United States Government Accountability Office

Testimony

Before the Subcommittee on Economic and Consumer Policy, Committee on Oversight and Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Tuesday, March 26, 2019

CONSUMER DATA PROTECTION

Action Needed to Strengthen Oversight of Consumer Reporting Agencies

Statement of Michael Clements, Director
Financial Markets and Community Investment

Accessible Version

GAO-19-469T

March 26, 2019

CONSUMER DATA PROTECTION

Action Needed to Strengthen Oversight of Consumer Reporting Agencies

GAO Highlights

Highlights of GAO-19-469T, a testimony before the Subcommittee on Economic and Consumer Policy, Committee on Oversight and Reform, House of Representatives

Why GAO Did This Study

CRAs collect, maintain, and sell to third parties large amounts of sensitive data about consumers, including Social Security numbers and credit card numbers. Businesses and other entities commonly use these data to determine eligibility for credit, employment, and insurance. In 2017, Equifax, one of the largest CRAs, experienced a breach that compromised the records of at least 145.5 million consumers.

This statement is based on GAO's February 2019 report on the CRA oversight roles of FTC and CFPB. This statement summarizes (1) measures FTC has taken to enforce CRA compliance with requirements to protect consumer information, (2) measures CFPB has taken to ensure CRA protection of consumer information, and (3) actions consumers can take after a breach.

What GAO Recommends

In its February 2019 report, GAO recommended that Congress consider giving FTC civil penalty authority to enforce GLBA's safeguarding provisions. GAO also recommended that CFPB (1) identify additional sources of information on larger CRAs, and (2) reassess its prioritization of examinations to address CRA data security. CFPB neither agreed nor disagreed with GAO's recommendations.

View GAO-19-469T. For more information, contact Michael Clements at (202) 512-8678 or clementsm@gao.gov

What GAO Found

In its February 2019 report, GAO found that since 2008, the Federal Trade Commission (FTC) has settled 34 enforcement actions against various entities related to consumer reporting violations of the Fair Credit Reporting Act (FCRA), including 17 actions against consumer reporting agencies (CRA). Some of these settlements included civil penalties—fines for wrongdoing that do not require proof of harm—for FCRA violations or violations of consent orders. However, FTC does not have civil penalty authority for violations of requirements under the Gramm-Leach-Bliley Act (GLBA), which, unlike FCRA, includes a provision directing federal regulators and FTC to establish standards for financial institutions to protect against any anticipated threats or hazards to the security of customer records. To obtain monetary redress for these violations, FTC must identify affected consumers and any monetary harm they may have experienced. However, harm resulting from privacy and security violations can be difficult to measure and can occur years in the future, making it difficult to trace a particular harm to a specific breach. As a result, FTC lacks a practical enforcement tool for imposing civil money penalties that could help to deter companies, including CRAs, from violating data security provisions of GLBA and its implementing regulations.

Since 2015, the Consumer Financial Protection Bureau (CFPB) has had five public settlements with CRAs. Four of these settlements included alleged violations of FCRA; and three included alleged violations of unfair, deceptive, or abusive practices provisions. CFPB is also responsible for supervising larger CRAs (those with more than $7 million in annual receipts from consumer reporting) but lacks the data needed to ensure identification of all CRAs that meet this threshold. Identifying additional sources of information on these CRAs, such as by requiring them to register with the agency through a rulemaking or leveraging state registration information, could help CFPB ensure that it can comprehensively carry out its supervisory responsibilities. After the Equifax breach, CFPB used its existing supervisory authority to examine the data security of certain CRAs. CFPB's process for prioritizing which CRAs to examine does not routinely include an assessment of companies' data security risks, but doing so could help CFPB better detect such risks and prevent the further exposure or compromise of consumer information.

Consumers can take actions to mitigate the risk of identity theft—such as implementing a fraud alert or credit freeze—and can file a complaint with FTC or CFPB. However, consumers are limited in the direct actions they can take against CRAs. Consumers generally cannot exercise choice in the consumer reporting market—such as by choosing which CRAs maintain their information—if they are dissatisfied with a CRA's privacy or security practices. In addition, according to CFPB, consumers cannot remove themselves from the consumer reporting market entirely.

Chairman Krishnamoorthi, Ranking Member Cloud, and Members of the Subcommittee:

I am pleased to be here today to discuss our recent work on the oversight of consumer reporting agencies' (CRA) data protection. As you know, CRAs collect, maintain, and sell to third parties large amounts of sensitive data about consumers, including Social Security numbers and credit card numbers. The 2017 data breach of Equifax highlighted the data security risks associated with CRAs and underscored the importance of appropriate federal oversight in this market where consumers have limited control over whether or which CRAs possess their information.

This statement is based on our February 2019 report.[1] For this work, we focused on the CRA oversight roles of the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB). FTC and CFPB have taken steps to enforce CRA compliance with requirements to protect consumer information. However, this statement and our report identified specific actions that could strengthen the oversight of these companies and better protect consumers from the compromise of their personal information.

This statement discusses (1) measures FTC has taken to enforce CRA compliance with requirements to protect consumer information, (2) measures CFPB has taken to ensure CRA protection of consumer information, and (3) actions consumers can take after a breach. For this work, we reviewed the types of enforcement actions available to FTC and CFPB for violations of relevant laws, as well as specific enforcement actions these agencies have brought against CRAs. We also reviewed CFPB examination guidance for supervising these CRAs, including CFPB's internal guidelines for conducting data security examinations. In addition, we reviewed documents related to CFPB's process for prioritizing which institutions and which product lines should receive supervisory examination. We interviewed officials from FTC and CFPB on their oversight activities. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. More details on our methodology can be found in our February 2019 report.

[1]GAO, *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, GAO-19-196 (Washington, D.C.: Feb. 21, 2019).

Background

Oversight Agencies

FTC and, most recently, CFPB, are the federal agencies primarily responsible for overseeing CRAs. FTC has authority to investigate most organizations that maintain consumer data and to bring enforcement actions for violations of statutes and regulations that concern the security of data and consumer information.[2] CFPB, created in 2010 by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), has enforcement authority over all CRAs for violations of certain consumer financial protection laws.[3] In general, it also has the authority to issue regulations and guidance for those laws. CFPB has supervisory authority over larger market participants in the consumer reporting market. In 2012, CFPB defined larger market participant CRAs as those with more than $7 million in annual receipts from consumer reporting.[4] CFPB's supervision of these companies includes monitoring, inspecting, and examining them for compliance with the requirements of certain federal consumer financial laws and regulations. As discussed below, these laws include most provisions of the Fair Credit Reporting Act (FCRA); several provisions of the Gramm-Leach-Bliley Act (GLBA); and provisions of the Dodd-Frank Act concerning unfair, deceptive, or abusive acts or practices.[5]

[2]*See* 15 U.S.C. §§ 6801-6809; 16 C.F.R. § 314.1(a) and § 314.3(b)(2)-(3).

[3]Pub. L. No. 111-203, tit. X, 124 Stat. 1376, 1955 (2010).

[4]*See* Defining Larger Participants of the Consumer Reporting Market, 77 Fed. Reg. 42874 (July 20, 2012).

[5]The rulemaking authority for GLBA's safeguards provision and FCRA's red flags and records disposal provisions are statutorily excluded from CFPB's authority. *See* 12 U.S.C. § 5481(12)(F),(J). According to CFPB staff, CFPB can examine the data security practices of larger market participant CRAs for compliance with the provisions of the Dodd-Frank Act, including the prohibition of unfair, deceptive, or abusive acts or practices; and can obtain information about CRAs' compliance management systems, including those for data security. *See* 12 U.S.C. § 5514(b)(1). However, CFPB staff said they cannot examine for compliance with or enforce the data security standards in these provisions of GLBA and FCRA or the FTC's implementing rules, even at larger market participant CRAs.

Data Breaches and the Equifax Breach

Although there is no commonly agreed-upon definition of "data breach," the term generally refers to an unauthorized or unintentional exposure, disclosure, or loss of sensitive information. This information can include personally identifiable information such as Social Security numbers, or financial information such as credit card numbers. A data breach can be inadvertent, such as from the loss of an electronic device; or deliberate, such as the theft of a device or a cyber-based attack by individuals or groups, including an organization's own employees, foreign nationals, or terrorists.[6] Data breaches have occurred at all types of organizations, including private, nonprofit, and federal and state entities.

In the Equifax data breach, Equifax system administrators discovered on July 29, 2017, that intruders had gained unauthorized access via the Internet to a server housing the company's online dispute portal.[7] The breach compromised the personally identifiable information of at least 145.5 million individuals, and included names, addresses, and birth dates; and credit card, driver's license, and Social Security numbers.[8] Equifax's investigation of the breach identified the following factors that led to the breach: software vulnerabilities, failure to detect malicious traffic, failure to isolate databases from each other, and inadequately limiting access to sensitive information such as usernames and passwords. Equifax's public filings after the breach noted that the company took steps to improve security and notify individuals about the breach. Our August 2018 report provides more information on the breach and Equifax's response.[9]

[6]For more information on types of cyberattacks, see GAO, *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*, GAO-15-509 (Washington, D.C.: July 2, 2015).

[7]Equifax's online dispute portal is a web-based application that allows an individual to upload documents to research and dispute an inaccuracy in their Equifax credit report.

[8]On October 2, 2017, Equifax revised the number of affected individuals from 143 million to 145.5 million after it had incorrectly concluded that one of the attackers' queries had not returned any data. On March 1, 2018, Equifax stated that it had identified approximately 2.4 million U.S. consumers whose names and partial driver's license information were stolen, but as of August 2018, Equifax had not determined how many of these individuals were included in the estimate of 145.5 million affected individuals.

[9]See GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, GAO-18-559 (Washington, D.C.: Aug. 30, 2018).

FTC Has Taken Enforcement Measures against CRAs but Lacks Civil Penalty Authority for GLBA Data Protection Provisions

FTC enforces compliance with consumer protection laws under authorities provided in FCRA, GLBA, and the FTC Act. As we reported in February 2019, according to FTC, in the last 10 years, it has brought 34 enforcement actions for FCRA violations, including 17 against CRAs. In addition, FTC said that it has taken 66 actions against companies (not just in the last 10 years), including CRAs, that allegedly engaged in unfair or deceptive practices relating to data protection.

In some circumstances, FTC enforcement authority can include civil money penalties—monetary fines imposed for a violation of a statute or regulation.[10] However, FTC's civil penalty authority does not extend to initial violations of GLBA's privacy and safeguarding provisions. These provisions require administrative, physical, and technical safeguards with an emphasis on protection against anticipated threats and unauthorized access to customer records. For violations of GLBA provisions, FTC may seek an injunction to stop a company from violating these provisions and may seek redress (damages to compensate consumers for losses) or disgorgement (requirement for wrongdoers to give up profits or other gains illegally obtained).

Determining the appropriate amount of consumer compensation requires FTC to identify the consumers affected and the amount of monetary harm they suffered. In cases involving security or privacy violations resulting from data breaches, assessing monetary harm can be difficult. In addition, consumers may not be aware that their identities have been stolen as a result of a breach and or identity theft, and related harm may occur years in the future. It can also be difficult to trace instances of identity theft to specific data breaches. According to FTC staff, these factors can make it difficult for the agency to identify which individuals were victimized as a result of a particular breach and to what extent they were harmed and then obtain related restitution or disgorgement. Having civil penalty authority for GLBA provisions would allow FTC to fine a company for a violation such as a data breach without needing to prove

[10]*See* 15 U.S.C § 45(l). Generally, a civil money penalty is one of several forms of monetary sanctions that an agency can impose on a violator as a punitive measure.

the monetary harm to individual consumers. FTC staff noted that in the case of a data breach, each consumer record exposed could constitute a violation; as a result, a data breach that involved a large number of consumer records could result in substantial fines.

In 2006, we suggested that Congress consider providing FTC with civil penalty authority for its enforcement of GLBA's privacy and safeguarding provisions.[11] We noted that this authority would give FTC a practical tool to more effectively enforce provisions related to security of data and consumer information. Following the 2008 financial crisis, Congress introduced several bills related to data protection and identity theft, which included giving FTC civil penalty authority for its enforcement of GLBA. However, in the final adoption of these laws, Congress did not provide FTC with this authority. Since that time, data breaches at Equifax and other large organizations have highlighted the need to better protect sensitive personal information. Accordingly, we continue to believe FTC and consumers would benefit if FTC had such authority, and we recommended in our February 2019 report that Congress consider providing FTC with civil penalty authority for the privacy and safeguarding provisions of GLBA to help ensure that the agency has the tools it needs to most effectively act against data privacy and security violations.

CFPB Enforces and Examines CRAs for Compliance with Consumer Protection Laws but Does Not Fully Consider Data Security in Prioritizing Examinations

CFPB enforces compliance with most provisions of FCRA; several provisions of GLBA; and the prohibition of unfair, deceptive, or abusive

[11]GAO-06-674.

acts or practices under the Dodd-Frank Act.[12] In our February 2019 report, we noted that since 2015, CFPB has had five public settlements with CRAs. Four of these settlements included alleged violations of FCRA, and three included alleged violations of provisions related to unfair, deceptive, or abusive practices. CFPB also has an ongoing investigation of Equifax's data breach.

Under its existing authority, CFPB has examined several larger market participant CRAs, but may not be identifying all CRAs that meet the $7 million threshold. CFPB staff told us that as of October 2018, they were tracking between 10 and 15 CRAs that might qualify as larger market participants. CFPB staff told us that they believe the CRA market is highly concentrated and there were not likely to be many larger market participants beyond the 10 to 15 they are tracking. However, CFPB staff said that the 10 to 15 CRAs may not comprise the entirety of larger market participants, because CRAs' receipts form consumer reporting may vary from year to year, and CFPB has limited data to determine whether CRAs meet the threshold.

Our January 2009 report on reforming the U.S. financial regulatory structure noted that regulators should be able to identify institutions and products that pose risks to the financial system, and monitor similar institutions consistently.[13] CFPB could identify CRAs that meet the larger market participant threshold by requiring such businesses to register with it, subject to a rulemaking process and cost-benefit analysis of the burden it could impose on the industry. Another method CFPB could use to

[12]CFPB has authority under FCRA, except for the provisions governing the disposal of information and the "red flags" of identity theft. Those provisions were carved out of the CFPB's authority by section 1002(12)(F) of the Dodd-Frank Act. See 12 U.S.C. § 5481(12)(F). The red flags rule requires financial institutions and creditors (as defined by statute) to implement a written identity theft prevention program designed to detect the red flags of identity theft in their day-to-day operations, among other things. The disposal provision requires any person who maintains or otherwise possesses consumer information for a business purpose to dispose of such information properly by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. See 15 U.S.C. §§ 1681m(e), 1681s(a)(1) and 1681w(a)(1) and 16 C.F.R. pts. 681 and 682. Those provisions remain under FTC's authority and apply to entities, including CRAs as applicable, subject to the agency's jurisdiction. In addition, CFPB has authority over title V, subtitle A of GLBA, except for the data safeguards in section 501(b) of GLBA, 15 U.S.C. 6801(b). The data safeguards provision was carved out of the CFPB's authority by section 1002(12)(J) of the Dodd-Frank Act. See 12 U.S.C. § 5481(12)(J). That provision remains under FTC's jurisdiction with respect to CRAs and certain other entities. See 15 U.S.C. §§ 6801, 6804, 6805, and 16 C.F.R. pt. 314.

[13]GAO-09-216.

identify CRAs subject to its oversight would be to leverage information collected by states. We recommended in February 2019 that CFPB identify additional sources of information, such as through registering CRAs or leveraging state information, that would help ensure the agency is tracking all CRAs subject to its authority. CFPB neither agreed nor disagreed with our recommendation.

Each year CFPB determines the institutions (for example, banks, credit unions, non-bank mortgage servicers, and CRAs) and the consumer product lines that pose the greatest risk to consumers, and prioritizes these for examinations. CFPB segments the consumer product market into institution product lines, or specific institutions' offerings of consumer product lines. CFPB then assesses each institution product line's risk to consumers at the market level and institutional level. To assess risk at the market level, CFPB considers market size and other factors that contribute to market risk. To assess risk at the institution level, CFPB considers an institution's market share within a product line, as well as field and market intelligence. Field and market intelligence includes quantitative and qualitative information on an institution's operations for a given product line, including the strength of its compliance management systems, the number of regulatory actions directed at the institution, findings from prior CFPB examinations, and the number and severity of consumer complaints CFPB has received about the institution.

CFPB then determines specific areas of compliance to assess by considering sources such as consumer complaints, public filings and reports, and past examination findings related to the same or similar products or institutions. Most recently, CFPB examinations of CRA's consumer reporting have focused on issues such as data accuracy, dispute processes, compliance management, and permissible purposes.

Although CFPB's examination prioritization incorporates several important factors and sources, the process does not routinely include assessments of data security risk, such as how institutions detect and respond to cyber threats. CFPB staff said the bureau cannot examine for or enforce compliance with the data security standards in provisions of GLBA and FCRA or FTC's implementing rules, even at larger participant CRAs. After the Equifax breach, however, CFPB used its existing supervisory authority to develop internal guidelines for examining data security, and

conducted some CRA data security examinations.[14] CFPB staff said that they do not routinely consider data security risks during their examination prioritization process and have not reassessed the process to determine how to incorporate such risks going forward.

Statute requires CFPB to consider risks posed to consumers in the relevant product and geographic markets in its risk-based supervision program. In addition, federal internal control standards state that agencies should identify, analyze, and respond to risks related to achieving defined objectives. This can entail considering all significant internal and external factors to identify risks and their significance, including magnitude of impact, likelihood of occurrence, nature of the risk, and appropriate response.[15] In light of the Equifax breach, as well as CFPB's acknowledgment of the CRA market as a higher-risk market for consumers, it is important for CFPB to routinely consider factors that could inform the extent of CRA data security risk such as the number of consumers that could be affected by a data security incident and the nature of potential harm resulting from the loss or exposure of information. In our February 2019 report, we recommended that CFPB assess whether its process for prioritizing CRA examinations sufficiently incorporates the data security risks CRAs pose to consumers, and take any needed steps identified by the assessment to more sufficiently incorporate these risks. CFPB neither agreed nor disagreed with our recommendation.

[14]CFPB's general supervisory authority includes (1) assessing compliance with the requirements of federal consumer financial law, including the Dodd-Frank Act's prohibition of unfair, deceptive, and abusive acts or practices; (2) obtaining information about the activities and compliance systems of the examined institution; and (3) detecting and assessing risks of consumer financial products and services to consumers and markets. See 12 U.S.C. § 5514(b)(1). CFPB staff noted that unless the bureau finds that the institution has violated the Dodd-Frank Act's prohibition on unfair, deceptive, or abusive acts or practices, or another provision of federal consumer financial law over which CFPB has authority, the bureau cannot take enforcement action, and can only make supervisory recommendations.

[15]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

Regulators Inform Consumers about Protections Available and Consumers Can Take Some Actions after a CRA Data Breach

In our February 2019 report, we noted that FTC and CFPB provide educational information for consumers on ways to mitigate the risk of identity theft. In addition, after a breach, FTC and CFPB publish information specific to that breach. For example, shortly after Equifax's announcement of the breach, FTC published information on when the breach occurred, the types of data compromised, and links to additional information on Equifax's website. Similarly, CFPB released three blog posts and several social media posts that included information on ways that consumers could protect themselves in the wake of the breach and special protections and actions for service members.[16]

At any time, consumers can take actions to help mitigate the risk of identity theft. For example, consumers can implement a credit freeze free of charge, which can help prevent new-account fraud by restricting potential creditors from accessing the consumer's credit report.[17] Similarly, implementing a free fraud alert with a credit bureau can help prevent fraud because it requires a business to verify a consumer's identity before issuing credit.[18] However, consumers are limited in the direct actions they can take against a CRA in the event of a data breach,

[16]CFPB placed all of the information related to the Equifax breach, including information about known or potential scams, at www.consumerfinance.gov/equifaxbreach.

[17]A credit freeze generally allows consumers to request a freeze on their credit reports by contacting each of the nationwide CRAs. Consumers are given a unique personal identification number or password that they use to temporarily lift or remove the freeze (for example, when they are applying for credit or employment). In May 2018, Congress passed the Economic Growth, Regulatory Relief, and Consumer Protection Act, which requires that, free of charge, CRAs place credit freezes no later than 1 business day after and lift credit freezes no later than 1 hour after receiving a direct request from a consumer via telephone or secure electronic means. Pub. L. No. 115-174, § 301(a), 132 Stat. 1296, 1326 (2018) (codified at 15 U.S.C. § 1681c–1(i)).

[18]Consumers who suspect that they have been or are about to become victims of fraud can request an initial fraud alert at no cost with any one of the three nationwide consumer reporting agencies, which automatically notify the other two. See 15 U.S.C. § 1681c-1(a)(1). An initial fraud alert stays on the victim's credit file for not less than one year. Consumers with identify theft reports may request an extended fraud alert, which lasts for seven years. See 15 U.S.C. § 1681c-1(b)(1). Active duty alerts, which last for not less than one year, are available to deployed service members. See 15 U.S.C. § 1681c-1(c).

for two primary reasons. First, consumers generally cannot determine the source of the data used to commit identity theft. As a result, it can be difficult to link a breach by a CRA (or any other entity) to the harm a consumer suffers from a particular incidence of identity theft, which makes it challenging to prevail in a legal action. Second, unlike with many other products and services, consumers generally cannot exercise choice if they are dissatisfied with a CRA's privacy or security practices. Specifically, consumers cannot choose which CRAs maintain information on them. In addition, consumers do not have a legal right to delete their records with CRAs, according to CFPB staff, and therefore cannot choose to remove themselves entirely from the CRA market.

FTC and CFPB have noted that the level of consumer protection required can depend on the consumer's ability to exercise choice in a marketplace. For example, when determining whether a practice constitutes an unfair practice, FTC considers whether the practice is one that consumers could choose to avoid. Similarly, according to CFPB staff, the consumer reporting market may pose higher risk to consumers because consumers cannot choose whether or which CRAs possess and sell their information.

Chairman Krishnamoorthi, Ranking Member Cloud, and Members of the Subcommittee, this concludes my prepared remarks. I would be happy to answer any questions that you may have.

GAO Contact and Staff Acknowledgment

If you or your staff have any questions about this statement, please contact Michael Clements at (202) 512-8678 or clementsm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. In addition to the contact named above, John Forrester (Assistant Director), Winnie Tsen (Analyst-in-Charge), and Rachel Siegel made key contributions to the testimony. Other staff who made key contributions to the report cited in the testimony are identified in the source product.

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 GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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