United States Government Accountability Office

Report to Congressional Requesters

February 2019

# CONSUMER DATA PROTECTION

# Actions Needed to Strengthen Oversight of Consumer Reporting Agencies

GAO-19-196

February 2019

# CONSUMER DATA PROTECTION

## Actions Needed to Strengthen Oversight of Consumer Reporting Agencies

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 Marinos at (202) 512-9342 or marinosn@gao.gov.

### 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.

# Contents



Figures

## Abbreviations

| | |
|---|---|
| CFPB | Consumer Financial Protection Bureau |
| CRA | Consumer Reporting Agency |
| Dodd-Frank Act | Dodd-Frank Wall Street Reform and Consumer Protection Act |
| FCRA | Fair Credit Reporting Act |
| FTC | Federal Trade Commission |
| FTC Act | Federal Trade Commission Act |
| GLBA | Gramm-Leach-Bliley Act |

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

February 21, 2019

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

The Honorable Elizabeth Warren
Ranking Member
Subcommittee for Financial Institutions and Consumer Protection
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
House of Representatives

The Honorable Elijah Cummings
Chairman
Committee on Oversight and Reform
House of Representatives

In 2017, the consumer reporting agency (CRA) Equifax, Inc., disclosed that it had experienced a data breach and that unknown individuals had extracted from its databases sensitive consumer information—such as names, addresses, birth dates, and credit card, driver's license, and Social Security numbers—of at least 145.5 million consumers in the U.S. Such unauthorized access to personally identifiable information could lead to identity theft, raising concerns among policymakers about how CRAs in general are collecting, using, and protecting sensitive consumer information. We have addressed issues related to data breaches and identity theft in our prior work, including our recent analysis of the Equifax data breach.[1]

According to the Consumer Financial Protection Bureau (CFPB), the consumer reporting market comprises more than 400 companies, and the Consumer Data Industry Association reports that these companies issue

[1]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).

three billion reports and make more than 36 billion updates to consumer files each year. These companies collect vast amounts of sensitive consumer information, package it into consumer reports, and sell the reports to third parties.[2] Banks, employers, and others use these reports to make credit, employment, insurance, and other decisions. According to a 2018 Department of the Treasury report, the three nationwide CRAs—Equifax, Experian, and TransUnion—maintain credit files on nearly 210 million Americans.[3]

You asked us to examine issues related to the causes of the Equifax breach, Equifax's response to the breach, federal oversight of CRAs, and the role of CRAs in federal agencies' implementation of government programs.[4] This report, one in a series of our reports that addresses these issues, examines the oversight of CRAs, specifically (1) the federal laws and regulations governing CRAs' collection, use, and protection of consumer information; (2) measures the Federal Trade Commission (FTC) has taken to enforce CRA compliance with requirements to protect consumer information; (3) measures CFPB has taken to ensure that CRAs protect consumer information; and (4) FTC's and CFPB's roles in assisting consumers following a data breach and actions consumers can take following a data breach of a CRA.

To examine the laws governing CRAs, we identified relevant laws and reviewed them for their application to CRAs. We interviewed and reviewed documentation from the three nationwide CRAs and interviewed three additional CRAs that produce or compile consumer reporting

[2]A consumer report is a CRA's communication of information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected for the purpose of serving as a factor in establishing the consumer's eligibility for credit, insurance, employment, or other authorized purposes. 15 U.S.C. § 1681a(d)(1).

[3]Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (Washington, D.C.: July 2018).

[4]GAO-18-559 addresses questions related to the causes and impacts of the Equifax breach and Equifax's response to the breach, and a forthcoming report will address the role of CRAs in federal agencies' implementation of government programs.

information.[5] We selected these CRAs because they are not sector-specific and hold information on a broad segment of the population. We conducted a site visit to Equifax's Alpharetta, Georgia data center to learn more about steps the company takes to comply with relevant consumer protection laws. In addition, we interviewed staff from CFPB and FTC, and the Office of the Attorney General of four states with existing or proposed information protection laws or regulations that vary from federal requirements (California, Illinois, Massachusetts, and New York). We also interviewed associations representing companies that furnish consumer information to and use consumer reports from CRAs—the American Bankers Association, the Property Casualty Insurance Association of America, and the National Retail Federation—about their roles in the collection, use, and protection of consumer data, and steps they take to comply with relevant laws.

To assess FTC and CFPB measures to enforce information protection provisions and to ensure CRAs' proper collection, use, and protection of consumer information, we reviewed documents from FTC and CFPB. 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 documentation on the scope of CFPB examinations of larger market participant CRAs since 2015, as well as findings from recent CRA examinations.[6] In addition, we reviewed CFPB examination guidance for supervising these CRAs, including CFPB's internal guidelines for conducting data security examinations. We also reviewed documents related to CFPB's process for prioritizing which institutions and which product lines should receive supervisory examination, and we interviewed CFPB staff about this process. We interviewed officials from FTC and CFPB on their oversight activities, and we interviewed representatives of industry, consumer, and privacy groups on their views about supervision and oversight of CRAs.

[5]We use "nationwide CRA" to refer to what the Fair Credit Reporting Act (FCRA) defines as a "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis." FCRA defines this phrase as a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining public record information and credit account information regarding consumers residing nationwide for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity. 15 U.S.C. § 1681a(p).

[6]CFPB defines larger market participant CRAs as those with more than $7 million in annual receipts from consumer reporting. *See* 12 C.F.R. § 1090.104(b).

To assess FTC's and CFPB's roles in assisting consumers, as well as actions consumers can take following a data breach of a CRA, we reviewed the two agencies' websites and other publicly available consumer educational materials. We also interviewed staff from these agencies about their roles in assisting consumers following a breach. To identify actions consumers can take following a data breach, we reviewed our prior related reports and spoke with the industry and consumer representatives noted above.[7] See app. I for a more detailed discussion of our scope and methodology for this report.

We conducted this performance audit from November 2017 to February 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Background

## The Consumer Reporting Process

Information on consumers is exchanged through a consumer reporting process that includes consumers, CRAs, furnishers, and users of that information (see fig.1).

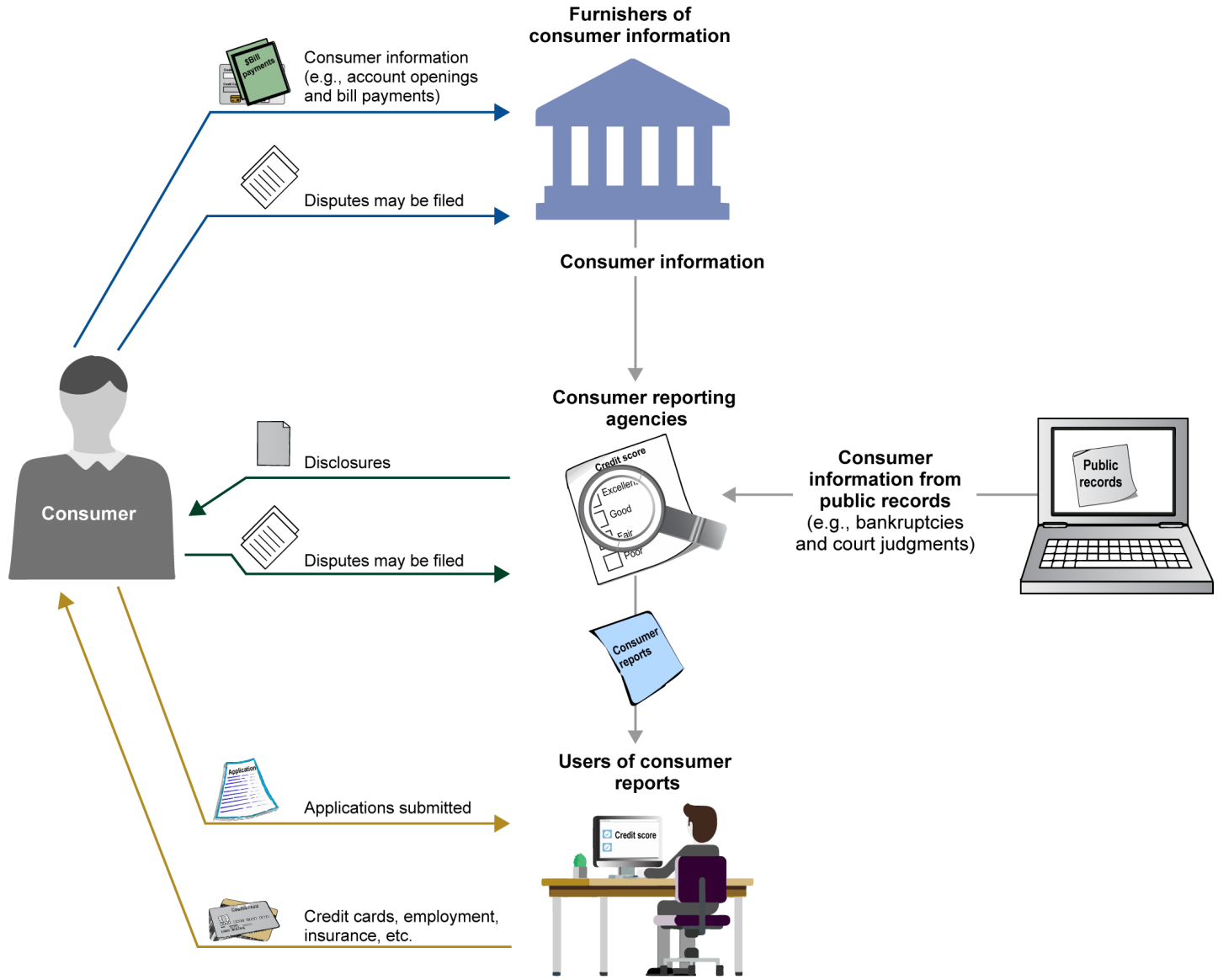
- **Consumers** are individuals whose information is collected and shared to make eligibility decisions, such as for credit, insurance, or employment.[8]

[7]Prior GAO reports included GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, GAO-17-254 (Washington, D.C: Mar. 30, 2017) and GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: June 26, 2006).

[8]Under the Gramm Leach Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999), a "consumer" is an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes. 15 U.S.C. § 6809(9). Under FCRA, Pub. L. No. 91-508, tit. VI, §§ 601-622, 84 Stat. 1114, 1127-1136 (1970), a "consumer" is an individual. 15 U.S.C. § 1681a(c). For purposes of this report, we use "consumer" to refer to any individual about whom a CRA has consumer report information, such as payment history, regardless of whether the individual engaged the services of the CRA.

- **CRAs** are companies that assemble or evaluate consumer information for the purpose of furnishing consumer reports to third parties who use the reports to determine consumer eligibility for employment, or products and services such as credit and insurance.
- **Furnishers** are entities such as banks or credit card companies that provide CRAs with consumer information, such as account openings, bill payments, or delinquency information. CRAs use this information, along with other information, including from public records such as bankruptcies, to compile consumer reports.
- **Users** are banks, credit card companies, employers, or other entities that use consumer reports to make eligibility decisions for individual consumers. Users vary in the specific information they request from CRAs and how they interpret the data. Some institutions, such as banks, may act as both furnishers and users.

**Figure 1: The Consumer Reporting Process**




Source: GAO analysis of consumer reporting information. | GAO-19-196

During the consumer reporting process, a consumer would not necessarily interact with the CRA; however, if the consumer discovered inaccurate information on their credit report as a result of, for example, being denied credit, the consumer could file a dispute with the CRA or the furnisher. Consumers may also request copies of their consumer reports

from CRAs directly, and CRAs may provide consumers with disclosures about how their information is being shared.

## 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.[9] 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.[10] 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.[11] 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.[12]

## 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

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

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

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

[12] 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.

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 from the theft of a device. A breach can also occur as a result of a cyber-based attack by individuals or groups, including organizations' own employees, foreign nationals, or terrorists.[13] 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.[14] 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.[15] Equifax's investigation of the breach identified 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.[16]

While data breaches do not always result in measurable harm, intruders may retain or resell stolen information to commit identity theft, which can include existing-account fraud and new-account fraud. In existing-account fraud, identity thieves use financial account identifiers, such as credit card or debit card numbers, to take over an individual's existing accounts to make unauthorized charges or withdraw money. In new-account fraud,

[13]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).

[14]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.

[15]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.

[16]GAO-18-559.

identity thieves use an individual's identifying data, such as Social Security and driver's license numbers, to open new financial accounts and incur charges and obtain credit in an individual's name without that person's knowledge. In addition, identity thieves may commit synthetic identity fraud, where they combine real and/or fictitious information to create identities with which they may defraud financial institutions, government agencies, or individuals.[17]

## Several Federal Laws Govern the Collection, Use, and Protection of Consumer Information

### FCRA Governs the Accuracy, Use, and Sharing of Consumer Information, and CRAs Reported Taking Actions to Comply

FCRA, enacted in 1970, is one of the primary federal laws governing the personal information that CRAs hold.[18] It governs the accuracy of this information and gives consumers rights to view, correct, or opt out of the sharing or use of certain aspects of their personal information among affiliates. FCRA also applies to how CRAs can use and share the information.

**Accuracy of collected information.** FCRA requires that when preparing a consumer report, CRAs follow reasonable procedures to assure "maximum possible accuracy" of the information concerning the individual about whom the report relates.[19] Companies that furnish information to CRAs also must take steps regarding the accuracy of information they report, as required by FCRA and its implementing

[17]See GAO, *Highlights of a Forum: Combating Synthetic Identity Fraud,* GAO-17-708SP (Washington, D.C.: July 2017) for more information on synthetic identity fraud.

[18]Pub. L. No. 91-508, tit. VI, §§ 601-622, 84 Stat. 1114, 1127-1136 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x). In this section, we focus on the primary laws that govern CRAs' collection, use, and protection of consumer information generally. Additional laws may apply to certain specialty CRAs, such as those that collect health-related information.

[19]15 U.S.C. § 1681e(b).

regulation, Regulation V.[20] A 2012 CFPB report cited steps that nationwide CRAs take to help ensure that information they collect from furnishers is legitimate and accurate.[21] The report notes that initial screening of furnishers generally includes an inspection of the companies' physical headquarters, phone numbers, websites, business licenses, and company records such as annual reports. In addition, these CRAs may hire third-party investigation services to screen for illegal or unethical business practices. They may also conduct additional inspections in response to consumer complaints, variations in data reporting, or changes in a furnisher's ownership. To conduct quality checks on data submitted by furnishers, CFPB reported that the nationwide CRAs check for blank fields or logical inconsistencies. Representatives of CRAs we spoke with provided examples of the quality assurance steps they take. For example, one representative told us that they look for violations of logical patterns, such as a loan going from 30 days past due to 90 days past due over the course of one month. CFPB reported that when inaccuracies are identified, the CRAs can reject the information. These steps may improve the quality of the information received from furnishers, but they cannot ensure the accuracy of such data.

**Use and sharing of information.** FCRA permits CRAs to provide users with consumer reports only if the user has a "permissible purpose," such as to process a credit application, screen a job applicant, or underwrite an insurance policy, subject to limitations where the credit or insurance transaction is not initiated by the consumer.[22] FCRA also prohibits the use of a consumer report for any purpose other than that specified to the CRA when the user obtained the report.[23] It also requires that CRAs take steps to validate the

[20]*See* 15 U.S.C. § 1681s-2(a) and 12 C.F.R. § 1022.42(a). Those who furnish information to CRAs regularly and in the ordinary course of business have a duty to provide accurate information about their transactions or experiences with consumers; if a furnisher determines that information it provided to a CRA is not complete or accurate, the furnisher must promptly notify the CRA about the error and provide any corrections. See 15 U.S.C. § 1681s-2(a)(2). We will discuss requirements related to the accuracy of data collected and used by CRAs in a forthcoming report.

[21]Consumer Financial Protection Bureau, *Key Dimensions and Processes in the U.S. Credit Reporting System: A Review of How the Nation's Largest Credit Bureaus Manage Consumer Data* (Washington, D.C.: December 2012).

[22]*See* 15 U.S.C. § 1681b.

[23]*See* 15 U.S.C. § 1681b(f).

legitimacy of users and their requests for consumer report information and apply FCRA requirements to the sharing of information within their companies.[24]

**Validating the legitimacy of users and their requests for consumer report information.**[25] Representatives of CRAs told us they take several steps to validate the legitimacy of users and their requests, including verifying credit transactions, periodically evaluating user agreements, and validating users' identities. For example, representatives of one CRA said they sometimes conduct on-site visits to verify the existence of an entity and the business it conducts. In addition, they said they randomly select 6,000 to 8,000 consumer files each year and ask users associated with those files to show proof that the consumers engaged in the credit transactions contained in those files. However, several CRAs told us that these steps cannot guarantee that the users and requests are valid. For example, representatives of one CRA noted that once a user has the information, a CRA would find it difficult to prevent that user from retaining and reusing it for purposes other than the original permissible purpose.

**Applying FCRA requirements to sharing information internally.** As amended by the Fair and Accurate Credit Transactions Act of 2003, FCRA limits the ability of affiliated companies to market products or services to consumers using shared consumer data. Affiliates may use consumer report information for product or service marketing only if they clearly and conspicuously disclose to the consumer that the information may be shared for such solicitations, the consumer is provided a simple method to opt out of such solicitations, and the consumer does not opt out.[26] Representatives of CRAs told us that they apply the same FCRA protections when they share consumer reporting data among their departments or subsidiaries, which may use the data for other purposes. For

[24] *See* 15 U.S.C. § 1681e and § 1681s-3(a).

[25] Under FCRA, CRAs must make a reasonable effort to verify the identity of a new prospective user prior to furnishing such user a consumer report. If a CRA has reasonable grounds for believing that a consumer report will not be used for a permissible purpose, the CRA may not furnish the consumer report. 15 U.S.C. § 1681e(a).

[26] *See* 15 U.S.C. § 1681s-3(a) (as amended by Pub. L. 108–159, tit. II, § 214(a)(2), 117 Stat. 1952, 1980).

example, one nationwide CRA said that one of its internal groups seeks to ensure that the company implements appropriate legal protections when it shares data for other uses within the company.

Staff from state Attorneys General offices we spoke with told us that their states also have laws pertaining to consumer reporting, which have similar requirements to those in FCRA.[27] In addition, they noted that while there is no federal data breach notification law, all 50 states have laws requiring companies to notify consumers in the event of a data breach. According to the National Conference of State Legislatures, those laws have varying requirements, such as the timing or method of notification, and who must be notified.

## GLBA and Other Laws Govern the Protection of Consumer Information

Congress enacted GLBA in part to protect the privacy and security of nonpublic personal information that individuals provide to financial institutions.[28] According to FTC staff, CRAs may be considered financial institutions under GLBA if they collect, maintain, and report on consumer information.[29] As with FCRA, GLBA restricts financial institutions from sharing consumers' private information, but GLBA restricts sharing with nonaffiliated third parties specifically, and those parties face similar restrictions in how they may further share or use the information.[30]

[27]If a state consumer reporting or protection law conflicts with FCRA, FCRA requirements preempt the state requirements; but if a state consumer reporting law has additional requirements that are consistent with FCRA, the state requirements may apply.

[28]*See* Pub. L. No. 106-102, tit. V, §§ 501-509, 113 Stat. 1338, 1436 (1999) (codified as amended at 15 U.S.C. §§ 6801-6809). Subtitle A of title V of the act contains the privacy, security, and confidentiality provisions relating to nonpublic personal information. 15 U.S.C. §§ 6801-6809.

[29]As applicable to consumer reporting agencies, GLBA privacy provisions (but not its data safeguards provision) are implemented in CFPB's Regulation P, 12 C.F.R. pt. 1016. Under GLBA, "financial institution" is defined as any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k)), among other things. *See* 15 U.S.C. § 6809(3)(A). Activities that are financial in nature includes any activity that the Board of Governors of the Federal Reserve System has determined to be so closely related to banking or managing or controlling banks as to be a proper incident thereto. 12 U.S.C. § 1843(k)(4)(F). Maintaining information related to the credit history of consumers and providing the information to a credit grantor who is considering a borrower's application for credit or who has extended credit to the borrower is considered an activity that is financial in nature. *See* 12 C.F.R. § 225.28(b)(2)(v).

[30]*See* 15 U.S.C. § 6802(c).

In addition, unlike FCRA, GLBA includes a provision directing FTC and certain federal regulators (not including CFPB) to establish standards specifically with respect to protection against any anticipated threats or hazards to the security of customer records. Specifically, under GLBA, these federal regulators are directed to establish appropriate standards for financial institutions under their jurisdiction to ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.[31] To implement these standards for CRAs, and other entities that fall under its jurisdiction, FTC adopted its Safeguards Rule, which requires, among other things, that financial institutions have a written information security program, assess the risks to customer information, and evaluate and adjust the information security program in light of foreseeable risks.[32] FTC staff told us that because GLBA applies to information about a consumer with a customer relationship with a financial institution, the Safeguards Rule may not apply in all cases where a CRA holds personal information on individuals.[33] For example, they said that GLBA would more clearly apply if the consumer had purchased credit monitoring or other products or services directly from the CRA, or if the CRA obtained customer information from another financial institution, such as a bank. Representatives of the three nationwide CRAs told us that for purposes of protecting information, they do not distinguish between consumers with whom they have a direct customer relationship and those with whom they do not.

[31] *See* 15 U.S.C. § 6801(b). Banking agencies have implemented GLBA's safeguards requirements through the Interagency Guidelines on Information Security. *See* Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616 (Feb. 1, 2001). Authority to write, supervise for compliance with, and enforce these standards was carved out of CFPB's authority by section 1002(12)(J) of the Dodd-Frank Act. *See* 12 U.S.C. § 5481(12)(J); *see also* 15 U.S.C. § 6801(b).

[32] *See* 16 C.F.R. § 314.3-4. The Safeguards Rule implements GLBA's requirements for entities that fall under FTC jurisdiction, including CRAs, check-cashing businesses, payday lenders, mortgage brokers, and other entities.

[33] Under GLBA, "consumer" means an individual who obtains from a financial institution financial products or services that are to be used primarily for personal, family, or household purposes, or that individual's legal representative. 15 U.S.C. § 6809(9). Under GLBA's implementing Regulation P, a "customer" is a consumer who has a continuing relationship with a financial institution that provides one or more financial products or services to the consumer primarily for personal, family, or household purposes. *See* 12 C.F.R. § 1016.3(i)-(j).

CRAs we spoke with provided examples of how they protect consumer information and meet GLBA requirements to maintain administrative, technical, and physical safeguards. For example, with respect to administrative safeguards, representatives of one CRA said they enforce contractual requirements for data access and data security. Representatives of another CRA said that the technical safeguards they use include firewalls, anti-virus software, and malware protection. Examples of physical safeguards from another CRA included monitoring data centers by video and restricting access to secure data rooms. To address data protection more generally, representatives of CRAs we spoke with told us they routinely conduct internal audits of their data security systems, and that the financial institutions they work with frequently conduct audits of their risk management practices, including CRAs' data security controls.[34]

Provisions related to unfair or deceptive acts or practices also may apply to CRAs' protection of consumer data. Specifically, under FTC's authority, section 5 of the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices" in or affecting commerce.[35] In the context of privacy and security, these provisions require companies to truthfully represent practices to consumers. For example, FTC has found companies that alleged that they were following certain security protections, but did not in fact have such security features, to have engaged in unfair or deceptive practices. Similarly, the Dodd-Frank Act prohibits providers of consumer financial products or services from engaging in "unfair, deceptive, or abusive acts or practices," and CFPB has authority to enforce and supervise for compliance with this provision.[36] CFPB has alleged that claims to consumers that transactions are safe and secure while simultaneously lacking basic security practices can constitute unfair, deceptive, or abusive acts or practices. FTC and

[34]Federal banking regulators expect supervised financial institutions to exercise due diligence when selecting third parties with which they enter into business relationships and to maintain effective risk management practices with such third parties, which, according to regulators we spoke with, can include CRAs. *See, e.g.*, OCC Bulletin 2013-29, Third-Party Relationships (Oct. 30, 2013).CRAs we spoke with said that because of this expectation, they are subject to frequent data security reviews by their financial institution clients. For example, one nationwide CRA told us it receives roughly 30 to 50 requests for such reviews a month.

[35]*See* 15 U.S.C. § 45.

[36]*See* Pub. L. No. 111-203, §§ 1031, 1036, 124 Stat. 1376, 2005, 2010 (2010) (codified at 12 U.S.C. §§ 5531, 5536).

CFPB officials said that in the case of data breaches, they would examine each case individually to determine whether the institution violated these provisions in connection with the breach.

Some states also have laws that protect consumer information, including laws that generally govern data security. For example, staff from the Massachusetts Attorney General's office told us that their state has a data security law similar to FTC's Safeguards Rule but with more specific requirements, including those for malware detection and firewalls. According to the National Consumer Law Center, all 50 states have consumer protection laws that prohibit unfair or deceptive practices. Staff from state Attorneys General offices told us that they can prosecute entities for potential violations of these provisions, including data breaches. They told us that following the Equifax breach, several states' Attorneys General launched a joint investigation into whether Equifax violated state laws, including prohibitions of unfair or deceptive practices. According to staff from one state Attorney General office, as of February 2019, this investigation was ongoing. In addition, Equifax reported that individual states have also filed legal action or have ongoing investigations. For example, Massachusetts and West Virginia have filed civil enforcement actions against Equifax that seek various remedies, including civil penalties.

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

## FTC Enforces CRA Compliance with Consumer Protection Laws

FTC enforces compliance with consumer protection laws under authorities provided in FCRA, GLBA, and the FTC Act. FCRA authorizes FTC to enforce compliance for nearly all companies not supervised by either a federal banking regulator or certain other federal agencies.[37] GLBA authorizes FTC to issue certain rules and enforce compliance for all nonbank financial institutions and other entities not under the jurisdiction of a federal banking regulator, the National Credit Union Administration, Securities and Exchange Commission, or state insurance regulators.[38] The FTC Act authorizes FTC to investigate and take administrative and civil enforcement actions against companies under its jurisdiction that engage in unfair or deceptive acts or practices in or affecting commerce.[39] 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 had taken a total of 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.

If FTC has reason to believe that a company has violated laws under its jurisdiction, it may initiate an investigation to determine whether to take enforcement action. FTC staff said that in determining whether to take on a case related to privacy and data security matters, they consider factors

[37] *See* 15 U.S.C. § 1681s(a)(1).Other agencies with FCRA enforcement authority include, but are not limited to, the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, National Credit Union Administration, Securities and Exchange Commission, and Department of Transportation. *See* 15 U.S.C. § 1681s(b)(1).

[38] *See* 15 U.S.C. § 6805(a)(7).

[39] *See* 15 U.S.C. § 45.

such as the company's size and the sensitivity of the data in the company's network. For example, FTC may choose not to investigate a data breach of a small company that affects few people; however, it may investigate a potential data security violation of a large company, even without evidence of a breach. Under its statutory authority, FTC can ask or compel companies to produce documents, testimony, and other materials to assist in its investigations.[40] In June 2018, FTC notified Equifax that it was considering legal action against the company as a result of its 2017 data breach, including seeking civil penalties.

If FTC finds that a company violated consumer law, the agency may take several different actions depending on its legal authority and what it considers to be the most appropriate response. For example, FTC may, in administrative proceedings, issue cease-and-desist orders for unfair or deceptive acts or practices. Further, FTC generally may seek a range of remedies from the U.S. district courts, including injunctions, damages to compensate consumers for their actual losses, and disgorgement of ill-gotten funds.[41] In limited circumstances, FTC also may seek civil money penalties, which are monetary fines imposed for a violation of a statute or regulation.[42]

Examples of FTC enforcement actions related to consumer reporting include:

- In May 2016, FTC settled with a furnisher that allegedly violated FCRA requirements to have adequate policies and procedures for reporting accurate credit information to CRAs.[43] FTC alleged that a debt collector acting as a furnisher did not have a written policy regarding the accuracy and integrity of information it furnished, and in numerous instances failed to inform consumers about these outcomes.

[40] *See* 15 U.S.C. § 49.

[41] Injunctions are judicial orders commanding a party to take an action or prohibiting a party from doing or continuing to do a certain activity. Disgorgement requires wrongdoers to give up profits or other gains illegally obtained.

[42] *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.

[43] *U.S. v. Credit Protection Assoc. LP*, Case No. 3:16-cv-01255-D (N.D. Tex. May 9, 2016)(stipulated final order for permanent injunction and civil penalty judgment).

- In 2011, FTC brought enforcement actions against three CRAs that merge, and then sell, information from the three nationwide CRAs. FTC alleged that these companies did not meet GLBA standards and violated unfair or deceptive practices prohibitions by not providing reasonable and appropriate security for consumers' personal information. These violations included not developing and disseminating information security policies, and not addressing risks by, for example, evaluating the security of end users' computer networks.[44]
- In 2006, FTC settled with ChoicePoint—a CRA—and imposed a $10 million civil penalty for violations of FCRA stemming from a 2005 data breach. In 2009, FTC obtained an additional $275,000 in equitable monetary relief due to ChoicePoint's violation of the order after an additional data breach occurred in 2008.[45]

## FTC's Lack of Civil Penalty Authority for GLBA May Hinder Its Effectiveness in Enforcing Data Security Provisions

As previously discussed, in some circumstances, FTC enforcement authority can include civil money penalties. This includes cases of knowing violations of FCRA.[46] For example, in a 2014 settlement, FTC levied $525,000 in civil penalties against a CRA after alleging that the company did not comply with FCRA provisions to ensure the accurate and permissible use of its reports. FTC does not have civil penalty authority for initial violations of the FTC Act but may obtain civil penalties from companies for violations of FTC Act orders.

FTC's civil penalty authority does not extend to initial violations of GLBA's privacy and safeguarding provisions, which 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, which are enforced pursuant to FTC Act authority, 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. However, determining the appropriate amount of consumer compensation requires

[44]In the Matter of ACRAnet, Inc.; SettlementOne Credit Corp.; and Fajilan and Associates, Inc. d/b/a Statewide Credit Services, 76 Fed. Reg. 7213 (Feb. 9, 2011).

[45]*U.S. v. ChoicePoint, Inc.*, Case No. 1:06-cv-198-JTC (N.D. Ga. Oct. 19, 2009) (supplemental stipulated judgment and order for permanent injunction and monetary relief).

[46]*See* 15 U.S.C. § 1681s(a)(2)(A). Liability under this provision may be up to $2,500 per violation.

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. 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. In addition, it can 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 redress 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 the monetary harm to individual consumers.

FTC staff told us and testified before Congress that civil penalties are often the most appropriate remedy for a data breach, and that such penalties serve as an effective deterrent in cases involving weak data privacy and security policies and practices.[47] 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. Unlike FTC, other regulators have civil penalty authority to punish entities that violate provisions of GLBA. For example, the Office of the Comptroller of the Currency has said that it can enforce GLBA privacy and safeguard provisions with civil money penalties against any insured depository institution or institution-affiliated party subject to its supervision.[48]

In our 2009 report on modernizing the financial regulatory framework, we stated that financial regulators should have the authority to carry out and enforce their statutory missions.[49] In the case of FTC, this includes having the tools necessary to meet its mission of protecting consumers from

[47]In December 2018, FTC also held a hearing on data security. This hearing included discussions on several issues, including whether Congress should provide FTC with civil penalty authority for data security enforcement. The full hearing can be accessed at https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018.

[48]Under the Federal Deposit Insurance Act, the federal banking regulators have broad civil money penalty authority. *See* 12 U.S.C. § 1818(i)(2).

[49]GAO, *Financial Regulation: A Framework for Crafting and Assessing Proposals to Modernize the Outdated U.S. Financial Regulatory System,* GAO-09-216 (Washington, D.C: Jan. 8, 2009).

harm, including the harm caused by misuse of personal information, by having the range of authorities to punish entities for violations of the statutes and regulations the agency enforces.

In 2006, we suggested that Congress consider providing FTC with civil penalty authority for its enforcement of GLBA's privacy and safeguarding provisions.[50] We noted that providing this authority would give FTC a practical enforcement 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.

[50]GAO-06-674.

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

## CFPB Enforces and Examines CRA Compliance with Consumer Protection Laws

CFPB enforces compliance with most provisions of FCRA; several provisions of GLBA; and the prohibition of unfair, deceptive, or abusive acts or practices under the Dodd-Frank Act.[51] According to CFPB staff, CFPB cannot enforce data security standards under these statutory provisions or the FTC's implementing rules because CFPB does not have authority to supervise for or enforce compliance with the GLBA's safeguards provision or FCRA's red flags or records disposal provisions.[52]

[51]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, while 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.

[52]Under GLBA, CFPB has enforcement authority over any financial institution and other covered persons or service providers that are subject to the the agency's jurisdiction and the act, with the exception of the safeguards rule issued under section 501 of GLBA. *See* 15 U.S.C. § 6805(a)(8).

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 unfair, deceptive, or abusive practices provisions. For example, in March 2017, CFPB settled with Experian for $3 million in civil penalties for an alleged violation of FCRA and alleged deceptive acts or practices.[53] Experian marketed to consumers an "educational credit score" that the company claimed lenders used to make credit decisions.[54] CFPB alleged that lenders did not use these "educational credit scores" for this purpose, and that Experian violated FCRA's implementing regulation by requiring consumers to view Experian advertisements before obtaining a free credit report. In December 2015, CFPB levied a fine of $8 million against another CRA—Clarity Services, Inc.—for obtaining consumer reports without a permissible purpose in violation of FCRA and failing to investigate consumer disputes.[55] CFPB is also continuing its investigation of Equifax's data breach.

CFPB supervises the larger market participant CRAs (those with more than $7 million in annual receipts from consumer reporting, as defined by CFPB) and has the authority to examine these CRAs for compliance with federal consumer financial protection laws. From 2015 through 2017, CFPB examined several CRAs. Some of these examinations resulted in findings of deficiencies related to data accuracy and dispute processes, and follow-up examinations were conducted as necessary.[56] As part of its supervisory role, CFPB also periodically monitors the nationwide CRAs by requesting information on their activities and identifying any changes in risk to consumers and the market. CFPB uses this information to learn of changes to a CRA's compliance, personnel, issues raised by the CRA's internal audits, or other developments that might affect CFPB's strategy for supervising the CRA.

[53] *In the Matter of Experian Holdings, Inc., et al*, File No. 2017-CFPB-0012 (Mar. 23, 2017) (consent order).

[54] CFPB reported that in addition to the credit scores that are used by lenders, several companies had developed "educational credit scores," which lenders rarely, if ever, used. These scores were intended to inform consumers, but were not used for credit decisions.

[55] *In the Matter of Clarity Services, Inc., et al*, File No. 2015-CFPB-0030 (Dec. 3, 2015) (consent order).

[56] *See*, *e.g.*, CFPB, *Supervisory Highlights Consumer Reporting Special Edition,* March 2017.

## CFPB May Not Be Identifying All CRAs under Its Supervisory 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 (as defined by CFPB). 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 whether CRAs meet the threshold may vary from year to year and CFPB has limited data to determine whether CRAs meet the threshold. Specifically, CFPB staff said that identifying additional larger market participant CRAs can be challenging. For example, the Securities and Exchange Commission does not require nonpublicly traded CRAs to file financial and other information that CFPB could otherwise use to identify these CRAs, which are generally not widely known to the public. In addition, CFPB staff said they do not ask CRAs to provide their annual receipts, with the exception of the specific CRAs being considered for examination in a given year, because CFPB staff said calculating these receipts could create an additional cost to the companies.

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.[57] One method for identifying institutions for oversight, particularly where data are limited, is to require companies to register with the relevant regulator. For example, among other requirements, insured depository institutions must obtain a charter to operate, and money services businesses generally must register with the Financial Crimes Enforcement Network. Similarly, CFPB could identify CRAs that meet the larger market participant threshold by requiring such businesses to register with them, subject to a rulemaking process and cost-benefit analysis of the burden it could impose on the industry. Another method CFPB could use to identify CRAs and inform its oversight activities would be to leverage information collected by states. Stakeholders we spoke with cited New York and Maine as examples

[57] GAO-09-216.

where CRAs are required to register with the state.[58] Implementing strategies such as registration or leveraging existing information could be a cost-effective way for CFPB to identify all CRAs under its authority. Identifying additional sources of information on the population of larger market participant CRAs—including those that are lesser-known, possibly unknown to CFPB, and possibly in possession of large amounts of sensitive consumer information—could help ensure that CFPB has more comprehensive information for carrying out its supervisory responsibilities.[59]

## CFPB's Prioritization of CRA Examinations Does Not Specifically Account for Data Security Risk

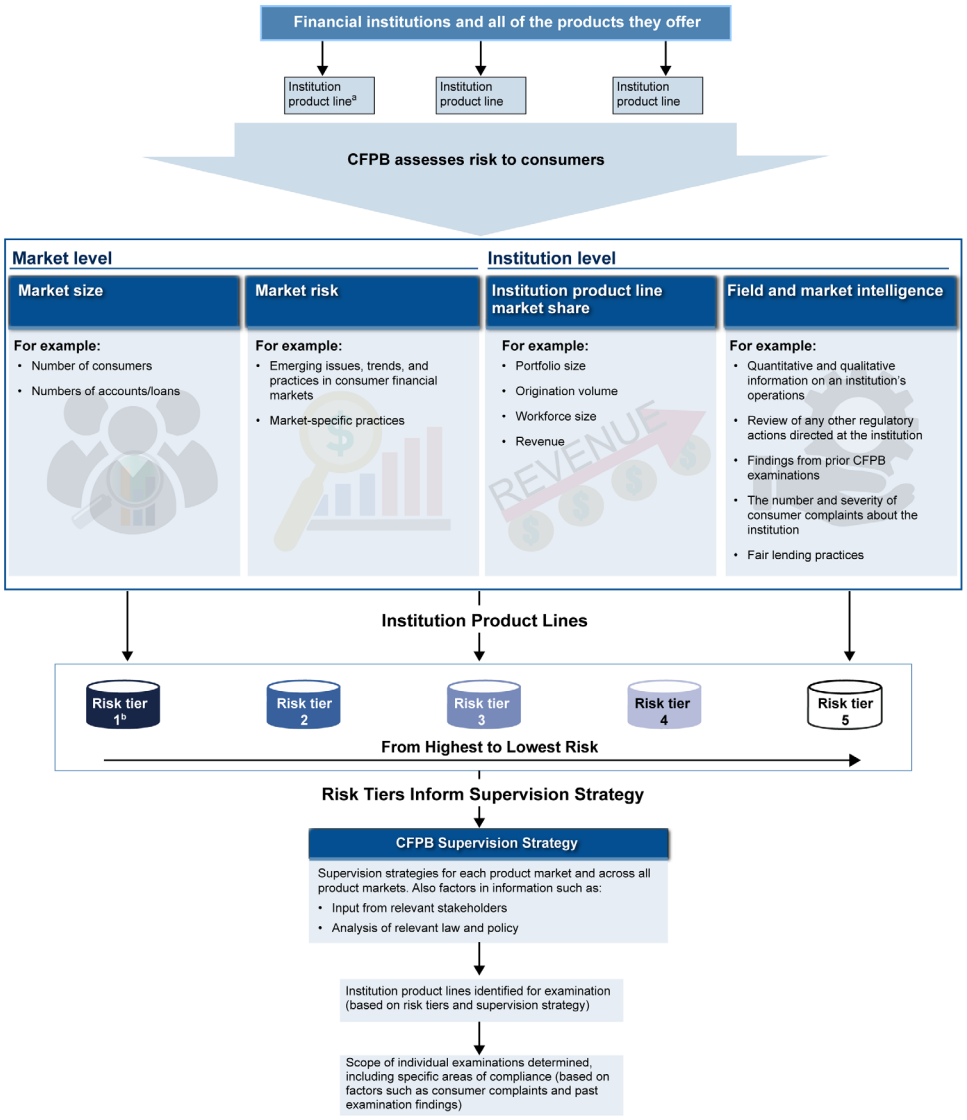
To determine which product lines, institutions, and compliance issues to examine, CFPB determines the institutions (for example, banks, credit unions, non-bank mortgage servicers, and CRAs) and the consumer product lines that pose the greatest risk to consumers, and prioritizes these for examinations annually (see fig.2). 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. Market size includes a consideration of a product's market size relative to other consumer finance product markets. Other market risk factors include the potential risk to consumers from new or existing products offered in the market as well as emerging risks and trends in consumer financial products. For example, CFPB noted that a market may be considered higher risk if consumers cannot choose the provider of a financial product or service in that market, or if the transactions occur between two businesses rather than between a business and consumers. Because they do not face the same risk of losing customers as companies in other

[58]In June 2018, the New York Department of Financial Services adopted a regulation requiring registration of consumer credit reporting agencies that have assembled, evaluated, or maintained a consumer credit report on one thousand or more New York consumers in the previous 12 months. Similarly, any credit reporting agency that is used by creditors in Maine must register with the Maine Department of Professional and Financial Regulation.

[59]In a prior report, we similarly found that CFPB lacked comprehensive data on all nonbank mortgage servicers. We recommended that CFPB collect more comprehensive data on the identity and number of nonbank mortgage servicers in the market, and CFPB implemented our recommendation. See GAO, *Nonbank Mortgage Servicers: Existing Regulatory Oversight Could Be Strengthened.* GAO-16-278 (Washington, D.C.: March 10, 2016).

markets, companies in higher-risk markets may not have the same financial incentives to protect the interests of consumers.

**Figure 2: Consumer Financial Protection Bureau (CFPB) Supervision Prioritization Framework**




Source: GAO analysis of Consumer Financial Protection Bureau (CFPB) information. | GAO-19-196

[a]Institution product lines are specific products offered by a particular financial institution.

[b]Risk tiers represent CFPB's sorting of institution product lines by the relative risk posed to consumers.

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. An institution's market share correlates with the number of consumers who could be affected by that institution's practices; therefore, CFPB generally places a higher priority on larger providers of products. 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, information obtained from CFPB's quarterly monitoring of institutions, public reports, and the number and severity of consumer complaints CFPB has received about the institution. Field and market intelligence can also include information about an institution's fair lending practices and its ability to provide fair, equitable, and nondiscriminatory access to credit.

Taking market and institutional considerations together, CFPB places institution product lines into tiers based on its determination of their relative risk to consumers. These risk tiers range from 1 to 5, with 1 being the lowest risk and 5 being the highest risk. Risk tiers then feed into CFPB's development of its supervision strategy, which includes other information, including information from subject matter experts and recent legal and policy decisions that could affect examinations, and consultations with internal stakeholders. CFPB uses both the risk tiers and information from its supervision strategy to identify potential institutions for examination. Following this process, CFPB has regularly determined CRAs' consumer reporting to be a high priority for examination since it began supervising them in 2012.

After identifying institution product lines to examine, CFPB determines specific areas of compliance to assess. These determinations are made 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. According to CFPB staff, the agency's process for determining

risk tiers incorporates the risk factors specifically cited in the Dodd-Frank Act, including those related to the size of a product market.[60] The Act also states that CFPB should consider other factors it determines to be relevant; as such, CFPB staff noted that certain elements of data protection have been included in the scope of some of its past CRA examinations. For example, CFPB staff said that in assessing compliance with FCRA's permissible purposes provision, the examination scope would include ensuring that data are not improperly shared. CFPB staff noted that the bureau cannot examine for compliance with or enforce 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 conduct some CRA data security examinations.[61] 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.

The Dodd-Frank Act requires CFPB, when implementing its risk-based supervision program, to consider risks posed to consumers in the relevant product and geographic markets. 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,

[60]The Dodd-Frank Act states that CFPB's risk-based supervision program should take into consideration risks posed to consumers in the relevant product markets and geographic markets, including the asset size of the covered person; the volume of transactions involving consumer financial products or services in which the covered person engages; the risks to consumers created by the provision of such consumer financial products or services; the extent to which such institutions are subject to oversight by state authorities for consumer protection; and any other factors that CFPB determines to be relevant to a class of covered persons. *See* Pub. L. No. 111-203, § 1024(b)(2), 124 Stat. 1376, 1987 (2010)(codified at 12 U.S.C. § 5514(b)(2)).

[61]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 is limited to supervisory recommendations.

nature of the risk, and appropriate response.[62] 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.

CFPB's reliance primarily on consumer complaints, information from public filings, and information and findings from past examination for prioritizing examinations may not fully detect data security risks that CRAs pose. Data accuracy and dispute resolution feature prominently in consumer complaints, according to CFPB staff, because consumers mostly interact with CRAs in these contexts. But consumers likely did not know, for example, about Equifax's data security challenges prior to its breach, so that vulnerability was not a focus of complaints. While the three nationwide CRAs acknowledged the risk of data breaches in recent public filings, other larger participant CRAs may not be publicly traded and therefore may not have public filings. Further, if CFPB's past examinations have not addressed data security, the agency cannot use those past examination findings to target current risks.

The Equifax breach demonstrated the vulnerability that CRAs may face with regard to data security. We have noted that advancements in technology, combined with the increasing sophistication of hackers and others with malicious intent, have increased the risk of sensitive personal information being exposed and compromised.[63] We have also reported that rapid developments in new technologies will continue to pose new threats to security, privacy, and safety.[64] In recent years, insured depository institutions—which, like CRAs, maintain large amounts of sensitive consumer data—have been subject to regular information technology examinations, which, according to one regulator, may include a cybersecurity component. Banking regulators have noted that unauthorized access to the information and systems that support these

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

[63]GAO, *High Risk Series: Urgent Actions are Needed to Address Cybersecurity Challenges Facing the* Nation, GAO-18-645T (Washington, D.C.: Jul. 25, 2018).

[64]GAO, *High Risk Series: Progress on Many High Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb.15, 2017).

institutions can affect operations, pose risk to consumers through exposure of private information, and undermine consumer confidence.

The risks may be similar for CRAs—companies that by definition also maintain extensive amounts of sensitive consumer information. By including routine consideration of data security risks into its process for prioritizing CRA examinations, CFPB can better ensure that its supervision of CRAs proactively detects such risks and helps prevent the further exposure or compromise of consumer information.

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

### FTC and CFPB Provide Consumers with Information on How to Address Identity Theft Risk

FTC and CFPB provide educational information for consumers on ways to mitigate the risk of identity theft. For example, FTC has a dedicated website (IdentityTheft.gov) that allows consumers to report suspected identity theft to FTC and develop and implement a recovery plan. In addition, FTC offers businesses guidance on steps to take in the event of a data breach, including notification of relevant parties and a model notification letter. CFPB's website offers consumers tips on how to protect their information and spot identity theft.[65] CFPB also publishes a consumer guide that lists CRAs and their websites, and ways to obtain free credit reports.

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

[65]For example, see https://www.consumerfinance.gov/ask-cfpb/how-can-i-spot-identity-theft-en-1359/.

shortly after Equifax's public announcement of the breach. These included information on ways that consumers could protect themselves in the wake of the breach and special protections and actions for service members.[66]

## Consumers Have Options to Mitigate Identity Theft Risk and Respond to Breaches

At any time, consumers can take actions to help mitigate identity theft risk. 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.[67] 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.[68] Consumers also can monitor their credit report for suspicious activity, either through self-review or by using a free or paid credit monitoring service.[69] FTC and others recommend that consumers regularly review their credit card and bank statements to detect fraudulent charges.[70]

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

[67]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)).

[68]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).

[69]Federal law requires each nationwide consumer reporting agency to provide one free credit report to consumers, upon request, each year. *See* 15 U.S.C. § 1681j(a); 12 C.F.R. § 1022.136. The authorized website for ordering these free credit reports is AnnualCreditReport.com.

[70]See GAO-17-254 for additional information about options consumers have to address identity theft, including paid identity theft services.

Consumers whose data have been compromised in any data breach can file a complaint with FTC or CFPB.[71] FTC has an online "complaint assistant," and FTC staff told us they use consumer complaints to help inform their investigatory and enforcement activity. CFPB staff told us that they use consumer complaints to help prioritize examinations and inform enforcement activity. In the 6 months following Equifax's announcement of its data breach, CFPB received more than 20,000 consumer complaints about the impact of the breach or Equifax's response.

However, consumers are limited in the direct actions they can take against a CRA in the event of a data breach, for two primary reasons. First, consumers generally cannot trace the source of the data used to commit identity theft to a particular breached entity. 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 may make 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 about 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.

## Conclusions

The 2017 data breach of Equifax highlighted the data security risks associated with CRAs. While companies in many industries have experienced data breaches, CRAs may present heightened risks because of the scope of sensitive information they possess and because consumers have very limited control over what information CRAs hold

[71]Consumers can also file complaints with other entities, such as state Attorneys General offices or consumer protection agencies.

and how they protect it. These challenges underscore the importance of appropriate federal oversight of CRAs' data security.

While FTC has taken significant enforcement actions against CRAs that have violated federal privacy or data security laws, it is important that the agency have all of the appropriate enforcement options to fulfill its mission of protecting consumers. However, GLBA, one of the key laws governing the security of consumer information, does not provide FTC with civil penalty authority. The remedies that FTC does have available under GLBA—such as disgorgement and consumer redress—may be less practical enforcement tools for violations involving breaches of mass consumer data. Accordingly, providing FTC with civil penalty authority can enable it to more effectively or efficiently enforce GLBA's privacy and safeguarding provisions.

Although CFPB is responsible for overseeing larger market participant CRAs, it lacks the data to identify with certainty all the CRAs under its supervision, in part because the sources it is using, such as public filings, are not comprehensive. Using additional methods to obtain information, such as requiring larger market participant CRAs to register with the agency or leveraging state registration information, would help CFPB ensure it is tracking all CRAs under its supervision and is providing appropriate oversight.

CFPB considers a number of market and institutional factors in prioritizing which CRAs to examine, but data security has not routinely been among these factors. Given the nature and amount of consumer information CRAs hold, as well as increasing threats from hackers and others with malicious intent, vulnerabilities in these companies' data security can pose significant risk to a vast number of consumers. By ensuring that its process for determining the scope of CRA examinations routinely includes factors that would detect data security risks, CFPB can better ensure the effectiveness of its supervision and help prevent further exposure or compromise of consumer information.

## Matter for Congressional Consideration

Congress should consider providing the Federal Trade Commission with civil penalty authority for the privacy and safeguarding provisions of the Gramm-Leach-Bliley Act to help ensure that the agency has the tools it needs to most effectively act against data privacy and security violations. (Matter for Consideration 1)

## Recommendations for Executive Action

We are making two recommendations to CFPB:

The Director of CFPB should identify additional sources of information, such as through registering CRAs or leveraging state information, that would help ensure the agency is tracking all CRAs that meet the larger participant threshold. (Recommendation 1)

The Director of CFPB should 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. (Recommendation 2)

## Agency Comments and Our Evaluation

We provided a draft of this report to CFPB, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FTC, and the Office of the Comptroller of the Currency. All of the agencies provided technical edits, which we incorporated as appropriate. In addition, we received written comments from CFPB, which are reprinted in appendix II.

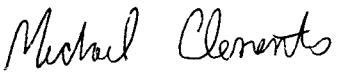
CFPB neither agreed nor disagreed with our recommendations. Regarding our recommendation that it identify additional sources of information that would help ensure that it is tracking all CRAs that meet the larger market participant threshold, CFPB noted that it cannot require CRAs to register with the bureau without first undertaking a rulemaking. While we acknowledge the challenges of tracking larger participant CRAs, we maintain that CFPB should be able to identify and monitor them consistently. In its letter, CFPB stated that this may be feasible. The agency noted that, short of rulemaking, there may be cost-effective ways to better ensure that it is appropriately tracking larger participant CRAs and added that they intend to track these CRAs by exploring ways to leverage state registration information. These actions, if fully implemented, would meet the intent of our recommendation.

With respect to the recommendation that CFPB assess whether its process for prioritizing CRA examinations sufficiently incorporates data security risks, CFPB said it will continue to evaluate risks to consumers, including data security risks, as part of its prioritization process. CFPB also said it will assess whether that process should incorporate data security risks CRAs pose to consumers. However, CFPB expressed concern with the scope of its statutory authority, such as its lack of authority to supervise for compliance with GLBA safeguard provisions.

CFPB noted that we did not adequately consider or discuss its limited statutory authority in the area of data security. Specifically, CFPB stated that it does not have authority to supervise for, enforce compliance with, or write regulations implementing GLBA's safeguards provisions or FCRA's records disposal provision. In response, we added language in the report to clarify CFPB's lack of certain authorities over these data security provisions. Nonetheless, as we discuss in the report, CFPB has conducted data security examinations of some CRAs under its existing authority, including its authority to assess compliance with the requirements of federal consumer financial law. We continue to believe that effective supervision of CRAs and the protection of consumer information require that CFPB consider data security risks in its prioritization of CRA examinations.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, CFPB, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FTC, and the Office of the Comptroller of the Currency. 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 Michael Clements at (202) 512-8678 or clementsm@gao.gov, or Nick Marinos at (202) 512-9342 or marinosn@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 major contributions to this report are listed in appendix III.



Michael Clements
Director, Financial Markets and Community Investment

Nick Marinos
Director, Information Technology and Cybersecurity

# Appendix I: Objectives, Scope, and Methodology

Our objectives were to examine (1) the federal laws and regulations governing consumer reporting agencies' (CRA) collection, use, and protection of consumer information; (2) measures the Federal Trade Commission (FTC) has taken to enforce CRA compliance with requirements to protect consumer information; (3) measures the Consumer Financial Protection Bureau(CFPB) has taken to ensure that CRAs protect consumer information; and (4) FTC's and CFPB's roles in assisting consumers following a data breach and actions consumers can take following a data breach of a CRA.[1]

To examine the laws governing CRAs, we identified the relevant laws, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and statutes related to unfair or deceptive acts or practices. We reviewed these laws for their application to CRAs and their collection, use, and protection of consumer information. We interviewed representatives of relevant federal agencies, including CFPB and FTC, about these laws and regulations and how they apply to CRAs. We also reviewed documents from and interviewed federal banking regulators on their role in overseeing financial institutions' management of third-party risk, including those of CRAs. We selected four states with existing or proposed information protection laws or regulations that vary from federal requirements (California, Illinois, Massachusetts, and New York); reviewed related documentation; and interviewed Attorneys General from these states about their enforcement of state laws. In addition, we interviewed and reviewed documentation from the three nationwide CRAs and interviewed three other CRAs that produce or compile consumer reporting information. We selected these CRAs because they are not sector-specific and hold information on a broad segment of the population. We conducted a site visit to Equifax's Alpharetta, Georgia data center to learn more about steps the company takes to comply with relevant consumer protection laws. We also interviewed representatives of furnishers and users of CRA consumer information—the American Bankers Association, the Property Casualty Insurance Association of America, and the National Retail Federation—about their roles in the

[1]We were also requested to examine consumer options to address risks of harm from data breaches, and the impact of data breaches at CRAs on federal programs. In addition, section 308 of the Economic Growth, Regulatory Relief, and Consumer Protection Act requires us to further examine issues related to the oversight of CRAs. *See* Pub. L. No. 115-174, § 308, 132 Stat.1296, 1347 (2018). We currently have additional audit work underway to address these topics and plan to issue separate reports on the results of those audits.

collection, use, and protection of consumer data, and steps their members take to comply with relevant laws.

To assess FTC's and CFPB's measures to enforce information protection provisions and to ensure CRAs' proper collection, use, and protection of consumer information, we reviewed agency documentation and interviewed agency officials on their oversight activities. We reviewed the types of enforcement actions available to FTC and CFPB for violations of laws related to consumer reporting, as well as specific enforcement actions these agencies have brought against CRAs, data furnishers, and users of consumer reports. We also interviewed agency staff about FTC enforcement actions against CRAs and how it determines when to pursue such actions. We reviewed CFPB documentation on the scope of its supervisory examinations of larger market participant CRAs since 2015, as well as findings from recent CRA examinations. In addition, we reviewed CFPB examination guidance for supervising these CRAs, including CFPB's internal guidelines for conducting data security examinations. We also reviewed documents related to CFPB's process for prioritizing which institutions and which product lines (specific product offerings) should receive supervisory examination, and we interviewed CFPB staff about this process. Finally, we interviewed representatives of industry, consumer, and privacy groups for their views on the supervision of CRAs. These included the three nationwide CRAs, three other CRAs, the Consumer Data Industry Association, National Consumer Law Center, Consumer Federation of America, Consumers Union, World Privacy Forum, ID Theft Resource Center, and Consumer Action.

To assess FTC and CFPB roles in assisting consumers, and actions consumers can take following a data breach of a CRA, we reviewed the two agencies' efforts to inform and educate consumers following breaches. Specifically, we reviewed consumer education materials on FTC's and CFPB's websites related to data breaches and identify theft in general, as well as specific information posted after the Equifax data breach. We also interviewed staff from these agencies about their roles in assisting consumers following a breach. To identify actions consumers can take following a data breach, we reviewed our prior related reports

and spoke with representatives of the industry and consumer representatives noted above.[2]

We conducted this performance audit from November 2017 to February 2019 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.

[2]Prior GAO reports included GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, GAO-17-254 (Washington, D.C: Mar. 30, 2017) and GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: June 26, 2006).

# Appendix II: Comments from the Bureau of Consumer Financial Protection

Bureau of Consumer Financial Protection
1 700 G Street NW
Washington, D.C. 20552

January 22, 2019

Michael Clements
Director, Financial Markets and Community Investment
Government Accountability Office
441 G Street, NW
Washington DC, 20548

Dear Mr. Clements,

Thank you for the opportunity to review and comment on the draft report by the Government Accountability Office (GAO), titled *Consumer Data Protection: Activities Needed to Strengthen Oversight of Consumer Reporting Agencies* (19-196). The Bureau greatly appreciates GAO's work over the course of this engagement and believes the report provides the public important information regarding federal oversight of the protection of consumer information by consumer reporting agencies (CRAs) and actions consumers can take after a data breach.

Oversight of the credit reporting market has been a top priority at the Bureau because credit reporting plays a critical role in the overall consumer financial services market and has enormous reach and impact; over 200 million Americans have credit files with tradelines furnished voluntarily by over 10,000 providers. For any individual consumer, an accurate consumer report can be critically important, given the significant impact that information can have on the consumer's ability to obtain or pay for financial and other products and services. Despite the impact credit reports can have on a consumer, consumers do not get to choose who collects and sells consumer report information about them.

In both its supervision and enforcement work in connection with CRAs, the Bureau has, to date, focused the bulk of its oversight on assessing compliance with the accuracy, dispute investigation, and permissible purpose obligations outlined in the Fair Credit Reporting Act

consumerfinance.gov

(FCRA). Those were the areas that were both committed to the Bureau's jurisdiction and presented risk to consumers that could be assessed through the supervisory process.

Those reviews helped further FCRA compliance. As discussed in the March 2017 special edition of its *Supervisory Highlights*, as a result of the numerous supervisory reviews in this area, CRAs made specific improvements in data accuracy and dispute resolution, including: implementing quality control programs of compiled consumer reports; monitoring of furnisher dispute metrics to identify and correct root causes of inaccuracies; conducting reasonable reinvestigations of consumer disputes, including review of relevant information provided by consumers; and improving communication to consumers about dispute results. CRAs also enhanced their management and compliance programs to address FCRA requirements that consumer reports are issued and used for permissible purposes.

In addition to its supervisory work, the Bureau has brought actions and entered into settlements to enforce the FCRA's accuracy requirements, the statutory requirements regarding investigation of disputed information, and the permissible purpose requirements to obtain consumer reports.

The GAO's report discusses the FTC's and Bureau's respective authorities over CRAs as they relate to data security. Although the Bureau does have certain authorities in this regard, the report does not adequately consider or discuss the statutory authorities relating to data security Congress did not provide the Bureau. Critically, Congress specifically excluded important statutory provisions related to data security from the Bureau's purview. The Bureau does not have any authority to supervise for, enforce compliance with, or write regulations implementing the Gramm-Leach-Bliley Act's (GLBA) safeguards provision or the FCRA's records disposal provision.[1] The GLBA safeguards provision and the FTC's implementing rule require CRAs to develop, implement, and maintain comprehensive information security programs that contain administrative, technical, and physical safeguards. The FCRA records disposal provision and the FTC's implementing rule requires CRAs to take reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal.

[1] The Bureau also does not have any authority over the FCRA's red flags provision and the FTC's implementing rule requiring that certain entities implement written Identity Theft Prevention Programs designed to detect, prevent, and mitigate identity theft. The red flags provision remains under FTC's jurisdiction with respect to entities under its enforcement authority, but only applies to financial institutions and creditors (as defined in statute). *See* 15 U.S.C. §§ 1681m(e), 1681s(a)(1) and 1681w(a)(1) and 16 C.F.R. pts. 681 and 682.

Accordingly, the Bureau lacks authority to implement, supervise for, or enforce data security standards under these statutory provisions.

GAO makes two recommendations to the Bureau:

- The Director of the CFPB should identify additional sources of information, such as through registering CRAs or leveraging state information, that would help ensure the agency is tracking all CRAs that meet the larger participant threshold; and
- The Director of the CFPB should 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.

The Bureau does not object to the first recommendation. With respect to the first recommendation, the Bureau notes that it cannot require larger participant CRAs to register with the Bureau at this time. Registration would require a rulemaking and is not something that the Bureau has required of participants in other markets for which the Bureau issued a larger participant rule. To undertake such a rulemaking, the Bureau would need to consider the potential benefits and costs to consumers and covered persons.

As the report notes, the Bureau prioritizes its exams based on the entities and product lines that pose the greatest risk to consumers. To assess risks to consumers, the Bureau looks at a host of quantitative and qualitative information. Because an institution's size is a significant factor in the Bureau's risk analysis, the Bureau has focused its supervision of larger participants in the CRA market on the largest market participants, which are well known to the Bureau. Identifying potential additional larger participant CRAs may not materially alter any of the Bureau's prioritization decisions.

Nevertheless, the Bureau recognizes that there may be cost-effective ways short of a rulemaking to better ensure the Bureau is appropriately tracking larger participant CRAs. As the report notes, several states, such as New York and Maine, have begun requiring CRA registration. The Bureau is aware of these efforts and intends to explore ways of leveraging state registration information, recognizing that states may be requiring registration of all CRAs and not just those that meet the Bureau's larger participant threshold.

With respect to the second recommendation, the Bureau will continue to evaluate risks to consumers as part of its process to prioritize examinations and other supervisory work. As part of that evaluation, the Bureau will assess whether that process should incorporate data security risks CRAs pose to consumers in light of all of its supervisory responsibilities, including

consideration of other risks to consumers, available resources, and the scope of its statutory authority, such as the Bureau's lack of authority to supervise for compliance with GLBA safeguards provisions.

The Bureau looks forward to continuing to work with GAO on this important topic.

Sincerely,

Kathleen L. Kraninger
Director

# Appendix III: GAO Contacts and Staff Acknowledgments

## GAO Contacts

Michael Clements, (202) 512-8678, clementsm@gao.gov
Nick Marinos, (202) 512-9342, marinosn@gao.gov

## GAO Staff Acknowledgments:

In addition to the individuals named above, John de Ferrari and John Forrester (Assistant Directors); Winnie Tsen (Analyst-in-Charge), Bethany Benitez, Kavita Daitnarayan, Farrah Graham, Andrea Harvey, Thomas Johnson, Tovah Rom, Rachel Siegel, Jena Sinkfield, and Tina Torabi made key contributions to this report.