPB and FDIC contains precourse and postcourse assessments that stakeholder organizations can use to evaluate the impact of the training on participants. CFPB officials stated they have used these assessments to evaluate the effectiveness of the Money Smart guide. CFPB has also developed a 10-question Financial Well-Being scale that stakeholder

[74]GAO, *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts,* GAO-23-105460 (Washington, D.C.: July 12, 2023).

[75]Consumer Financial Protection Bureau, *Financial Literacy Annual Report* (December 2019), https://files.consumerfinance.gov/f/documents/bcfp_financial-literacy_annual-report_2019.pdf.

organizations can use to measure the impact of a financial literacy program on the participants' feelings of financial security.[76]

FBI officials noted that the agency tracks the number and location of events conducted and the approximate number of attendees and collects some demographic information about attendees at each of its in-person trainings. However, FBI officials also noted that it has not measured the outcomes of its in-person outreach and education activities on individuals that attended education programs. According to FBI officials, the agency does not believe it is possible to evaluate an overall reduction of fraud that links specifically to the impact of education on an individual's ability to recognize scams. FBI officials noted that the agency has explored ways to measure whether its education efforts influence consumers' ability to recognize scams but has determined there is no methodology to measure the success, utility, or impact of its efforts. According to FBI, it cannot monitor or control individuals' actions after they have participated in an FBI outreach or consumer education activity, and it does not have the resources to follow up with attendees to survey their success or failure at scam prevention.

FTC noted that it measures the number of page views to its consumer education webpages and obtains feedback from website users through a satisfaction survey. However, FTC has not measured the outcome of its outreach and education activities on individuals that attended education programs in-person or online. In response to the Stop Senior Scams Act, FTC has encouraged greater research to evaluate the effectiveness of consumer protection messages. According to FTC officials, no agency has found a way to measure or quantify how much fraud was avoided as a result of education programs. In addition, the officials noted that collecting information on the success of any workshops or trainings would

[76]In our prior work, we cited the collection of participant data by other agencies to assess the effectiveness of training, including questionnaires administered to measure behavior change in core areas. For example, we found that the U.S. Department of Agriculture regularly collects participant data to assess the effectiveness of the Expanded Food and Nutrition Education Program interventions nationwide. The Expanded Food and Nutrition Education Program participants take standardized questionnaires before and after participating in an intervention, such as a class. The Expanded Food and Nutrition Education Program administrators use this information to measure participant behavior change and report it to its reporting system to be able to assess the effectiveness of the Expanded Food and Nutrition Education Program interventions nationwide. GAO, *Nutrition Education: USDA Actions Needed to Assess Effectiveness, Coordinate Programs, and Leverage Expertise,* GAO-19-572 (Washington, D.C.: July 25, 2019).

require the Office of Management and Budget approval under the Paperwork Reduction Act.[77]

We recognize that linking outreach and other education efforts explicitly to a reduction in the number of scam victims may not be possible. However, measuring the effectiveness of the education efforts on increasing the knowledge of, and changing the behaviors of, consumers that participated in the training is possible.[78] By incorporating valid measures of effectiveness into their trainings, CFPB, FBI, and FTC could better ensure that they adequately address training objectives and thereby increase the likelihood that desired changes will occur in the target population's skills, knowledge, abilities, attitudes, or behaviors. For example, after receiving approval under the Paperwork Reduction Act, the agencies may be able to survey program participants to determine the extent to which their education activities improve program participants' ability to recognize scams and thus reduce the likelihood that participants or those they work with become victims of scams. In addition, having feedback from training participants can help agencies identify areas of weakness in their presentations so that they can continually revise and improve their training materials, as needed.

Selected Businesses Use Various Methods to Counter Scams

Selected businesses we met with use various methods to counter scams. These methods include, but are not limited to, consumer education, including information on websites and at business locations; scam notices posted at gift card displays; data analytics; and employee education.[79]

[77]44 U.S.C. §3501 et seq. The Paperwork Reduction Act requires an agency to receive clearance from the Office of Management and Budget before collecting information "by means of identical questions posed to..., ten or more persons, whether such collection of information is mandatory, [or] voluntary". 5 C.F.R. 1320.3(c)(1). FTC noted that the Paperwork Reduction Act requirements create an administrative hurdle that can limit FTC's ability to conduct posttraining knowledge or satisfaction assessments in a statistically significant manner.

[78]According to FTC, some research indicates that providing information to consumers about specific fraud can reduce the risk that someone will lose money to fraud. A study of 1,408 Americans and Canadians who were targeted and reported a scam found that prior knowledge of scams and fraud can reduce susceptibility. Financial Industry Regulatory Authority Investor Education Foundation, BBB Institute for Marketplace Trust, and the Stanford Center on Longevity, *Exposed to Scams: What Separates Victims from Non-Victims?* (September 2019), https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-what-separates-victims-from-non-victims_0_0.pdf.

[79]See GAO-24-107107 for additional information.

Consumer Education

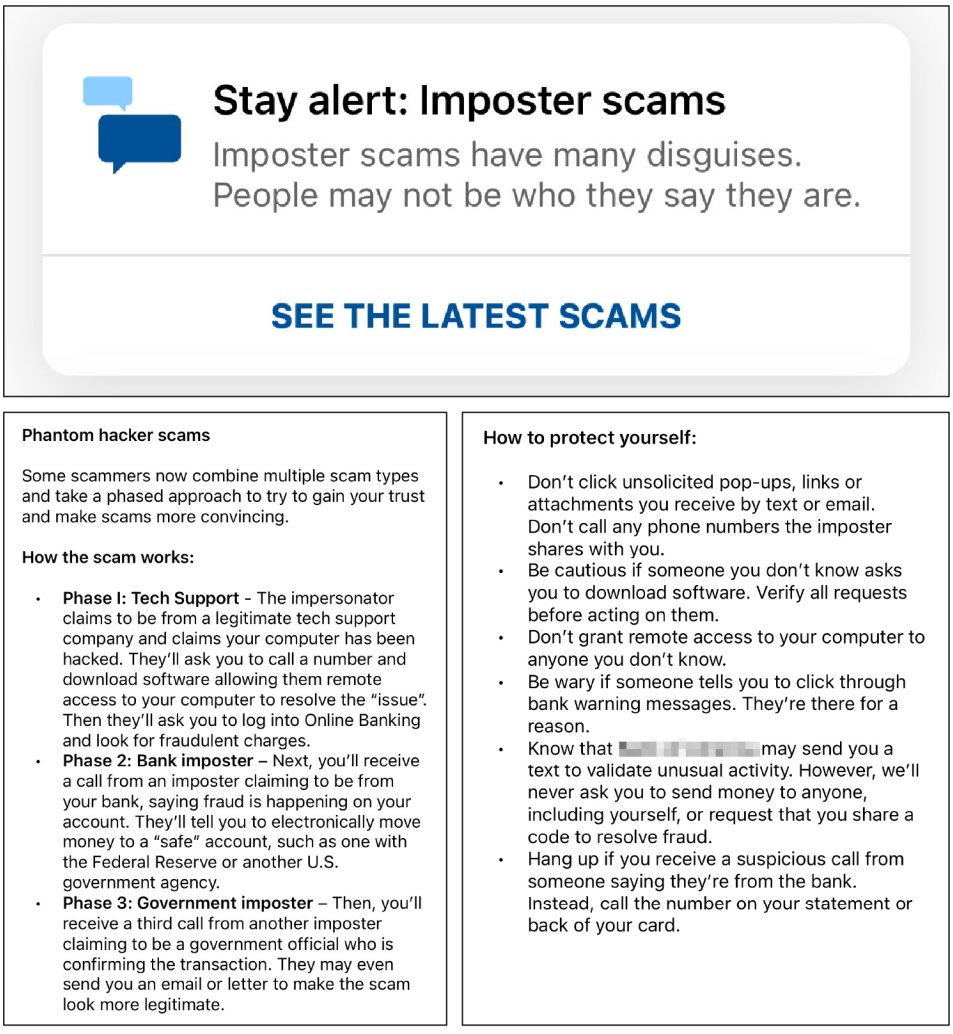
P2P service providers we reviewed offer information about scams on their websites and when consumers transmit money. MSBs also provide scam warnings on their websites. Further, representatives we spoke with from the gift card and retail industries told us they provide information about scams on their websites and at their business locations.

P2P service providers. Providers we reviewed have published scam warnings on their websites and platforms that provide information on how to protect consumer information, recognize scams, and report fraudulent activity. These education resources include warnings and messages during payment initiation, websites containing videos, information on website posts, and links to external resources. Additionally, P2P service providers noted partnerships with various nonprofit organizations, including the National Council on Aging, BBB, and the Cybercrime Support Network, to help educate consumers about scam prevention.[80]

P2P service providers also alert users of the potential for scams during transactions via in-app notifications by encouraging users to verify the identity of the recipient. During a transaction, users may be presented with notifications advising them to only send money to individuals or businesses they know or trust and with a list of potential scams they could be experiencing. See figure 5 for the different types of scam prevention notifications provided by a P2P service provider application that we accessed through different financial institutions.

[80]The National Council on Aging is a nonprofit organization supporting older adults, caregivers, professionals serving older adults, and advocates in aging policy. The Cybercrime Support Network is a nonprofit organization supporting victims of cybercrime with educational and reporting resources.

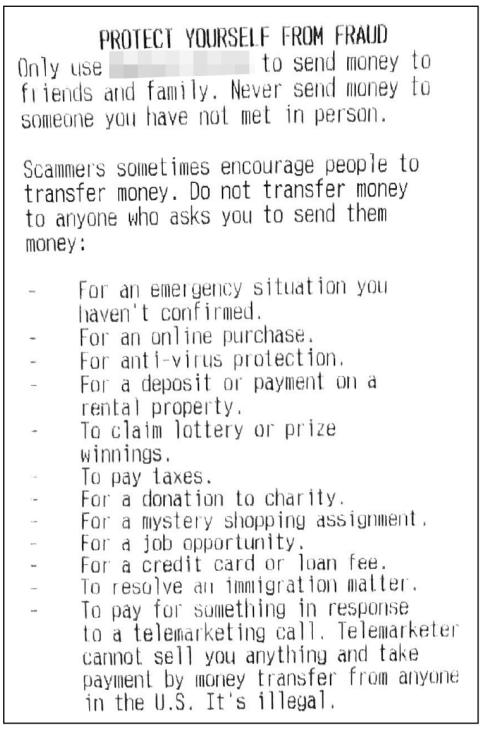
Figure 5: Examples of an In-App Scam Prevention Notification Provided by Financial Institutions



Source: Screenshots of the Peer-to-Peer Service Provider Application. | GAO-25-107088

Wire transfers. A representative from an association that represents the MSB industry told us that businesses may post warnings at locations where consumer transactions are made. Additionally, this representative told us that consumer receipts may, but not always, have consumer scam warnings. See figure 6 for an example of scam warnings on a consumer receipt.

Figure 6: Example of a Scam Prevention Warning on a Wire Transfer Consumer Receipt


PROTECT YOURSELF FROM FRAUD

Only use [redacted] to send money to friends and family. Never send money to someone you have not met in person.

Scammers sometimes encourage people to transfer money. Do not transfer money to anyone who asks you to send them money:

- For an emergency situation you haven't confirmed.
- For an online purchase.
- For anti-virus protection.
- For a deposit or payment on a rental property.
- To claim lottery or prize winnings.
- To pay taxes.
- For a donation to charity.
- For a mystery shopping assignment.
- For a job opportunity.
- For a credit card or loan fee.
- To resolve an immigration matter.
- To pay for something in response to a telemarketing call. Telemarketer cannot sell you anything and take payment by money transfer from anyone in the U.S. It's illegal.

Source: Excerpt of a wire transfer receipt. | GAO-25-107088

No federal law specifically requires financial institutions or MSBs to display consumer warnings, but we identified one state that encourages posting notices. Specifically, Massachusetts encourages its licensed money transmitters to display signage at all agent locations stating specific warnings against sending money to unknown individuals and for unconfirmed emergencies.[81]

[81]An agent is an MSB that is authorized to sell or distribute its MSB services.

Additionally, some MSBs and financial institutions provide scam warnings on their websites. Officials from a financial institution that offers wire transfer services stated that consumers requesting wire transfers at a branch location are required to sign a document that provides information about scams and affirms that their wire transfer is not associated with a scam, and another document stating that the consumer understands that a transfer cannot be unsent.

Gift cards. Gift card industry representatives we spoke with stated that there were ongoing media efforts to warn the public against providing gift card numbers to individuals as a form of payment. Industry representatives have also cited coordination with AARP and BBB to explore additional means to reach consumers. For example, BBB has published information for consumers about scams, citing information from the gift card industry.

Representatives from the gift card and retail industries told us that scam warnings to consumers are available on gift card and retail business websites. There is no federal requirement for gift card and retail business websites to display this information.

We selected a nongeneralizable sample of eight national businesses that sell gift cards to examine information on their websites about fraud scams, including the types of scams that scammers may use to obtain payment through gift cards. Five of the eight businesses we examined had information on their websites about gift card scams. Four selected gift card issuers also had similar warnings on their websites.

Scam Notices at Gift Card Displays

Gift card and retail industry representatives told us that posting notices at retail business gift card displays was a widely used method of warning consumers about gift card scams. Although there are states that require

notices, there is currently no federal requirement for businesses that sell gift cards to display such warnings.[82]

Gift card and retail industry representatives told us that some businesses include scam notices at their locations throughout the United States. One retail gift card industry representative noted that the consumer experience of observing gift card scam notices could vary, depending on the business visited, as there could be variation in store-level implementation. One gift card retail business told us that it was its standard practice to include scam notices at its locations, near gift card displays, and on the gift cards directly. Representatives from another business that issues gift cards told us that retailers often include scam warnings on the back of cards and packaging used for physical gift cards.

To better understand the consumer experience related to gift card scam notices and obtain information on the content, placement, and size of any displayed notices, we visited a nongeneralizable selection of 68 business locations in eight states and the District of Columbia representing eight national businesses that sell gift cards. Within these 68 locations, we observed 147 individual gift card displays.[83] Our observations are illustrative only and not projectable to all business locations.[84]

According to our observations, the consumer experience related to gift card scam notices can vary, depending on the specific business location

[82]Based on our conversations with a professional association, we identified three states—Maryland, New York, and Rhode Island—that have enacted legislation requiring all businesses selling gift cards within these states to display a notice at or near where any gift card is displayed or sold to warn consumers about gift card fraud. The states require that the warnings caution consumers about prepaid card scams and instruct the purchaser on what to do if they suspect they might be a potential victim. Maryland's law, which goes into effect in June of 2025, also requires that these notices state that a gift card may not be used to pay debt and also requires scam notices on the webpage where a gift card is offered for sale online or before the online sale is finalized. There are no additional content requirements. The state laws do not have requirements on the size of the notice or its location within a gift card display.

[83]For this report, we define a gift card display as a specific area within a business that displays gift cards for purchase. See app. I for additional information on the business selection criteria.

[84]A 2023 qualitative study reported that people who made gift card payments to scammers saw warning signs posted in retail stores but were coached by scammers to ignore them. Marguerite DeLiema, Julia Volker, and Arthur Worley, *Consumer Experiences with Gift Card Payment Scams: Causes, Consequences, and Implications for Consumer Protection* (2023), https://experts.umn.edu/en/publications/consumer-experiences-with-gift-card-payment-scams-causes-conseque.

visited and could even vary within a location's multiple gift card displays. For example, not every gift card display we visited had gift card scam notices. Specifically, we did not observe any gift card scam notices at any of the displays at 13 of the 68 business locations we visited, and we observed notices on 68 of the 147 gift card displays we observed.

Of the displays that did have gift card scam notices, there was variation in the notices' content, placement, and size.

Scam notice content. The scam notices we observed at gift card displays contained different types of information about gift card scams and agencies that consumers could contact for assistance.

- The notices we observed advised scam victims to contact one or more of the following agencies: CFPB, FBI, FTC, a state consumer protection agency, or local law enforcement.
- Some notices did not have agencies listed and instead provided the business' website addresses for consumers to visit for additional information.
- Some notices contained information about specific gift card scams and methods, while others warned consumers not to share their gift card number with other individuals.

Figure 7 highlights some of the different notices we observed that provide various information to consumers, including where to report scams and websites to visit for scam information.

Figure 7: Gift Card Scam Notice Examples

Gift card warning notice examples

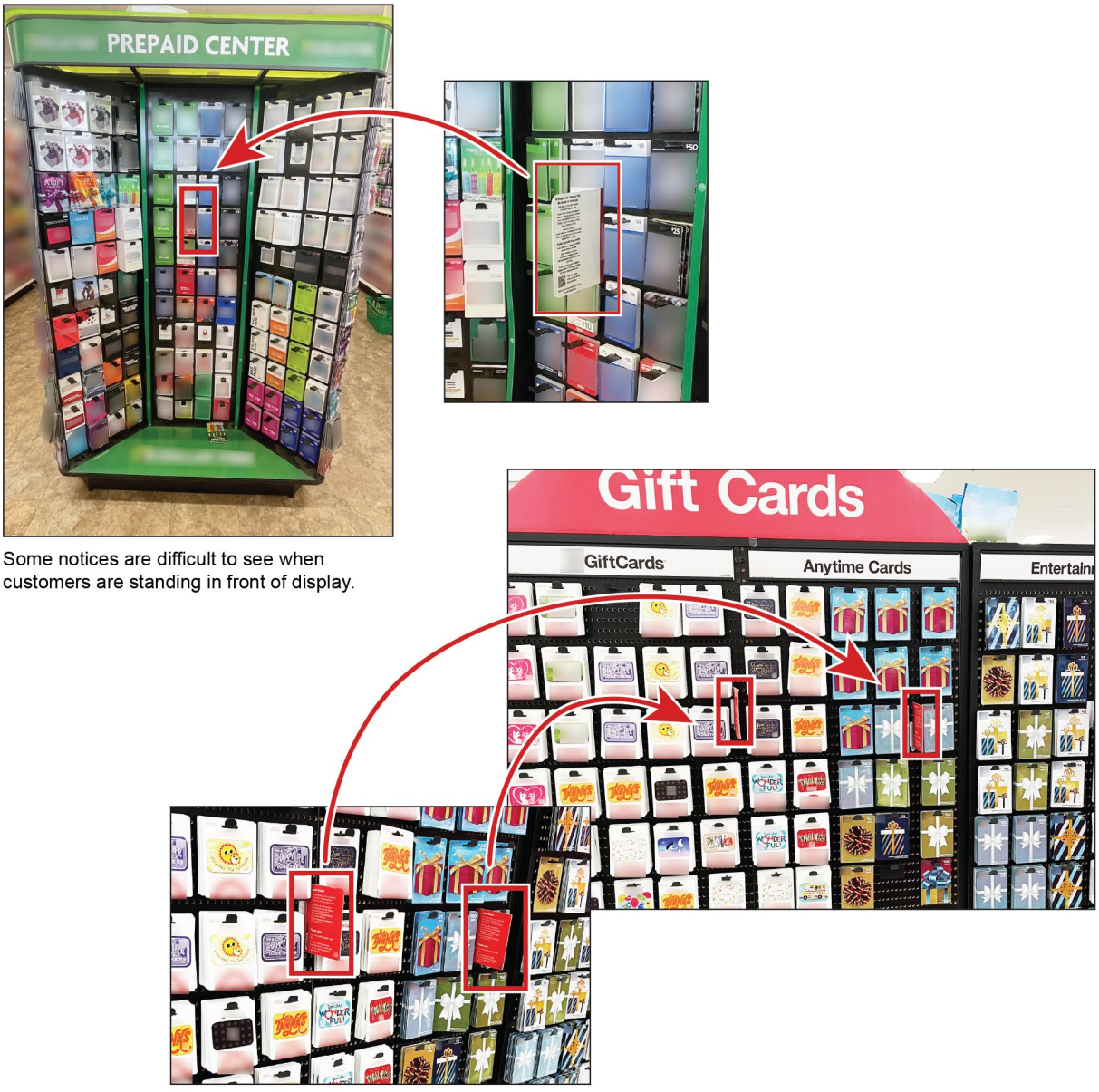
Notice refers consumers to business gift card website.

Source: GAO. | GAO-25-107088

Scam notice placement. Scam notices were placed in different locations among the displays we visited.

- Our observations included scam notices directly in the center of gift card displays, built into the display above where the gift cards were posted, on the corners of the displays, and stickers below the gift cards near the floor.
- We observed multiside gift card displays that had notices on each side of the display and those that only had a notice on one side.
- We observed that some notices were inserted into the displays perpendicular to the consumer's line of sight, which could make it difficult for consumers to see that a notice was posted, as shown in figure 8.

Figure 8: Gift Card Scam Notice Display Examples

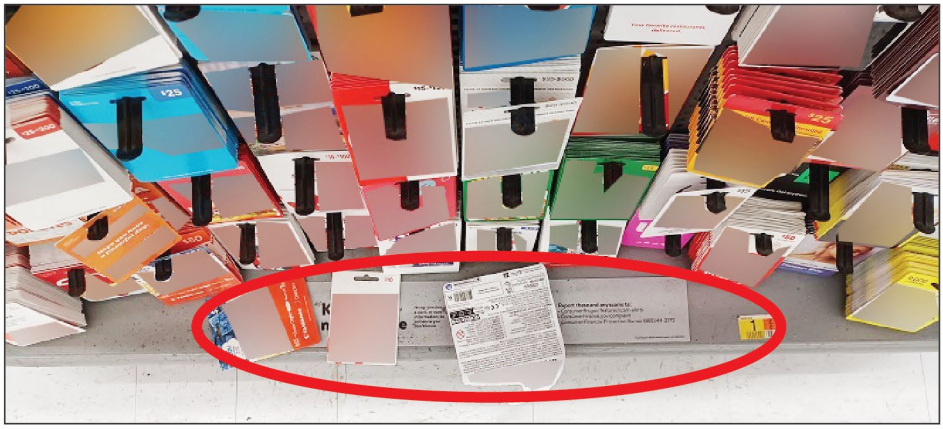


Some notices are difficult to see when customers are standing in front of display.

Source: GAO. | GAO-25-107088

- We observed that gift card notices that were facing up from the floor could be obscured by other gift cards and merchandise, as shown in figure 9.

Figure 9: Gift Card Scam Notices Obstructed by Merchandise



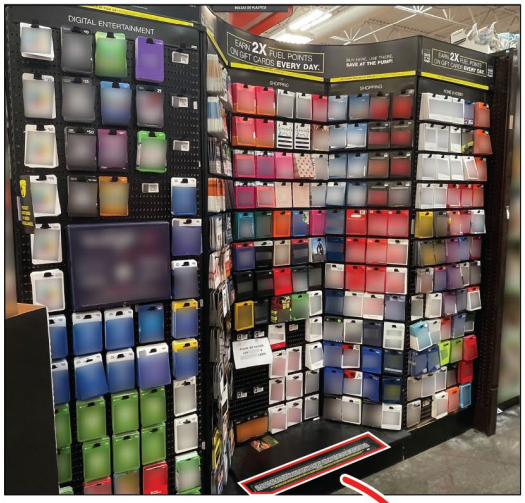
Merchandise sometimes covering the gift card notices.

Source: GAO. | GAO-25-107088

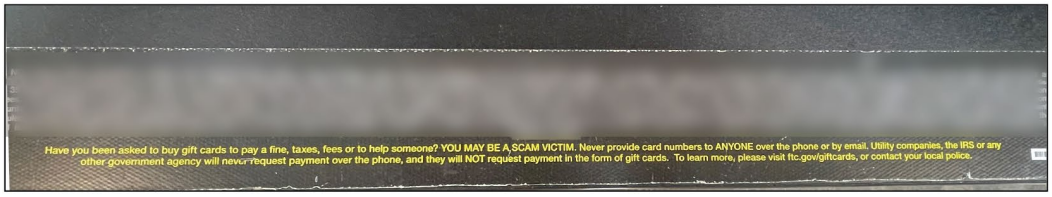
- We observed that the placement of the scam notices could vary between locations of the same business. For example, one business had two notices at eye level on a larger display, while another location owned by the same company had a sticker with small font near the floor, as shown in figure 10.

Figure 10: Gift Card Scam Notice Variation at Different Business Locations

One location of a company has two scam notices at eye level on the side of its gift card display.



Another location of the same company has a scam notice at the bottom of the gift card display, near the floor.



Source: GAO. | GAO-25-107088

Note: The yellow text above states the following “Have you been asked to buy gift cards to pay a fine, taxes, fees or to help someone? YOU MAY BE A SCAM VICTIM. Never provide card numbers to ANYONE over the phone or by email. Utility companies, the IRS, or any other government agency will never request payment over the phone, and they will NOT request payment in the form of gift cards. To learn more, please visit ftc.gov/giftcards, or contact your local police.”

Scam notice size. The size of the scam notices varied across the displays we visited.

- Some notices were larger than others, increasing the chances that they could be seen by consumers.
- Some notices were approximately the size of a gift card, potentially making them more difficult to be seen and distinguished by consumers, as shown in figure 11.

Figure 11: Examples of the Size of Some Gift Card Scam Notices

Gift card scam notices can be approximately the same size as, or smaller than, the gift cards themselves.

Source: GAO. | GAO-25-107088

Analytics

According to gift card and MSB representatives, their businesses perform analyses to block scammers from receiving funds. For example, an MSB representative told us that the company has fraud monitoring controls that can help predict indicators of fraudulent transactions and help systematically block scammers from receiving funds, put transactions on hold, or reach out to customers. A P2P service provider noted that it had developed a risk assessment tool that could be used to assess and

interdict potentially high-risk transactions, including stopping or delaying transactions in real time. Another P2P service provider noted that it analyzes transaction information, such as internet protocol address location and transaction amount, to identify suspicious activity.[85] According to a representative with a gift card retail business, gift card issuers have developed numerous controls to help protect consumers from scams. Controls include having dollar amount and card purchase limits and freezing gift cards due to patterns detected on both the original purchase and use of a gift card.

Employee Education

Retail, gift card, and MSB representatives told us that their employees were trained to be aware of scams and to identify transactions that may indicate that a consumer is being deceived by a scammer. One retail and gift card company and organizations that support the gift card and MSB industries told us their related industries train employees to identify indicators that a customer is purchasing gift cards or wiring money as part of a scam. MSB industry representatives also told us they train their employees on the most common types of fraud and indicators of fraudulent transactions. Further, MSBs often also provide training to the agent locations that offer MSB services. This training helps educate frontline associates of agent locations on the same types of fraud schemes; indicators of fraudulent transaction activity; as well as behavioral characteristics of both potential victims and perpetrators.

Like the gift card notice observations we discuss above, the training received by employees could potentially vary, depending on each individual business location. A 2022 testimony submitted to the U.S. Senate Special Committee on Aging described research supported by AARP that interviewed store managers who stated they had not received any formal training on how to detect scams or how to effectively intervene.

While conducting our gift card notice observations, we observed that one such business scam notice informed consumers that they could obtain more information from a fraud warning brochure but did not inform consumers where the brochure was located. Despite having this information on the sign, store customer service employees we spoke with at this one location did not initially know where the brochures were located. After looking for the brochures for approximately 30 minutes,

[85]An internet protocol address is one of the primary mechanisms used to define how and where information, such as text, voice, and video, moves across internet networks.

store employees found them locked in the store's safe. Although the brochures contained information about scams, they were marked with a destroy date that was more than 2 years prior to our visit.

A P2P service provider noted that it holds monthly fraud forums for its network participants to discuss fraud and scam trends, share best practices on the prevention and detection of fraud and scams, and receive feedback from participants on emerging risks. Another P2P service provider told us that it provides training about scams to new employees, including those who interact with consumers. This provider said that it also provides annual training and ad hoc training on emerging scams.

Federal Agency and Business Responses to Scam Victims Can Vary and Do Not Always Result in Victims Retrieving Lost Funds

Federal Agencies' Responses to Consumer Complaints

Federal agencies we met with record information about consumer complaints but do not generally investigate individual complaints to determine if assistance can be provided to the consumer. We asked officials from CFPB, FBI, and FTC how they respond to consumer scam complaints.

CFPB. CFPB officials told us that the agency's focus is primarily on sending consumer complaints to businesses named in the complaints or to other federal agencies that can take action. According to these officials, complaints are referred to another agency, if a business does not participate in the CFPB's complaint process.[86] Participating businesses

[86]Congress has directed CFPB to collect, monitor, and receive responses to complaints about financial products and services. Businesses sign up to respond to complaints in their company's dedicated CFPB Company Portal, which is a secure online environment that protects consumer privacy and the confidentiality of company responses. CFPB currently accepts complaints about checking and savings accounts, credit cards, personal consumer reports, debt collection, debt and credit management, money transfers, virtual currencies, and money services, mortgages, prepaid cards, payday, personal, and student loans, and vehicle loans or leases.

conduct their own investigations to determine what, if any, actions to take and provide a written response to CFPB and the consumer. Businesses are given 15 days to provide an initial response and 60 days to provide a final response. Those that do not are reflected in the CFPB's consumer complaint database as not having provided a timely response. According to the CFPB's Consumer Response Annual Report, when a company cannot act on a complaint because it was the result of fraud, scam, or business identity theft, the company can provide an administrative response that includes a statement or other evidence supporting this response.[87]

FBI. According to FBI, IC3 does not respond to each consumer complaint report received, and investigation is at the discretion of the agencies that receive complaints from IC3. IC3 analysts review complaints and disseminate information to the appropriate FBI field office or to federal, state, local, or international law enforcement or regulatory agencies for criminal, civil, or administrative action, as appropriate. FBI, in conjunction with other law enforcement agencies, may investigate cases involving scams.

According to FBI, IC3 is used to develop law enforcement referrals that focus on internet crimes with significant financial impact, large numbers of victims, or social impact on internet users. For example, 50 initial consumer complaints to IC3 about a technical support scam resulted in an FBI investigation and subsequent prosecution of multiple individuals who were orchestrating a criminal enterprise based outside of the United States. Imposters posing as technicians would pretend to perform repairs or install unneeded computer programs. The victim would be billed for the bogus work and would be instructed to send a payment of between $300 and $1,500. According to FBI, the case involved over 14,000 victims, with over $4 million in losses.

According to FBI officials, there is no specific threshold or policies and procedures stating which consumer complaints are investigated. Investigations conducted by FBI are driven by the information in each complaint, how the complaint might relate to other investigations, and available resources. According to these officials, each FBI field office prioritizes its own threats for investigation. FBI officials told us that any

[87]Consumer Financial Protection Bureau, *Consumer Response Annual Report* (Mar. 29, 2024), https://files.consumerfinance.gov/f/documents/cfpb_cr-annual-report_2023-03.pdf.

related subsequent prosecutions were not categorized by whether they were related to scams.

If certain criteria are met, IC3 can take action to freeze funds made through a domestic wire transfer. We discuss that process later in this report.

FTC. According to FTC, the agency does not resolve individual consumer complaints or generally speak to all victims about their complaints. FTC enforces the Federal Trade Commission Act, as amended, and the Telemarketing Sales Rule, among other laws and regulations.[88] As part of the FTC's enforcement authority, it files legal complaints in court for monetary relief and injunctions against companies that have engaged in unfair or deceptive business practices and, depending on the facts and circumstances, for violations of other laws and regulations, and works to get refunds to individuals, when possible. According to FTC, Sentinel complaint data are used for investigations and law enforcement actions. The complaint data are also made readily available to the members of Sentinel, which comprise users from law enforcement agencies. In addition, FTC provides self-help information to consumers, including information to help them try to get their money back, depending on the payment mechanism they used to pay a scammer. This information includes correspondence telling victims to contact the company that was used to facilitate the payment.

Federal Agencies' Scam Investigations and Prosecutions

Consumer complaints to federal agencies can result in investigations and subsequent prosecution but, as discussed above and demonstrated by our covert scenarios discussed later in this report, not all reported consumer complaints are investigated. According to federal agency and law enforcement officials, the large number of consumer fraud complaints received, limited resources, unknown identity of the scammers, the speed at which money is moved, and the sophistication of international scam operations may make it difficult to respond to each complaint and to investigate and recover funds. For example, FBI reported receiving, on average, over 2,400 internet crime complaints per day, and FTC's

[88]As codified at 15 U.S.C. § 41-58; 16 C.F.R. pt. 310. In addition to the Federal Trade Commission Act, as amended, and the Telemarketing Sales Rule, FTC also enforces several regulations that prohibit or relate to fraud. For example, Regulation E, 12 C.F.R. pt. 1005, the Business Opportunity Rule, 16 C.F.R. pt. 437, and the Rule on Impersonation of Government and Businesses, 16 C.F.R. pt. 461.

Sentinel recorded over 7,000 consumer fraud complaints per day in calendar year 2023.

According to one analysis of law enforcement data and IC3 cybercrime and scams consumer complaints, the ratio of the 2016 cybercrime arrests made and reported by federal, state, and local law enforcement agencies was 0.31 percent of the 298,728 complaints received by IC3 for that year.[89] Considering the estimated number of unreported fraud crimes could bring this ratio down to 0.05 percent. However, the study did not consider that one arrestee could be responsible for multiple reported fraud complaints. Additionally, cybercrime arrests and IC3 complaints could include crimes other than scams. For example, some of the arrests analyzed included hacking/computer invasion. Additionally, the number of arrests may be understated, as 63 percent of the country's eligible law enforcement agencies did not report their arrests to FBI that year.

According to one expert who has prosecuted scam cases and worked to recover funds for victims, many areas of the country do not have sufficient law enforcement resources to assist victims with recovering their funds.[90] This expert also believed that federal law enforcement would generally not prosecute cases involving less than hundreds of thousands of dollars in losses or assist with recovery of funds at the individual victim level.

Additionally, according to HSI, while federal law enforcement will sometimes not pursue cases that do not reach a certain threshold, most complex scams have a wide array of victims across multiple jurisdictions that could make it difficult for investigators to obtain enough information needed for DOJ prosecutors to open a case.

Although not necessarily resulting from one of the consumer-complaint contact methods discussed above, DOJ has prosecuted cases investigated by FBI, HSI, and other law enforcement agencies that involved scam victims who paid scammers through gift cards, wire

[89]Third Way, "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors" (Oct. 29, 2018), accessed May 10, 2024, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

[90]The expert is a district attorney who has educated consumers and led prosecutions related to scammers receiving money from consumers. The expert is part of the Regional Enforcement Allied Computer Team task force that combines resources and specific investigative experience, along with federal jurisdiction, to conduct investigations of scam schemes.

transfers, and other payment methods. These cases can demonstrate the scope of the scammer's operations and how consumers, including older adults, are targeted.

According to DOJ, examples of adjudicated cases include the following:

- In 2024, an individual pleaded guilty for their role in managing a call center outside the United States that was used to target and exploit older adults.[91] The call center convinced the victims to pay for computer support services they did not need and that were never actually provided. According to DOJ, this scheme generated more than $6 million in criminal proceeds from at least 6,500 victims. Co-conspirators operating in the United States moved money outside the country by wire transfer, among other means.
- In 2023, three individuals were found guilty of conspiracy to commit money laundering for scheming to launder the proceeds of a transnational gift card fraud ring that targeted older adults and other victims. Overseas criminals posing as law enforcement, other government personnel, and businesses engaged in scams to obtain gift card numbers from victims as payment to avoid jail, a Social Security number issue, or other problems. According to court documents, these criminals provided more than 5,000 gift card numbers that were stolen from consumers to the defendants. The gift cards were valued at over $2.5 million. The defendants used the gift card numbers to purchase consumer electronics and other items. The electronics were resold.
- In 2023, three individuals were found guilty of conspiracy to commit wire fraud and mail fraud and conspiracy to commit money laundering for their roles in a scam based outside of the United States that involved contacting older adults and falsely claiming they had won prizes and needed to pay the scammers fees to collect their earnings. Victims transmitted funds through a P2P service, wire transfers, and other methods. According to DOJ, the scammers used lists containing the names and personal information of older adults to contact potential victims.[92]

[91]The individual pleaded guilty to conspiracy to commit wire fraud and conspiracy to intentionally damage victims' computers.

[92]According to the DOJ press release for this case, scammers are often able to identify prospective victims using "lead lists," which are lists of individuals who fit certain demographic features or other criteria that allow scammers to target their intended victims more efficiently.

- In 2024, one individual was convicted for their role in a scheme that defrauded U.S. victims of over $4 million from a call center outside the country. According to DOJ, scammers posed as U.S. government officials and convinced victims, including older adults, that they would receive financial prizes if they first paid taxes and other fees. As part of their efforts to deceive victims, the scammers used Voice over Internet Protocol technology to make it appear as though they were calling from locations in the United States.[93]

According to DOJ officials, the biggest challenge in prosecuting scam cases is establishing the identity of the scammers. As we discussed earlier in this report, scammers could be operating from foreign call centers as part of sophisticated criminal operations.

Consumer Recovery of Scam Funds

Officials from businesses, agencies, and individuals knowledgeable about scams we spoke with told us that funds are generally difficult to track and recover once they have been obtained by scammers. Recovery success also varies based on how quickly consumers report the scam, payment method, fraud type, and cooperation among banks and jurisdictions. However, there may be some instances where funds sent by a consumer to a scammer can be frozen or recovered before they are retrieved or, in the case of gift cards, depleted by a scammer. Below is a summary of consumer scam recovery mechanisms that may be available to consumers from depository institutions, money services providers, gift card companies, and P2P service providers. There are three mechanisms that may be used to recover funds. Specifically, (1) fund transfers may be able to be stopped or frozen; (2) consumers can try to obtain reimbursement from a financial institution; and (3) in some cases, consumers may be able to receive restitution through agencies or a court.

Stopped or Frozen Fund Transfers

Consumers can attempt to intervene soon after they send funds to a scammer to try to stop or freeze the funds. We discuss below how this can be done with the wire transfer, gift card, and P2P methods that consumers might have used to send funds or something of value (gift card number) to a scammer.

Wire transfers. In situations where consumers sent funds to a scammer through a wire transfer, consumers may be able to contact their

[93]Voice over Internet Protocol is a technology that allows individuals to make voice calls using a broadband internet connection instead of a regular (or analog) phone line. Voice over Internet Protocol can allow individuals to make a call directly from a computer, a special phone, or a traditional phone connected to an adapter. Service providers may permit individuals to select an area code different from the area in which they live.

depository institution or money services provider to request that it attempt to stop and retrieve the funds before the transaction has been completed. However, unless the wire transfer was pended for further review, there is no way to stop a wire once it is submitted. The recipient financial institution may have the ability to retrieve the funds before a scammer withdraws or transfers funds from an account, but the success of this depends greatly on the timing of reporting. Any attempts to recover funds require the consumer to notify their financial institution or the money services provider quickly after they initiated the transaction, so a recall request can be submitted. Representatives from the money services industry told us that there may also be situations where they could return funds to a victim while the transaction was in progress. They also explained, however, that little could be done once funds from the wire transfer had been retrieved by scammers.

In some cases, FBI can assist with freezing and returning funds to consumers who make bank-to-bank wire transfers to domestic financial institutions under fraudulent pretenses. Since its establishment in 2018, the FBI's Recovery Asset Team has acted on some IC3 consumer complaints by providing complaint transaction details to financial institutions receiving the transfers. According to FBI, individuals must immediately report information about their money transfer to IC3 for the program to be effective. For example, reports made within 24 hours of making the transfer have an 80 percent recovery rate versus reports made within 72 hours, which have a 0 percent recovery rate. Action is not taken by the Recovery Asset Team on all wire transfer complaints, as certain criteria must be met, such as the dollar threshold of the wire transfer. According to FBI officials, more than $2 billion has been frozen through this program since its inception through fiscal year 2023.

Similarly, FinCEN collaborates with U.S. law enforcement and foreign partner agencies through the Rapid Response Program that works to freeze funds sent through wire transfers to certain international jurisdictions under fraudulent pretenses. For this process to begin, consumers must file a complaint with one of FinCEN's four Rapid Response Program federal law enforcement partners. According to FinCEN officials, the Rapid Response Program works in partnership with FBI, Secret Service, HSI, and U.S. Postal Inspection Services to interdict, freeze, and support the recovery of funds stolen through cybercrime. These officials also stated that if FinCEN receives a referral from one of these law enforcement agencies that meets certain criteria, and the victim's funds have left the United States, it can work with foreign jurisdictions to attempt to freeze and return the victim's funds.

Gift cards. Gift card industry representatives we spoke with told us that companies may be able to freeze gift card balances, if a consumer reports the fraud to the retailer or issuer of the card. One gift card retail business told us that some retailers reimburse consumers for all or part of the value of a gift card, if they can freeze the balance. However, representatives from multiple organizations told us that scammers work to make purchases with the fraudulently obtained gift card balance as quickly as possible. These representatives explained there was generally nothing that could be done to retrieve and return the victim's funds once the gift card balance had been spent by the scammer. One gift card industry representative told us that gift cards were like cash. Once a scammer had spent that gift card balance, money could not be retrieved.

HSI officials explained that they had developed and currently use technology to decode information on gift cards to determine the monetary value contained on the cards. These officials stated that this technology can be used to freeze suspected victim funds to facilitate victim restitution without relying on coordination with the issuing retailer.

P2P. Depending on the P2P company, consumers may be able to request the P2P company to stop the transaction and retrieve the funds before the transaction has been completed.

Financial Institution Reimbursement

Consumers can report scams to their financial institutions at any time, including after the transaction has settled and the funds can no longer be frozen. However, the timeliness of notifying the financial institution of a scam involving an electronic fund transfer can affect a consumer's liability for the transaction.[94] Generally, if a consumer is induced to authorize a payment from their account to pay a scammer, then the consumer may be responsible for the payment under federal law. In contrast, if an unauthorized payment is made from a consumer's account, the consumer may not be held responsible for the payment in its entirety; rather, the financial institution holding the account may bear some responsibility.

If a consumer reports a fraudulent payment to a financial institution, that institution is required to investigate the transaction to determine whether

[94]12 C.F.R. § 1005.6(b). Regulation E applies to electronic fund transfers, which means any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. 12 C.F.R. § 1005.3(a), (b). There are also exclusions from the definition of electronic fund transfer. 12 C.F.R. § 1005.3(c). When we use the term "payment" in this section, we mean electronic fund transfer as defined in Regulation E, unless otherwise stated.

the consumer or the financial institution is responsible for the payment, pursuant to its error resolution obligations under federal law. The financial institution's investigation determines whether the payment was authorized or unauthorized, among other facts and circumstances, and who bears the responsibility for the payment and in what amount.[95] Payments made using a gift card are not entitled to these protections pertaining to reimbursement for unauthorized payments and resolving of errors.[96]

Officials from a P2P service provider told us that they generally do not reimburse consumers who authorize a transaction for a scam, as they generally are not required to do so under federal law. We identified two companies that offer purchase protection in which, depending on the specifics of the plan, consumers may be eligible for reimbursement in the case of certain items purchased but not received, or significantly not as described. These companies will, however, as required under regulations, reimburse consumers in cases of unauthorized transactions that result from an access device (such as a card, code, or other means of access to a consumer's account) being stolen by a fraudster.

A P2P service provider has announced that victims of certain qualifying imposter scams may be eligible for reimbursement. However, consumers who authorize transactions for other types of scams may not be able to get their money back. According to information posted to consumers on this provider's website, consumers are told to contact their financial institutions for possible assistance.

Consumer Restitution

In some situations, after the conclusion of legal action, consumers could be eligible for, or ordered by a court, to receive restitution. However, these consumers may not necessarily receive the full amount of funds lost.

FTC consumer restitution. As part of the FTC's enforcement authority, the agency has filed complaints for permanent injunction and monetary

[95]The Electronic Fund Transfer Act, as implemented by Regulation E, is the primary federal law that governs liability for a scam involving an electronic fund transfer. Regulation E applies to financial institutions, which covers both depository institutions, such as banks and credit unions, and nondepository institutions, which can include entities such as P2P companies and certain wire transfer providers to the extent that they provide international remittances. For a description of payments that result in required reimbursement by financial institutions under Regulation E, see GAO-24-107107.

[96]See 12 C.F.R. § 1005.20 regarding consumer protections for gift cards and gift certificates.

relief against companies and individuals that have perpetrated or facilitated scams, according to the agency.[97] In most cases, money recovered does not go directly from the defendant to the victims. Generally, once an FTC lawsuit or settlement is final and the defendants have paid the money ordered by the court, if any, or agreed to in settlement, FTC develops a plan for returning funds to affected victims, when possible. According to FTC, resolutions of their cases may not result in victims receiving the entirety of their lost funds, particularly in matters where the scammers have dissipated much of the stolen assets. Additionally, consumers may not be able to recover funds until years after the scam transactions were made, due to the time required for investigation and litigation.

As of January 2025, FTC had over 80 active refund programs, including, but not limited to, returning money to victims of scams, as well as other types of fraud and deceptive business practices. In fiscal year 2024, FTC issued consumer refunds totaling $319 million.[98] According to FTC officials, as of September 2024, consumers have received refunds associated with two FTC settlements totaling $700 million. These refunds are related to two cases involving two MSBs used by consumers to wire money to scammers around the world.[99] As part of these settlement agreements, consumers who transmitted money using these MSBs during a specific period were eligible to receive some, or all, of their money back, using the settlements paid by the businesses. In these cases, the MSBs were held liable for either failing to comply with anti-money-laundering laws or not having an effective antifraud program, among other violations; however, the perpetrators of the underlying scams were not party to this action.[100]

Court-ordered restitution. Criminal proceedings resulting from scam investigations, such as the prosecutions discussed earlier in this report,

[97]A permanent injunction is a court order requiring a person or business to do or cease doing a specific action that is issued as final judgement in a case.

[98]Salesforce Inc., *FTC Refunds to Consumers, Fiscal Year: 2024,* https://public.tableau.com/app/profile/federal.trade.commission/viz/Refunds_15797958402020/RefundsbyDate.

[99]Investigations conducted by DOJ, FTC, and other law enforcement organizations determined that these businesses aided and abetted, or otherwise facilitated, consumer scam schemes.

[100]Although not part of the settlement with MSBs, according to FTC, several of the scammers involved were criminally prosecuted by DOJ and other authorities prior to the FTC's actions against the MSBs.

could result in court-ordered restitution to victims. One DOJ official stated that it could take years for a restitution order to be issued and would not necessarily constitute the type of restitution most victims would be hoping for. According to DOJ, the chance of full financial recovery from restitution is very low.

Remission. Remission allows victims to recover financial losses that have been seized by law enforcement. Specifically, victims can receive remission of funds forfeited by law enforcement agencies participating in the DOJ or Treasury forfeiture funds, through petitions. Victims can petition in both administrative and judicial forfeiture cases.[101]

For example, one retailer noticed a pattern of scams where scammers directed victims to purchase gift cards and froze the balances of the gift cards that were connected to this suspected activity before the balance could be transferred to the scammers. Based on this conduct, DOJ filed a complaint for forfeiture of $3.9 million, representing the gift card balances frozen by this retailer. The money seized by DOJ in relation to this action was available to victims who filed a petition for remission.

Results of Covert Scenarios for Selected Federal Agencies and Businesses

Our covert scenarios of how federal agencies and businesses responded to consumer complaints about scams found that responses to victims varied by federal agency and business and payment method used. As part of our covert scenarios, we conducted seven gift card and wire transfer transactions and submitted consumer scam complaints for each transaction to CFPB, FBI, and FTC. Specifically, we submitted five impersonation scam complaints (including government, charity, business, and utility company impersonation), one investment scam complaint, and one sweepstakes scam complaint to each of the three agencies. In these complaints, we claimed to be victims of a scam, having voluntarily wired funds or provided gift card information to a scammer. We also submitted consumer complaints to an MSB and four gift card issuers to determine how they would respond to consumer complaints.

Our covert scenarios included consumer complaints submitted by adults with an age range between 20 and 64 to determine whether the agency or business response varied by age. We submitted our consumer complaints to the federal agencies and businesses within 1 to 3 days of the transaction. We did not assess whether the businesses should or should not reimburse financial losses incurred by consumers in

[101]28 C.F.R. Part 9.

accordance with applicable law. The results of our covert scenarios are illustrative only of the consumer complaints we submitted and responses we received and are not generalizable to other consumer complaints received by federal agencies and businesses or their responses.

The results of our covert scenarios involving businesses varied. In some instances, we were successful in retrieving transmitted funds and, in others, we were referred to a federal agency, such as CFPB or FTC. The response from federal agencies also varied by agency. Some agencies responded with additional education materials and a list of steps the consumers could take. Others did not contact us (i.e., the covert consumer) after the complaint was filed. See figure 12 for a summary of experiences with covertly submitted consumer complaints to selected federal agencies and businesses. See appendix I for additional details on the methods used for our covert scenarios.

Figure 12: Summary of Experiences of Covert Consumer Complaints Submitted to Selected Federal Agencies and Businesses

	Response to complaints			
	Business	CFPB	FBI	FTC
5 scenarios involving gift cards 	• **Issuer A:** Submitted one complaint. Gift card issuer directed complainant to FTC to obtain a refund. • **Issuer B:** Submitted one complaint. Gift card issuer refunded the balance on the gift card. • **Issuer C:** Submitted one complaint. Gift card issuer provided consumer protection information and informed the complainant that there may be no future correspondence from the business. • **Issuer D:** Submitted two posts in a public forum because issuer had the option to post complaints in a public forum for other consumers to provide assistance.	• One complaint was referred to the gift card issuer. • Four complaints were not referred due to the gift card issuer not being in their system or the agency not handling such complaints.	• Following each of the five complaint submissions, the web-based complaint system recommended contacting local law enforcement, the complainants' financial institution, and provided links to information about scams and consumer alerts.	• Following four complaint submissions, the web-based complaint system recommended contacting the gift card issuer. • Following one complaint submission, the web-based complaint system did not provide information specific to gift cards but did provide a link to report to FTC if a scammer had the complainant's personal information, such as the Social Security number. The complainant was also advised to hang up on robocalls. • The responses to all five complaints provided links to educational resources on the FTC's website.
2 scenarios involving wire transfer 	• **Wire Transfer Company A** (two separate locations): Following two complaint submissions, the business submitted both complaints to a law enforcement database, provided educational resources, and did not assist with recovery due to funds already withdrawn from the account.	• Both complaints were referred to the wire transfer company. • One location stated they could not recover the funds. • One location stated they blocked the payee and did not recover the funds.	• Following two complaint submissions, the web-based complaint system recommended contacting local law enforcement, the complainants' financial institution, and provided links to information about scams and consumer alerts.	• Following two complaint submissions, the email-based response recommended contacting the wire transfer provider and provided links to educational resources on the FTC's website.

CFPB: Consumer Financial Protection Bureau
FBI: Federal Bureau of Investigation
FTC: Federal Trade Commission

Source: GAO analysis. | GAO-25-107088

We also attempted six P2P payment transactions through two different payment apps to see how businesses and agencies would respond to complaints with this payment method; however, these transactions were unsuccessful. The two P2P payment companies blocked our transactions, citing suspicious activity on the accounts. Therefore, we did not submit

scam complaints to these two companies or P2P-related complaints to federal agencies. Further, we attempted to open accounts with financial institutions to perform two bank transfers and determine how the financial institutions would respond to the complaints.[102] The financial institutions' internal controls prevented us from opening the accounts. Consequently, we did not perform the bank transfers and submit scam complaints to the financial institutions or appropriate federal agencies.

Scam Complaint Responses by Selected Federal Agencies

The federal agencies' responses to the complaints we submitted through covert scenarios varied. Some agencies responded with additional education materials and a list of steps the covert consumers could take. Others did not contact us (i.e., the covert consumer) after the complaint was filed. Agency responses did not differ for older adult complainants.[103]

CFPB. We submitted seven scam complaints to CFPB through the agency's online complaint form. For our five complaints in which we cited gift cards as the scam payment method,

- CFPB responded to one of the five complaints with an email stating the agency had submitted the complaint to the appropriate business for a response and that we would receive a status update within 15 days. We did not receive an update from CFPB; and
- for the remaining four complaints, CFPB responded with emails stating that the agency was unable to forward our complaint to the appropriate business for a response. It said it could not forward the complaints because the company was not in the agency's complaint system, or because the agency did not handle such complaints. The correspondence we received for each of these complaints stated that the complaints had been provided to the FTC's Sentinel and noted that FTC could not resolve individual complaints. As discussed earlier in this report, some gift card scam warnings inform consumers to contact CFPB, if they have been the victim of a gift card scam.

For our two complaints involving two separate transactions related to one MSB—in which we cited wire transfer as the scam payment method—CFPB responded with an email stating that the agency had submitted the complaint to the appropriate business for a response and that we would receive a status update within 15 days. We received an update from the

[102]Bank transfer is the direct transfer of funds from one bank account into another.

[103]According to FTC, its response to consumer complaints changed after we conducted our covert tests. As of August 1, 2024, FTC provides additional information specific to older adult consumers who report that they are 60 or older.

MSB on the two complaints, through CFPB, in less than 15 days. For one of the complaint submissions, the MSB response stated that the wired funds sent due to a scam could not be refunded because they had already been paid to the intended payee. For the second complaint submission, the MSB response stated that it had taken action to block the payee (after the funds were transmitted) and advised us to review the business's social media channels and its fraud awareness website to learn more about fraud protection. This complaint did not result in a refund because the MSB did not recover the funds after they were transmitted.

FBI. We submitted our seven scam complaints to IC3 through the agency's online complaint form. We were notified on the IC3 online complaint site after the complaint form was submitted that the report would assist FBI with tracking and understanding the crime and noted that the consumer would be contacted if additional information was required. We did not receive an email or a phone call from FBI after submitting the complaints; however, FBI is not required to respond to the consumer.

The IC3 website recommended that we contact local law enforcement and our financial institution, if there was a monetary loss. Additionally, the website included hyperlinks to educational resources regarding staying safe online, common scams, and consumer alerts.

FTC. We submitted our seven scam complaints to FTC through the agency's online complaint form. For each of the complaints submitted to FTC, we received an email confirmation providing information on the next steps the consumer can take and links to learn more about different types of scams on the FTC's website. Each email from FTC also stated that the agency did not resolve individual complaints but the complaints would be available to federal, state, and local law enforcement. No additional communication was received from FTC. In this regard, like FBI, FTC is not required to respond to the consumer.

The nature of next steps the consumer can take, and the education material cited, varied based on the details of the complaint submitted. For our five complaints in which we cited gift cards as the scam payment method,

- the FTC's emailed responses to four of the five complaints stated that the consumer should quickly contact the gift card issuing business

and included a link with contact information for multiple gift card issuers; and

- the FTC's response to one complaint did not include information about contacting the gift card issuing business but stated that hanging up on robocalls and creating new passwords used to log in to personal accounts were steps that the consumer could take.

The FTC's responses to both complaints in which we cited wire transfer as the payment method informed the consumer to quickly contact the financial institution or the MSB that did the wire transfer and ask for the transfer to be reversed. The FTC's response noted that the transfer was unlikely to be reversed.

Scam Complaint Responses by Selected Businesses

The gift card issuing companies and the MSB to which we submitted scam complaints through covert scenarios provided some resolution of the complaint, or consumer-education materials. We submitted our complaints via phone or online.

Gift cards. We submitted five complaints to four different gift card issuing companies stating that we were induced by a scammer to purchase gift cards and provide gift card numbers as a form of payment.[104] Two of the complaints were submitted over the phone, and three were submitted following instructions on the issuer's website. The financial losses we reported ranged from $400 to $1,000. The gift cards we purchased still had a balance on them at the time of our complaint. As a result, our covert scenarios do not reflect the outcome of a complaint when a scammer has already spent the gift card balance.

- One gift card company froze the funds on the card so that a potential scammer could not continue using it and directed us to contact FTC to obtain a refund.[105] When we contacted FTC, the correspondence from the agency stated to contact the gift card company. As previously noted, FTC stated that it does not investigate individual complaints.

[104]One gift card issuer resolved two gift card purchases with one consumer complaint.

[105]According to FTC officials, however, FTC cannot issue refunds and can only issue redress as part of law enforcement actions it has taken and pursuant to court orders or settlement agreements with defendants.

- One of the five complaints resulted in the gift card issuer refunding the balance on the card. Specifically, after we submitted proof of purchase, the issuer sent a check for the gift card amount.[106]
- One of our complaints resulted in the gift card issuer sending us an email thanking us for the report and stating that we might not hear from the issuer again regarding our complaint. That email also provided four consumer protection tips against scammers.
- We submitted two complaints to another gift card company regarding two different gift card transactions and covert scenarios. When making one complaint, we selected the option to report the scam to the company. When making the second complaint, we selected the "contact us" option on the company's website. With both selections, we were given the option to post our complaints in a public forum for other consumers to provide a response. We made separate posts in the public forum for each of the two covert scenarios. We did not receive any additional information or responses regarding these two complaints, including the one where we asked the company to contact us.

Wire transfers. We submitted two complaints to an MSB stating that we were persuaded by a scammer to wire money. We submitted one complaint over the phone and the other complaint via the MSB's consumer complaint site. The financial losses we reported were $350 and $900.[107]

- When submitting the complaint over the phone, the MSB requested that we provide details regarding the scam, permission to submit the complaint details to a law enforcement database, and additional details on the scammer and method of contact. The MSB also asked if we had read the disclaimer (prior to sending the wire transfer) about not sending money to people we do not know. When sending the payment, we did not receive a verbal disclaimer or notice any posted scam warning in the store. However, there was a scam warning at the end of the "Terms and Conditions" and additional information on scams at the bottom of the receipt provided by the MSB. During the call, the MSB noted that we should only use its service to send money

[106]The covert scenarios were not designed to test the business controls for providing reimbursement to consumer complaints on scams. Each business has its own terms of service and reimbursement policy.

[107]The covert scenarios were not designed to test the business controls for providing reimbursement to consumer complaints on scams. Each business has its own terms of services and reimbursement policy.

to friends and family and provided the company's website link to additional fraud awareness materials. The MSB noted that it will block the scammer so it can no longer use the service. We received no additional communication regarding the phone complaint.

- When submitting the complaint online, we noted that there was a disclaimer on the MSB's website on reporting fraud. Specifically, the disclaimer stated that if we have been a victim of a fraud and the transfer has not been paid, to call the hotline as soon as possible. The online form requested details regarding the scam and permission to submit the complaint details to a law enforcement database. After submitting the complaint online, a link was provided regarding fraud prevention information available on the company's website. We received no additional communication regarding the complaint submitted online.

Conclusions

Scams are a growing problem in the United States and around the world in both scope and sophistication. Criminal organizations operate using a network of scammers to target victims and defraud them of their money. They have caused individual victims to lose tens of thousands of dollars and, in some cases, their entire life savings and to experience emotional distress.

Officials from the 13 federal agencies we spoke with reported they were engaged in a range of activities related to countering scams. However, each agency has its own mandate and authority, with each largely carrying out these activities independently. In carrying out their activities, they are not guided by a government-wide strategy to counter scams. While related strategies exist, none of them function as a comprehensive, government-wide strategy to counter scams. They are either agency-specific plans or do not focus on scams. The absence of a comprehensive, government-wide strategy poses risk for fragmentation of effort and overlap of activities, which can reduce their impact in protecting consumers. The desirable characteristics of such strategies include clear organizational roles, goals, and performance measures to gauge and monitor results, among other characteristics. Having a comprehensive, government-wide antiscam strategy with these characteristics would strengthen the ability of federal agencies to coordinate and strategically target their efforts to counter scams and thus help prevent consumers from becoming victims.

Although most scams go unreported, consumers can make fraud complaints, including those related to scams, to multiple federal agencies. CFPB, FBI, and FTC publish annual, publicly available reports

summarizing their complaint data. However, the data that these reports are based on have limitations that affect the ability of agencies to estimate the number of complaints and associated dollar losses related to scams. Since agencies largely counter scams independently, no single, government-wide estimate of the total number of scams and related financial losses, including losses from unreported incidents, exists.

Similarly, federal agencies have not produced a common, government-wide definition of scams in general or the various types of scams. Such a definition would help agencies to collaborate and produce an estimate of scams, as well as to coordinate their respective activities to counter scams. Developing a government-wide definition of scams and improving consumer scam complaint reporting could assist agency efforts to compare data across agencies, develop an overall estimate of the total number of scams, assess trends, target preventative efforts, measure progress in scam prevention, and inform an antiscam strategy. Improved data collection, estimates, and understanding regarding scams would help government agencies, Congress, industry, and the public have the information needed to accurately determine the extent of this type of crime and develop the necessary means to counter it.

Federal agencies have made efforts to educate consumers about scams through consumer alerts and training. However, they do not measure the effectiveness of these consumer education efforts on the consumers that participate in the training. By measuring the effectiveness of consumer education activities on program participants, CFPB, FBI, and FTC may be able to determine the extent to which their education activities affect the ability of training participants to recognize and protect themselves from scams and obtain information to inform adjustments to training materials.

We recognize the challenges involved in, for example, arriving at a common definition of what constitutes a scam, estimating the extent and nature of scams affecting consumers and associated financial losses, and crafting a government-wide strategy to guide federal agencies in countering scams. However, undertaking these types of activities would help ensure an effective federal response to a significant risk to consumers from a type of crime that is growing in scope and sophistication.

Recommendations for Executive Action

We are making a total of 16 recommendations—five to CFPB, six to FBI, and five to FTC. Specifically:

The Director of FBI should lead a U.S. government effort to develop and implement a government-wide strategy to counter scams and coordinate related activities. This effort should be done in collaboration with the Director of CFPB, the Chair of FTC, the Secretary of the Treasury, and other agencies, as appropriate (through their designees). This effort should address issues such as a common definition for scams; consumer complaint reporting; related types/granularity/aggregation of data, risks, and responses; a government-wide estimate of this type of crime; and coordination of federal and business activities. As appropriate, and consistent with desired characteristics, a strategy should also define agency roles, responsibilities, and authorities; identify necessary resources; and identify any legislative, regulatory, or administrative changes needed to enable a comprehensive, coordinated response. (Recommendation 1)

The Chair of FTC should, in collaboration with CFPB, FBI, and other major contributors, explore ways to harmonize data collection and contributions to Sentinel to better identify scams, such as consistently collecting data on scam type, dollar loss amount, payment method, and other data fields, as appropriate. (Recommendation 2)

The Director of CFPB should, in collaboration with FTC, explore ways to harmonize data collection to better identify scams, such as consistently collecting data on scam type, dollar loss amount, payment method, and other data fields, as appropriate. (Recommendation 3)

The Director of FBI should, in collaboration with FTC, explore ways to harmonize data collection to better identify scams, such as consistently collecting data on scam type. (Recommendation 4)

The Director of CFPB should use the agency's data collection and analysis to produce and report an estimate of the number of complaints it receives and the associated financial losses resulting from scams. (Recommendation 5)

The Director of FBI should use the agency's data collection and analysis to produce and report an estimate of the number of complaints it receives and the associated financial losses resulting from scams. (Recommendation 6)

The Chair of FTC should use the agency's data collection and analysis to produce and report an estimate of the number of complaints it receives

and the associated financial losses resulting from scams. (Recommendation 7)

The Director of CFPB should, in collaboration with FBI, FTC, and other agencies, as appropriate, develop and report a single, government-wide estimate of the number of consumers affected by, and dollar losses resulting from, scams, factoring in an estimate of incidents not reported. (Recommendation 8)

The Director of FBI should, in collaboration with CFPB, FTC, and other agencies, as appropriate, develop and report a single, government-wide estimate of the number of consumers affected by, and dollar losses resulting from, scams, factoring in an estimate of incidents not reported. (Recommendation 9)

The Chair of FTC should, in collaboration with CFPB, FBI, and other agencies, as appropriate, develop and report a single, government-wide estimate of the number of consumers affected by, and dollar losses resulting from, scams, factoring in an estimate of incidents not reported. (Recommendation 10)

The Director of CFPB, prior to developing a single estimate of the number of consumers affected by, and dollar losses resulting from, scams, should adopt the definition of scams developed by the Federal Reserve or work with FBI and FTC and other affected agencies to develop and adopt a common definition of scams and related scam types. (Recommendation 11)

The Director of FBI, prior to developing a single estimate of the number of consumers affected by, and dollar losses resulting from, scams, should adopt the definition of scams developed by the Federal Reserve or work with CFPB and FTC and other affected agencies to develop a common definition of scams and related scam types. (Recommendation 12)

The Chair of FTC, prior to developing a single estimate of the number of consumers affected by, and dollar losses resulting from, scams, should adopt the definition of scams developed by the Federal Reserve or work with CFPB and FBI and other affected agencies to develop a common definition of scams and related scam types. (Recommendation 13)

The Director of CFPB should establish metrics and a plan to measure the effectiveness of its antiscam training on the stakeholder organizations and consumers that receive it through in-person events or webinars. This

could include understanding the training's effect on consumers' ability to recognize and protect themselves from scams. (Recommendation 14)

The Director of FBI should establish metrics and a plan to measure the effectiveness of its antiscam training on the consumers that receive it through in-person events or webinars. This could include understanding the training's effect on consumers' ability to recognize and protect themselves from scams. (Recommendation 15)

The Chair of FTC should establish metrics and a plan to measure the effectiveness of its antiscam training on the consumers that receive it through in-person events or webinars. This could include understanding the training's effect on consumers' ability to recognize and protect themselves from scams. (Recommendation 16)

Agency Comments and Our Evaluation

We provided a draft of this report, for review and comment, to CFPB, FBI, Executive Office for the United States Attorneys, FTC, FDIC, Federal Reserve, Department of Health and Human Services, National Credit Union Administration, OCC, FinCEN, State, Secret Service, and HSI.

The FBI, FTC, Federal Reserve, FinCEN, and HSI provided technical comments, which we incorporated, as appropriate. CFPB, Executive Office for the United States Attorneys, FDIC, HHS, National Credit Union Administration, OCC, Secret Service, and State had no comments.

Letters from FBI, FTC, and National Credit Union Administration are reprinted in appendixes III, IV, and V, respectively. We summarize below the comments from FBI and FTC. FBI agreed with three of the six recommendations directed to it. FTC neither agreed nor disagreed with the five recommendations directed to it.

In addition, we provided excerpts of this draft report to businesses, trade organizations, and industry groups that were part of our review to help ensure the accuracy of our report. We received technical comments from these parties, which we have incorporated, as appropriate.

In its comments, FBI concurred with our recommendation to develop and implement a unified strategy to combat scams and said that it is fully committed to this mission and leading this effort. FBI also concurred with our recommendation to explore ways to harmonize data collection to better identify scams. FBI acknowledged the importance of a coordinated approach and agreed that improving consistency in data collection will strengthen its ability to effectively identify and respond to scams. FBI also

concurred with our recommendation to use the agency's data collection and analysis to produce and report an estimate of the number of complaints it receives and the associated financial losses resulting from scams.

FBI did not concur with our recommendation for it, in collaboration with FTC and other agencies, as appropriate, to develop and report a single, government-wide estimate of the number of consumers affected by and dollar losses resulting from scams. In its comments, FBI stated that it understands the critical need for a comprehensive estimate that reflects reported scam incidents to better inform policy and response efforts. However, FBI stated that it cannot reliably create an estimate of incidents not reported. FBI noted that it can review the DOJ's National Crime Victimization Survey data and use this as a resource to inform policy and response efforts.

We appreciate FBI's efforts to develop and report a single, government-wide estimate of the number of consumers affected by and dollar losses resulting from scams. FBI states that it cannot reliably create an estimate of incidents not reported. However, other agencies have made estimates that factor in underreporting. For example, FTC has made estimates of overall consumer loss from fraud that adjust for underreporting. Fraud estimates, including those specifically addressing scams, can demonstrate the scope of the problem, could help improve oversight prioritization, and could help determine the return on investment from activities to mitigate fraud. We continue to believe our recommendation is warranted.

FBI did not agree with our recommendation to adopt the definition of scams developed by the Federal Reserve or work with the FTC and other affected agencies to develop a common definition of scams and related scam types, prior to developing a single estimate of the number of consumers affected by, and dollar losses resulting from scams. In its comments, FBI stated that, while it acknowledges the Federal Reserve's efforts in defining scams, it believes that the current definition is too broad and aligns closer with a general definition of fraud rather than specifically addressing the unique characteristics of scams. FBI stated that it will collaborate with FTC, Federal Reserve, and other relevant agencies to identify a shared definition, which better distinguishes scams from other forms of fraud; however, FBI noted that it cannot compel other agencies to adopt a new definition.

While we understand FBI's concerns, our recommendation is geared toward agencies collaborating with each other in developing a scam definition. It is important to define terms and use definitions consistently, including using common definitions when measuring the volume and impact of scams over time. Using a common definition for this type of crime would improve the ability of agencies to compare and aggregate data across agencies, assess trends, and show progress in fraud prevention. We continue to believe our recommendation is warranted.

FBI also did not agree with our recommendation to establish metrics and a plan to measure the effectiveness of FBI's antiscam training on the consumers that receive it. In its comments, FBI stated that its extensive outreach efforts, which include in-person presentations, televised appearances, podcasts, webinars, and radio events, are decentralized and difficult to track. According to the FBI, accurately measuring the effectiveness of its outreach efforts would be resource intensive and it currently lacks the necessary capacity. FBI also added that even when individuals receive fraud/scam education and absorb the material, they may still fall for a scam because of cognitive biases, emotional manipulation, or lapses in judgment. However, FBI stated that it remains committed to improving its antiscam efforts and will continue to explore effective ways to measure the impact of its training programs.

Our recommendation does not ask FBI to measure its efforts against an increase or reduction in victimization or fraud overall. The intent of our recommendation is for FBI to measure the training's effect on course participants' ability to recognize and protect themselves from scams. For example, it might be possible to follow up with participants 6 months or a year after the training to ask if they were contacted by a scammer and, if so, ask how they used the information provided in the training to identify the scam and what subsequent steps they took. It is important for agencies to ensure that their training efforts incorporate performance measures that can be used to demonstrate contributions that training makes to improving results. In addition, such information would allow agencies to identify aspects of their training program that need improvement. Therefore, we maintain that our recommendation is warranted.

In its comments, FTC noted that GAO's definition of scams was not all inclusive for FTC's purposes, such as the FTC Act. In our report, we define scams as the use of deception or manipulation intended to achieve financial gain. We also note that this report highlights specific types of scams that include impersonation scams and investment scams, among

others. We added language into our final report to specifically note that these scams are included in the Scam Classifier Model but are not an exhaustive list of all current and other types of scams that may evolve in the future.

While FTC neither agreed nor disagreed with the five recommendations directed to it, the agency expressed some concerns with two of them. Specifically, for recommendations 10 and 13 related to developing a common definition of scams and developing a single, government-wide estimate of consumers affected by scams, FTC agreed that agencies should explore ways in which they can further consult with each other on fraud-related reporting. However, FTC noted that it had concerns related to the differing authorities of each agency and the diversion of law enforcement resources that would otherwise be used to address fraud. As we stated in our report, we understand that each agency has its own mandate and authority. We continue to believe, however, that a single, government-wide measure and a common definition of scams will best support a multiagency approach and response to scams.

We are sending copies to the appropriate congressional committees, the Director of CFPB, Director of FBI, Chair of FTC, and other interested parties. In addition, the report will be 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 Seto J. Bagdoyan at bagdoyans@gao.gov or Howard Arp at arpj@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 VI.

//SIGNED//

Seto J. Bagdoyan
Director, Forensic Audits and Investigative Service

//SIGNED//

J. Howard Arp
Director, Forensic Audits and Investigative Service

Appendix I: Objectives, Scope, and Methodology

This report

1. describes federal agencies' activities to prevent and respond to scams and evaluates the extent to which there is a comprehensive, government-wide strategy to guide their efforts;
2. evaluates the extent to which federal agencies compile scam-related consumer-complaint data and are able to estimate the total number of scams and related financial losses;
3. describes federal agencies' efforts to educate consumers about scams and evaluates the extent to which they measure their effectiveness;
4. describes selected private businesses' efforts to counter scams; and
5. describes actions by federal agencies and selected private businesses to respond to consumer complaints related to scams.

To describe the federal agencies' activities to prevent and respond to scams, we reviewed documentation and interviewed officials from the following 13 agencies:

- Consumer Financial Protection Bureau (CFPB),
- The Federal Bureau of Investigation (FBI) and the Executive Office for United States Attorneys (within the Department of Justice (DOJ)),
- The Federal Trade Commission (FTC),
- The Federal Deposit Insurance Corporation (FDIC),
- The Federal Reserve (Board of Governors of the Federal Reserve System and Federal Reserve Payment Services),
- the Administration for Community Living (within the Department of Health and Human Services),
- National Credit Union Administration,
- Office of the Comptroller of the Currency (OCC) and the Financial Crimes Enforcement Network (FinCEN) (within the Department of the Treasury),
- the Department of State (the Bureau of International Narcotics and Law Enforcement Affairs and the Bureau of Consular Affairs), and

- Secret Service and Homeland Security Investigations (within the Department of Homeland Security).[1]

We identified these agencies by reviewing publicly available information describing their work related to scams.[2] We interviewed officials and reviewed documentation from each of these agencies about their activities to counter scams. We specifically asked whether their agency engaged in any of 11 different activities. We identified the 11 activities by reviewing publicly available information describing the agencies' work related to scams and asking the agencies if there were additional activities to consider.

To evaluate the extent to which a comprehensive, government-wide strategy exists across federal agencies to prevent and respond to scams, we asked officials from each of the 13 agencies if they were aware of any such strategy to coordinate or guide U.S. efforts to counter scams. We also reviewed existing U.S. strategies related to cyberthreats, cybercrime, transnational criminal organizations, or fraud and money laundering to determine whether any of these strategies may serve as a comprehensive, government-wide strategy to counter scams.

Further, we reviewed strategies specifically intended to counter scams developed by foreign countries to understand what types of information had been included in the strategies. We identified these strategies through a review of publicly available information and attendance at the Global Anti-Scam Alliance summit in 2023.[3] We also interviewed the Consumer Federation of America, the Retail Gift Card Association, and a financial institution to discuss federal government coordination and strategies.[4] In addition, we reviewed our prior work on interagency

[1]See app. II for descriptions of the individual federal agencies' missions.

[2]On the basis of our research, we selected agencies because of their direct involvement in reporting on and responding to scams. We included the Department of State because of its involvement in transnational criminal organizations. We included the Department of Health and Human Services because of congressional and executive branch agencies' concerns about the impact of scams involving older adults. Other agencies may be involved in countering scams, such as the Federal Communications Commission, the U.S. Securities and Exchange Commission, and Social Security Administration.

[3]The Global Anti-Scam Alliance is an international knowledge-sharing organization composed of government, law enforcement, consumer protection groups, and the private sector.

[4]These industry experts and consumer organizations were selected based on our review of publicly available information regarding scams and referrals made by other organizations.

coordination to provide assurance that federal programs are based on coherent strategy and are well coordinated.[5]

To evaluate the extent to which federal agencies compile scam-related consumer complaint data, we obtained information from three federal agencies that told us they receive and report on consumer complaints related to scams: CFPB, FBI, and FTC. We obtained documents, interviewed officials, and reviewed their publicly available data, including reports specifically addressing scams.

To evaluate the extent to which federal agencies use scam-related consumer complaint data to estimate the full extent of scams and dollar losses and have a common definition of scams, we held additional discussions with officials at CFPB, FBI, and FTC. We focused on these three agencies because they publish reports and data on consumer complaints data they receive. We also reviewed these three agencies' published reports to obtain information on how they compile and report on consumer complaint data. Further, we reviewed our previous work related to the importance of knowing and understanding the scope of fraud in managing fraud risk.[6]

To describe federal agencies' efforts to educate consumers about scams and evaluate the extent to which they measure the effectiveness of such efforts, we interviewed the 13 agencies discussed above and reviewed documentation provided by the agencies. We had additional discussions with officials specifically from CFPB, FBI, and FTC to better understand the extent to which they measure the effectiveness of their consumer education activities. We focused on these three agencies because they provide consumer education materials directly to a broad range of consumers. We also reviewed our previous work related to program outcomes that can help federal agencies effectively manage and assess the results of their efforts.[7]

[5]GAO, *Countering Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

[6]GAO, *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments*, GAO-24-105833 (Washington D.C.: Apr. 16, 2024).

[7]GAO, *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts,* GAO-23-105460 (Washington, D.C.: July 12, 2023).

To describe the efforts of selected private businesses to counter scams, we met with seven businesses. We met with two Peer-to-Peer (P2P) payment apps service providers, two gift card issuers, one money services business (MSB), and two financial institutions.[8] We selected these businesses based on various criteria, such as the ownership structure of the business and efforts to counter scams. The information obtained from these interviews is illustrative and cannot be generalized to other businesses.

As part of this objective, we selected P2P payment apps to meet with, based on a review of public information detailing the most-used P2P payment apps. We also reviewed information on the reported ownership structure, availability to customers, and the manner in which funds are transferred using the apps. We selected gift card issuers to meet with, based on FTC-published reports that detailed the most frequent gift cards reported being used by consumers who were contacted by scammers.[9] We selected MSB and financial institutions to discuss wire transfers. Specifically, we considered their market presence, type of institution, availability to consumers, and published information related to scams reported by FTC.

We also selected and visited, unannounced, a nongeneralizable sample of 68 locations of eight different gift card retailers across eight states and the District of Columbia to observe gift card scam warning signs that may be voluntarily posted at gift card displays.[10] These retailers included grocery stores, hardware stores, department stores, and pharmacies.

[8]An MSB is generally an institution engaging as a business in the transfer of funds as a money transmitter or offering check cashing; foreign currency exchange services; or selling money orders, travelers' checks or prepaid access (formerly stored value) products.

[9]Federal Trade Commission, *Scammers increasingly demand payment by gift card* (Oct. 16, 2018), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2018/10/scammers-increasingly-demand-payment-gift-card; *Gift cards top scammers' wish lists* (Dec. 21, 2020), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2020/12/gift-cards-top-scammers-wish-lists; and *Scammers prefer gift cards, but not just any gift card will do* (Dec. 8, 2021), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/12/scammers-prefer-gift-cards-not-just-any-card-will-do.

[10]Federal law does not require gift card retailers to post fraud warning signs in retail stores. Some states, however, have enacted laws and regulations that may require certain signage. We did not assess for compliance with state laws. The eight selected states include California, Illinois, Maryland, New Jersey, New York, Texas, Virginia, and Washington.

Within the 68 locations, we observed 147 gift card displays. The results of our unannounced site visits are specific to the retailer location visited and cannot be projected to all gift card retailers. The gift card retailers were chosen by selecting among the retailers with the highest dollar 2022 gross retail sales and with the most U.S. locations.[11]

We met with the following industry representatives and advocacy groups to obtain additional information on scams: AARP, Consumer Federation of America, Better Business Bureau (BBB), The Retail Gift Card Association, Money Transmitter Regulators Association, and Money Services Business Association.[12] These associations and advocacy groups were selected because they were mentioned by agencies we interviewed or represent businesses associated with a payment method.

To describe actions taken by federal agencies and selected businesses to respond to consumer complaints related to scams, we interviewed officials from CFPB, FBI, and FTC. We focused on these agencies because they receive complaints directly from consumers and produce reports based on these data. We also interviewed the seven selected businesses about their actions to respond to consumer complaints. In addition, we interviewed a local district attorney, who has prosecuted scam cases, to obtain a better understanding of the process of investigating a scam case. This individual was identified through our prior work on fraud and research on scams. Further, we reviewed DOJ press releases to identify examples of adjudicated cases related to scams.

[11]We reviewed the 2022 gross retail sales because 2022 was the most recent year for which sales data were publicly available at the time of our review.

[12]AARP, formerly the American Association of Retired Persons, is an interest group in the United States focusing on issues affecting those over the age of 50. The Consumer Federation of America is a nonprofit organization founded to advance consumer interests through research, education, and advocacy. The BBB is a nonprofit organization focused on advancing marketplace trust. It consists of 91 independently incorporated local BBB organizations in the United States and Canada, coordinated under the International Association of Better Business Bureaus. The Retail Gift Card Association is a trade association representing the closed-loop gift card industry, and it is comprised of members committed to promoting and protecting the use of retail gift cards. The Money Transmitter Regulators Association is a national nonprofit organization dedicated to the efficient and effective regulation of the money transmission industry in the United States. Its membership consists of state regulatory authorities in charge of regulating money transmitters and sellers of travelers' checks, money orders, digital assets, drafts, and other money instruments. The Money Services Business Association supports the nonbank financial service industry, tracks legislation and regulation, and promotes education and communication with federal and state regulators.

As part of this objective, we conducted covert scenarios to obtain information on the experiences of consumers of varying demographics, including older adults, who report scams to selected federal agencies and businesses.[13] We executed different scenarios where we were the victims of different types of scams, such as government impersonation scams and investment scams, among others. We also selected a nongeneralizable sample of P2P payment apps, gift card issuing companies, and MSBs as scam payment methods used for our covert tests. We submitted consumer complaints to CFPB, FBI, and FTC, as well as to a nongeneralizable selection of four gift card issuers and a nonbank wire transfer company.[14] We did this to determine what initial action the agencies and selected businesses take when an individual informs them that they have been the victim of a scam.[15] As part of our covert scenarios, we conducted five gift card and two wire transfer transactions. For our covert wire transfers, we transmitted the funds from an account that we held to another account that we held.

When submitting these complaints, we informed the agencies and gift card issuers that we had provided gift card numbers to scammers as a form of payment. We also informed the agencies and the wire transfer company that we had been told by a scammer that we needed to transfer funds as a form of payment and provided information about the wire transfers. We selected the businesses for our covert scenarios based on various criteria, including the ownership structure of the business and FTC information about payment methods preferred and targeted by scammers.

The results of our covert scenarios are for illustrative purposes and cannot be projected to the outcomes of other consumer complaints or responses by agencies and entities.

[13]This report refers to persons 60 and older when using the term “older adults.” This definition is consistent with the requirements in Section 2(1) of the Elder Abuse Prevention and Prosecution Act, which references Section 2011 of the Social Security Act (42 U.S.C. 1397j(5)) (defining “elder” as an individual age 60 or older).

[14]The P2P payment app businesses blocked our attempted transactions, citing suspicious activity on the accounts. Therefore, we did not submit scam complaints to these two companies or P2P-related complaints to federal agencies.

[15]We reviewed what initial step these businesses undertook when scams were reported. We did not investigate how these businesses implement error resolution responsibilities under applicable law.

We conducted this performance audit from October 2023 to April 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. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Appendix II: Federal Agencies' Mission

As part of our work, we interviewed 13 federal agencies about the activities they engage in to prevent and respond to scams. The table below contains the mission statements for the 13 federal agencies, some of which are components within federal departments.

Table 1: Selected Agencies' Mission Statements

Agency	Mission statement
Consumer Financial Protection Bureau (CFPB)	CFPB was created to provide a single point of accountability for enforcing federal consumer financial laws and protecting consumers in the financial marketplace. Its work includes rooting out unfair, deceptive, or abusive acts or practices by writing rules, supervising companies, and enforcing the law; enforcing laws that outlaw discrimination in consumer finance; taking consumer complaints; enhancing financial education; researching the consumer experience of using financial products; and monitoring financial markets for new risks to consumers.
Department of Health and Human Services (HHS)	The mission of HHS is to enhance the health and well-being of all Americans, by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services.
Department of State	The mission of the Department of State is to protect and promote U.S. security, prosperity, and democratic values and shape an international environment in which all Americans can thrive.
Federal Bureau of Investigation (FBI) [a]	The mission of FBI is to protect the American people and uphold the Constitution of the United States. FBI is the lead federal agency for investigating cyberattacks and intrusions. It collects and shares intelligence and engages with victims while working to unmask those committing malicious cyber activities, wherever they are.
Federal Deposit Insurance Corporation (FDIC)	FDIC is an independent agency created by Congress established to maintain stability and public confidence in the nation's financial system. To accomplish this mission, FDIC insures deposits; examines and supervises financial institutions for safety, soundness, and consumer protection; makes large and complex financial institutions resolvable; and manages receiverships.
Federal Reserve Board	The Federal Reserve Board is the governing body of the Federal Reserve System, the central bank of the United States.
Federal Trade Commission (FTC)	The FTC's mission is protecting the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education. FTC has both consumer protection and competition jurisdiction in broad sectors of the economy.
Financial Crimes Enforcement Network (FinCEN)[b]	FinCEN's mission is to safeguard the financial system from illicit use and to counter money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and the strategic use of financial authorities. FinCEN carries out its mission by receiving and maintaining financial transactions data, analyzing and disseminating those data for law enforcement purposes, and building global cooperation with counterpart organizations in other countries and with international bodies. FinCEN is a bureau of the U.S. Department of the Treasury.
Homeland Security Investigations (HSI)[c]	HSI conducts federal criminal investigations into the illegal movement of people, goods, money, contraband, weapons, and sensitive technology into, out of, and through the United States. HSI's investigations are wide-ranging – cases include drug and weapons smuggling, cyber and financial crime, illegal technology exports, and intellectual property crime. HSI also plays a crucial role in investigating crimes of exploitation. This includes countering child exploitation, human trafficking, financial fraud and scams, and other crimes against vulnerable populations.

Agency	Mission statement
National Credit Union Administration	The National Credit Union Administration is an independent federal agency that insures deposits at federally insured credit unions, protects the members who own credit unions, and charters and regulates federal credit unions. The mission of the National Credit Union Administration is to protect the system of cooperative credit and its member-owners through effective chartering, supervision, regulation, and insurance.
Office of the Comptroller of Currency (OCC)[b]	The OCC is an independent bureau of the U.S. Department of the Treasury. The OCC charters, regulates, and supervises all national banks and federal savings associations, as well as federal branches and agencies of foreign banks. The mission of OCC is to ensure that the financial institutions, in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations.
Executive Office for United States Attorneys[a]	The United States Attorney is the chief federal law enforcement officer in their district and is also involved in civil litigation where the United States is a party. The Executive Office for United States Attorneys was created to provide for close liaison between the Department of Justice in Washington, D.C., and the 93 United States Attorneys located throughout the 50 states, the District of Columbia, Guam, the Mariana Islands, Puerto Rico, and the U.S. Virgin Islands.
United States Secret Service[c]	Secret Service has an integrated mission of protection and investigations to ensure the safety and security of its protectees, key locations, and events of national significance. Secret Service also protects the integrity of U.S. currency and investigates crimes against the U.S. financial system committed by criminals around the world and in cyberspace.

Source: GAO review of agencies' publicly available information. I GAO-25-107088

[a]Component of the Department of Justice.

[b]Component of the Department of the Treasury.

[c]Component of the Department of Homeland Security.

Appendix III: Comments from the Federal Bureau of Investigation

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 14, 2025

Seto Bagdoyan
Director
Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Bagdoyan:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to the draft report entitled *Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088). The FBI recognizes the importance of Government Accountability Office (GAO) oversight in promoting efficiency, effectiveness, and accountability in government operations, and is committed to addressing the findings and recommendations outlined in the report.

The FBI has reviewed the findings and six recommendations outlined in the report, and concurs with three and respectfully disagrees with three. The FBI's collaboration, coordination, and creation of a cohesive solution will be best served by a centralization of expertise across partner agencies to avoid fragmentation and strengthen our ability to combat authorized payment fraud. While the FBI is committed to leading and coordinating efforts, it does not have ultimate authority over other agencies, which may impact the scope and implementation of the recommendations. As detailed below, the FBI cannot concur with recommendations that are not within the FBI's scope.

Please find our response to the recommendations:

Recommendation #1 – The Director of the FBI should lead the U.S. government effort to develop and implement a government-wide strategy to counter scams and coordinate related activities. This effort should be done in collaboration with the Chair of the FTC, the Secretary of the Treasury, and other agencies as appropriate (through their designees). This effort should address issues such as a common definition for scams, consumer complaint reporting, related types/granularity/aggregation of data, risks and responses, a government-wide estimate of this type of crime, and coordination of federal and business activities. As appropriate and consistent with desired characteristics, a strategy should also: define agency roles, responsibilities, and authorities; identify necessary resources; and, identify any legislative, regulatory, or administrative changes needed to enable a comprehensive, coordinated response.

FBI Response – The FBI is fully committed to this mission and leading this effort in partnership with the Chair of the FTC, the Secretary of the Treasury, and other key agencies to develop and implement a unified strategy to combat scams and coordinate related activities. The FBI will lead the effort to develop and implement a government-wide strategy.

Recommendation #4 – The Director of the FBI should, in collaboration with FTC, explore ways to harmonize data collection to better identify scams, such as consistently collecting data on scam type.

FBI Response – The FBI acknowledges the importance of a coordinated approach and agrees improving consistency in data collection will strengthen our ability to effectively identify and respond to scams. The FBI is committed to enhancing its data collection practices and will collaborate with the FTC to identify areas in which common definitions and classification taxonomy may be applied.

Recommendation #6 – The Director of the FBI should use the agency's data collection and analysis to produce and report an estimate of the number of complaints it receives and the associated financial losses resulting from scams.

FBI Response – The FBI concurs with the recommendation and agrees with the importance of utilizing its data collection and analysis to better understand and report on the number of complaints it receives, along with the associated financial losses resulting from scams. To implement this recommendation, the FBI will explore ways to aggregate and report scam-related complaints and financial losses.

Recommendation #9 – The Director of the FBI should, in collaboration with the FTC and other agencies as appropriate, develop and report a single, government-wide estimate of the number of consumers affected by and dollar losses resulting from scams, factoring in an estimate of incidents not reported.

FBI Response – The FBI understands the critical need for a comprehensive estimate that reflects reported scam incidents to better inform policy and response efforts. The FBI will continue to collect this data through IC3 and work collaboratively to share the FBI's data with other agencies. However, the FBI cannot reliably create an estimate of incidents not reported. The FBI can, however, review the DOJ's National Crime Victimization Survey data and use this as a resource to inform policy and response efforts.

Recommendation #12 – The Director of the FBI, prior to developing a single estimate of the number of consumers affected by and dollar losses resulting from scams, should adopt the definition of scams developed by the Federal Reserve or work with the FTC and other affected agencies to develop a common definition of scams and related scam types.

FBI Response – While the FBI acknowledges the Federal Reserve's efforts in defining scams, we believe their current definition is too broad and aligns closer with a general definition of fraud rather than specifically addressing the unique characteristics of scams. The FBI will collaborate with the FTC, Federal Reserve, and other relevant agencies to identify a shared definition, which better distinguishes scams from other forms of fraud; however, the FBI cannot compel other agencies to adopt a new definition.

Recommendation #15 – The Director of the FBI should establish metrics and a plan to measure the effectiveness of its anti-scam training on the consumers that receive it through in-person

events or webinars. This could include understanding the training's effect on consumers' ability to recognize and protect themselves from scams.

FBI Response – The FBI does not concur with the recommendation. As cited in GAO-25-10788:

> *Specifically, CFPB, FBI, and FTC have not designated performance measures or metrics for their in-person and virtual education activities that target outcomes for participants. This is, in part, because some agencies do not believe it is possible to link education efforts to a reduction in overall fraud.*

The FBI's extensive outreach efforts, which include in-person presentations, televised appearances, podcasts, webinars, and radio events, are decentralized across field offices and difficult to track longitudinally. Accurately measuring their effectiveness in reducing fraud would require long-term tracking of participants, a resource-intensive effort the FBI currently lacks the capacity to support. Further, even when individuals are educated about scams, they may still fall victim due to cognitive biases, emotional manipulation, or lapses in judgment. Scammers often exploit emotions like fear, urgency, and trust, which overrides rational thinking, even among those who have received anti-scam education. While a reduction in fraud complaints or dollar losses may seem to indicate the effectiveness of education, it is challenging to attribute these declines solely to educational efforts. Various factors influence fraud rates, including law enforcement actions, economic conditions, and the evolving tactics of scammers. For instance, decreases in complaints may result from successful law enforcement disruption efforts, or victims' failure to report fraud due to shame, lack of awareness, or fear of loss of autonomy.

The FBI remains committed to improving its anti-scam efforts and will continue to explore effective ways to measure the impact of our training programs.

Thank you for the opportunity to comment on this report. The FBI appreciates GAO's thorough analysis and remains committed to continuous improvement. We will continue monitoring our progress on these initiatives and look forward to ongoing collaboration. If I may be of further assistance to you, please do not hesitate to contact me. Your staff may also contact Louise Duhamel, Assistant Director, JMD Audit Liaison Group at 202-514-4006.

Sincerely,

James C. Barnacle, Jr.
Acting Assistant Director
Criminal Investigative Division
Federal Bureau of Investigation

cc: The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Room 7071
Washington, DC 20548

Jason Bair
Managing Director
Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Rm. 6153
Washington, DC 20548

Tracey Cross
Assistant Director
Homeland Security and Justice Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Louise Duhamel
Assistant Director
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division
145 N Street, NE Suite 8W.300
Washington, DC 20002

Appendix IV: Comments from the Federal Trade Commission

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

March 14, 2025

Sent via Email

Seto Bagdoyan
Director for Audit Services
Forensic Audits & Investigative Service
Government Accountability Office
(202) 512-6722
bagdoyans@gao.gov

Howard Arp
Director
Forensic Audits & Investigative Service
Government Accountability Office
(202) 512-6722
arpj@gao.gov

Re: GAO Engagement No. 107088

Dear Messrs. Bagdoyan and Arp:

On January 28, 2025, the Government Accountability Office ("GAO") forwarded for the Federal Trade Commission's ("FTC") review and comment a draft report titled *Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088) ("Draft Report"). In connection with the preparation of this draft, FTC staff have met with GAO staff on several occasions and provided detailed responses to written questions and feedback on earlier drafts. In addition, FTC staff have engaged with GAO, including through meetings, written responses to questions, and Draft Report feedback, in connection with a related report, titled *Payment Scams: Information on Financial Industry Efforts* (GAO-107107). FTC staff appreciates the opportunity to engage with GAO on these important topics. In addition to the comments and edits provided to GAO on February 28, 2025, FTC staff would like to specifically address the draft report's use of the terms "fraud" and "scam" and related recommendations.

As GAO outlined in its January 28 Draft Report, fraud is costing American consumers billions of dollars every year.[1] It is an urgent problem, and one that has led to effective cross-government initiatives.[2] The FTC has taken extensive action to counter fraud, including through aggressive law enforcement,[3] wide-reaching consumer education and outreach, and by publishing data and trend analysis of the consumer fraud reports that Consumer Sentinel receives.[4]

While FTC staff welcomes GAO's thorough analysis and recommendations, FTC staff wishes to correct certain statements and articulate concerns with certain recommendations in GAO's Draft Report.

The January 28 Draft Report's Definition of "Scams" and Omission of "Fraud." In its Draft Report, GAO defined "scams" as "the use of deception or manipulation intended to achieve financial gain."[5] It derived this definition from the Federal Reserve Board's Scam Classifier Model, a model created by a working group led by the Federal Reserve Board which is specifically intended to be used by and applied to the payments industry.[6] Though not discussed in the Draft Report, the Federal Reserve Board also developed a parallel "Fraud Classifier" model.[7] The Classifiers distinguish

[1] Draft Report at 1. The FTC estimates that in 2023, overall consumer loss from fraud, adjusting for underreporting, was as high as $158.3 billion. FTC, Protecting Older Consumers 2023-2024 (Oct. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf.

[2] Examples include the Global Anti-fraud Enforcement Network, the Elder Justice Coordinating Council, the Scams Against Older Adults Advisory Group, and the COVID-19 Fraud Enforcement Task Force. *See, e.g.*, Draft Report at 18.

[3] *See, e.g.*, Press Release, FTC, MoneyGram Agrees to Pay $125 Million to Settle Allegations that the Company Violated the FTC's 2009 Order and Breached a 2012 DOJ Deferred Prosecution Agreement (Nov. 8, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/11/moneygram-agrees-pay-125-million-settle-allegations-company-violated-ftcs-2009-order-breached-2012; Press Release, FTC, Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits $586 Million in Settlement with FTC and Justice Department (Jan. 19, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles-consumer-fraud-charges-forfeits-586.

[4] For example, in 2024, the FTC received 2.6 million fraud complaints reporting overall losses of over $12.5 billion. *See, e.g.*, FTC, Consumer Sentinel Network Data Book 2024 (March 2024), https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024.

[5] Draft Report at 1.

[6] Draft Report at 40.

[7] *See* https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/.

"frauds" from "scams" and focus on whether payments are "authorized" or "unauthorized," terms that are drawn from Regulation E.[8]

However, for law enforcement actions the FTC takes to enforce Section 5 of the FTC Act, whether a payment was "authorized" by a consumer is not dispositive; rather, what matters is whether the transaction was induced by an unfair, deceptive or misleading representation, omission, or practice. For example, imposter scams violate the FTC Act regardless of whether a transaction was "authorized" or "unauthorized." Thus, the definitions and distinctions between "scams" and "fraud" do not align with the FTC's tracking of consumer report data or the FTC's application of its law enforcement authority.

To support its law enforcement mission, the FTC receives valuable reports from the public about the frauds consumers are experiencing in the marketplace. The FTC's consumer fraud reports typically include types of fraud that the Draft Report would define as "scams," such as imposter scams. The FTC regularly reports on these and other fraud reports it receives, including detailed information about fraud sub-types such as investment scams, money-making schemes, and others.[9] Such public reporting provides valuable information to businesses and consumers, as well as academics and others engaging in fraud prevention and education.

Because it is not dispositive, when it collects reports from consumers the FTC does not ask consumers specific questions about whether payments were "authorized" or "unauthorized" as described in Regulation E.[10] FTC staff believe its understanding of fraud, which does not distinguish between "authorized" or "unauthorized" payments in the first instance, more robustly captures unlawful conduct that is harming American

[8] Whether or not a transaction is "authorized" or "unauthorized" has implications for whether the financial institution or the consumer is liable for fraudulent or fraudulently induced transfers. Regulation E defines the term "unauthorized electronic fund transfer" as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit." 12 C.F.R. § 1005.2(m). Unauthorized transfers exclude payments initiated: (1) by a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized; (2) with fraudulent intent by the consumer or any person acting in concert with the consumer; or (3) by the financial institution or its employee. *Id*. *See also* 12 C.F.R. § 1005.2(m)-2(m), Supp. I (official interpretation of 2(m) unauthorized electronic fund transfer).

[9] For example, the FTC makes consumer report data available through its annual Consumer Sentinel Network Data Book. *See, e.g*., FTC, Consumer Sentinel Network Data Book 2024 (March 2024), https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024. It also makes fraud and other consumer reports available through its public Tableau, which is updated quarterly. *See* https://public.tableau.com/app/profile/federal.trade.commission/vizzes.

[10] Moreover, such a question likely would only confuse consumers who lost money to a scammer. Consumers would be unlikely to recognize and reliably report the legal distinction and such a question may have a chilling effect on reporting.

consumers and makes its consumer data reports more comprehensive. Indeed, were the FTC to use the GAO's definition exclusively, it would risk discounting a significant portion of fraud that affects everyday Americans.

To be sure, FTC staff agrees that agencies should explore ways in which they can further consult with each other on fraud-related reporting. But such efforts should be coterminous with the differing authorities of each agency. FTC staff therefore has concerns with the Draft Report's recommendations that the FTC and all other affected agencies utilize the same definition of "scams"[11] and develop a single, governmentwide estimate of consumers affected by scams using that common definition.[12] FTC staff is further concerned that interagency efforts to arrive at a common definition of "scams" could divert law enforcement resources that would otherwise be used to address fraud. Finally, FTC staff is concerned with a recommendation that requires the agreement of all affected agencies, each of which has its own mandate, authority, priorities, and resources, and each of which acts independently.[13]

FTC staff again would like to reiterate its appreciation for GAO's thoughtful and careful examination of this issue and for the opportunity to respond to the recommendations in its Draft Report. FTC staff hopes that GAO's report will raise public awareness of the importance of addressing fraud affecting consumers.

Sincerely,

Christopher G. Mufarrige

Christopher G. Mufarrige
Director, Bureau of Consumer Protection
Federal Trade Commission

[11] Draft Report Recommendation 13, which stated "The Chair of the FTC, prior to developing a single estimate of the number of consumers affected by and dollar losses resulting from scams, should adopt the definition of scams developed by the Federal Reserve or work with CFPB and FBI and other affected agencies to develop a common definition of scams and related scam types." Draft Report at 77-78.

[12] Draft Report Recommendation 10, which stated "The Chair of the FTC should, in collaboration with the CFPB, the FBI, and other agencies as appropriate, develop and report a single, governmentwide estimate of the number of consumers affected by and dollar losses resulting from scams, factoring in an estimate of incidents not reported." Draft Report at 77.

[13] The breadth of the recommendation in the Draft Report is particularly concerning because "affected agencies" could encompass state and international agencies that contribute to the FTC's Consumer Sentinel Network.

Appendix V: Comments from the National Credit Union Administration

National Credit Union Administration
Office of the Executive Director

February 28, 2025

Daniel Garcia-Diaz
Managing Director
Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Garcia-Diaz,

We have reviewed the GAO's study entitled *'Consumer Protection– Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams.'* While there are no recommendations for the NCUA, we acknowledge the GAO's observations.

Thank you for the opportunity to review and comment on this report.

Sincerely,

Larry Fazio
Executive Director

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-6320

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

Seto Bagdoyan, BagdoyanS@gao.gov

Howard Arp, ArpJ@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Dave Bruno (Assistant Director), Mark Macpherson (Assistant Director), Erin Barry, Robert Bastian, Barbara Lewis, Patricia Powell, Gloria Proa, Daniel Silva, and Sabrina Streagle made key contributions to this report. Other contributors include Sherwin Chapman, Julia DiPonio, David Dornisch, Aimee Elivert, Colin Fallon, Margaret Hettinger, Brenda Mittelbuscher, and Joseph Rini.

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, X, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

TTo 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us