

GAO Highlights

Highlights of [GAO-19-196](#), a report to congressional requesters

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.

GAO was asked to examine issues related to federal oversight of CRAs. Among other things, this report 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. GAO reviewed relevant laws, documentation related to CRA examinations, and policies and practices of selected CRAs; and interviewed representatives of regulatory agencies, CRAs, consumer and industry groups, and Attorneys General from four states with consumer reporting requirements.

What GAO Recommends

GAO recommends that Congress consider giving FTC civil penalty authority to enforce GLBA's safeguarding provisions. GAO also recommends 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-19-196](#). For more information, contact Michael Clements at (202) 512-8678 or clementsm@gao.gov, or Nicholas Marinoss at (202) 512-9342 or marinosn@gao.gov.

February 2019

CONSUMER DATA PROTECTION

Actions Needed to Strengthen Oversight of Consumer Reporting Agencies

What GAO Found

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. According to CFPB staff, the bureau does not have authority to examine for or enforce the GLBA's safeguards provisions. After the Equifax breach, however, 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.

If a CRA experiences a data breach, affected 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 the CRA. 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 because they do not have a legal right to delete their records with CRAs. This limited control by consumers, coupled with the large amount and sensitive nature of the information CRAs possess, underscores the importance of appropriate federal oversight of CRAs' data security.