



August 2018

DATA PROTECTION

Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach

GAO Highlights

Highlights of [GAO-18-559](#), a report to congressional requesters.

Why GAO Did This Study

CRA's such as Equifax assemble information about consumers to produce credit reports and may provide other services, such as identity verification to federal agencies and other organizations. Data breaches at Equifax and other large organizations have highlighted the need to better protect sensitive personal information.

GAO was asked to report on the major breach that occurred at Equifax in 2017. This report (1) summarizes the events regarding the breach and the steps taken by Equifax to assess, respond to, and recover from the incident and (2) describes actions by federal agencies to respond to the breach. To do so, GAO reviewed documents from Equifax and its cybersecurity consultant related to the breach and visited the Equifax data center in Alpharetta, Georgia, to interview officials and observe physical security measures. GAO also reviewed relevant public statements filed by Equifax. Further, GAO analyzed documents from the IRS, SSA, and USPS, which are Equifax's largest federal customers for identity-proofing services, and interviewed federal officials related to their oversight activities and response to the breach.

What GAO Recommends

GAO is not making recommendations in this report. GAO plans to issue separate reports on federal oversight of CRA's and consumer rights regarding the protection of personally identifiable information collected by such entities. A number of federal agencies and Equifax provided technical comments which we incorporated as appropriate.

View [GAO-18-559](#). For more information, contact Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, or Michael Clements at (202) 512-8678 or ClementsM@gao.gov.

August 2018

DATA PROTECTION

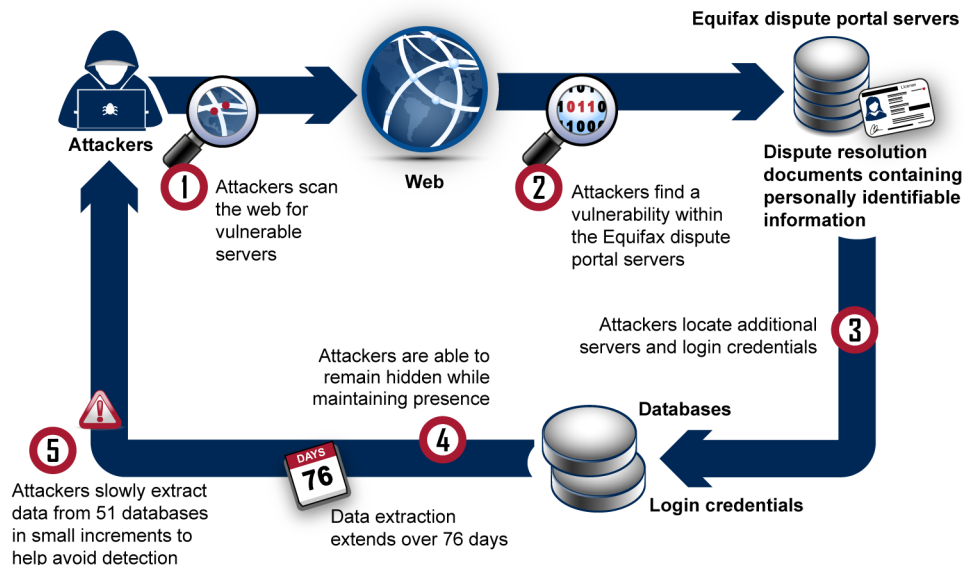
Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach

What GAO Found

In July 2017, Equifax system administrators discovered that attackers had gained unauthorized access via the Internet to the online dispute portal that maintained documents used to resolve consumer disputes (see fig.). The Equifax breach resulted in the attackers accessing personal information of at least 145.5 million individuals. Equifax's investigation of the breach identified four major factors including identification, detection, segmenting of access to databases, and data governance that allowed the attacker to successfully gain access to its network and extract information from databases containing personally identifiable information. Equifax reported that it took steps to mitigate these factors and attempted to identify and notify individuals whose information was accessed. The company's public filings since the breach occurred reiterate that the company took steps to improve security and notify affected individuals.

The Internal Revenue Service (IRS), Social Security Administration (SSA), and U.S. Postal Service (USPS)—three of the major federal customer agencies that use Equifax's identity verification services—conducted assessments of the company's security controls, which identified a number of lower-level technical concerns that Equifax was directed to address. The agencies also made adjustments to their contracts with Equifax, such as modifying notification requirements for future data breaches. In the case of IRS, one of its contracts with Equifax was terminated. The Department of Homeland Security offered assistance in responding to the breach; however, Equifax reportedly declined the assistance because it had already retained professional services from an external cybersecurity consultant. In addition, the Bureau of Consumer Financial Protection and the Federal Trade Commission, which have regulatory and enforcement authority over consumer reporting agencies (CRA's) such as Equifax, initiated an investigation into the breach and Equifax's response in September 2017. The investigation is ongoing.

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information



Source: GAO, based on information provided by Equifax. | GAO-18-559

Contents

| | | |
|--------------|---|----|
| Letter | | 1 |
| | Background | 2 |
| | Attackers Exploited Vulnerabilities That Equifax Subsequently Reported Taking Actions to Address | 10 |
| | Federal Agencies Took a Variety of Actions in Response to the Equifax Breach | 21 |
| | Agency Comments and Third-Party Views | 27 |
| Appendix I | Objectives, Scope, and Methodology | 30 |
| Appendix II | Comments from the Social Security Administration | 33 |
| Appendix III | Comments from the United States Postal Service | 34 |
| Appendix IV | GAO Contacts and Staff Acknowledgments | 35 |
| Figure | | |
| | Figure 1: Analysis of How Attackers Exploited Vulnerabilities | 13 |

Abbreviations

| | |
|------|--|
| BCFP | Bureau of Consumer Financial Protection |
| CMS | Centers for Medicare and Medicaid Services |
| CRA | consumer reporting agencies |
| DHS | Department of Homeland Security |
| FTC | Federal Trade Commission |
| IRS | Internal Revenue Service |
| PII | personally identifiable information |
| SSA | Social Security Administration |
| USPS | United States Postal Service |

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



August 30, 2018

Congressional Requesters

Recent data breaches at federal agencies, retailers, hospitals, insurance companies, consumer reporting agencies (CRA), and other large organizations have resulted in the potential compromise of millions of Americans' personally identifiable information (PII), which could lead to identity theft and other serious consequences. Such incidents highlight the importance of ensuring the security and privacy of PII collected and maintained by those entities.¹

As one example, the breach of an Equifax online dispute portal from May to July 2017 resulted in the compromise of records containing the PII of at least 145.5 million consumers in the U.S. and nearly 1 million consumers outside of the U.S. Among others, the customers of Equifax's services include federal agencies, such as the Internal Revenue Service (IRS); Social Security Administration (SSA); and U.S. Postal Service (USPS). In addition, the Bureau of Consumer Financial Protection (BCFP)² and Federal Trade Commission (FTC) have roles in providing oversight of Equifax and other CRAs.

You requested that we review aspects of the 2017 Equifax breach and the federal response. Our specific objectives were to (1) summarize the events regarding the 2017 Equifax breach and the steps taken by the company to assess, respond to, and recover from the incident and (2) describe the actions that federal customers and oversight agencies took in response to the breach.³

¹Companies that assemble consumer credit information and sell this information are referred to as "consumer reporting agencies" by the law governing credit reports. See 15 U.S.C. § 1681a(f). These companies can also be referred to as a "credit bureau," "credit reporting company," or a "credit reporting agency." Equifax, Experian, and TransUnion Corporation are the nation's largest consumer reporting agencies.

²The Bureau of Consumer Financial Protection was formerly known as the Consumer Financial Protection Bureau (CFPB). The name change effort began in March 2018 and continues to be phased in.

³We were also requested to examine federal oversight of CRAs and consumer rights regarding the protection of PII collected by CRAs, and the impact of data breaches at CRAs on federal programs. We currently have additional audit work underway to address these topics and plan to issue separate reports on the results of those audits.

To address the first objective, we analyzed documentation generated by Equifax and its cybersecurity consultant in response to the breach, such as the report summarizing the results of the consultant's forensic analysis of Equifax systems. In addition, we conducted a site visit at the Equifax data center in Alpharetta, Georgia, where we interviewed relevant company officials and observed the organization's physical security measures. We did not independently verify or assess Equifax's security controls or the steps the company took to address factors related to the breach. We also reviewed Equifax's relevant public filings it provided to the public and shareholders, which included information about the data breach and the company's efforts for remediation.

For the second objective, we analyzed documentation that described key actions taken by federal customers and oversight agencies following the breach. This included documentation that discussed the responses to the breach by IRS, SSA, and USPS, as key federal customers of Equifax. In addition, we analyzed documentation related to the oversight of Equifax (and other CRAs) by BCFP and FTC. We also conducted interviews with officials of these selected customer and oversight agencies to further understand the actions they took. Appendix I discusses our objectives, scope, and methodology in greater detail.

We conducted this performance audit from November 2017 to August 2018 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

A consumer reporting agency is a person or entity that assembles or evaluates consumer credit information or other consumer information for the purpose of furnishing consumer reports to others. This includes companies that compile and store electronic files of consumer information, which they then sell to other businesses and organizations that use the information to assess or evaluate creditworthiness.

Furnishing of information by creditors and others to CRAs is voluntary, as federal law generally does not require such reporting, and information compiled on individual consumers can vary among the CRAs. A lender uses the information provided to determine whether to offer credit to an individual, the rate of interest to be assigned to the loan, and other terms

of the contract. In addition, a growing number of entities use information provided by CRAs to help make decisions about individuals' credit worthiness when determining eligibility for insurance, housing, or employment, among other things. Information from CRAs can also be used for other purposes, such as to identify potential customers with specific characteristics for new credit card accounts.

CRAs may provide a variety of verification services to government and private sector organizations. For example, Equifax provides income and employment verification services using information collected from employers.

Equifax, TransUnion, and Experian—the three major CRAs—also leverage information they collect from organizations, such as financial institutions, utilities, cell phone service providers, public records, and government sources, to offer identity verification services. Other entities, including federal agencies, use identity verification when they enroll new applicants for benefits and services. In addition, the IRS uses identity verification to ensure that individuals who want to access prior year tax returns are the legitimate filers of those returns.

With regard to identity verification, CRAs typically use information they collect to generate questions that federal agencies and other entities can use to test applicants' knowledge of information in their credit file. These questions and answers are typically the basis for identity proofing—the process of comparing evidence from an individual with a trusted source of data to verify that the individual is who they claim to be. The evidence generally consists of information or documentation that only the legitimate individual should know or have access to. For example, a driver's license, passport, knowledge of recent financial transactions, and biometric information are all considered relatively strong evidence that the individual is who they say they are.

A Data Breach Can Have Harmful Results

Although there is no commonly agreed-upon definition, the term “data breach” generally refers to an unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information. This information can include PII, such as Social Security numbers, or financial information, such as credit card numbers.

A data breach can occur under many circumstances and for many reasons. It 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 a malicious individual or group, agency insiders, foreign nation, terrorist, or other adversary. Data breaches have occurred at all types of organizations, including private, nonprofit, and federal and state entities.

The loss or unauthorized disclosure of information in a data breach can lead to serious consequences and can result in substantial harm to individuals, private sector organizations, and the federal government. Examples of harmful results include:

- loss or theft of resources, including money and intellectual property, and identity theft;
- inappropriate access to and disclosure, modification, or destruction of sensitive information;
- harm to national security;
- use of computer services for unauthorized purposes or to launch an attack on other computer systems;
- damage to networks and equipment;
- loss of privacy, emotional distress, or reputational harm;
- loss of public confidence; and
- high costs to remediate the effects of the breach.

Attackers Use a Variety of Tools and Techniques

Cyber criminals seeking access to sensitive information, such as PII, typically use a variety of readily available software tools to carry out attacks. These tools can be used to intercept and capture data as they are transmitted, exploit known vulnerabilities⁴ in commercially available software, and facilitate e-mail phishing techniques for gaining unauthorized access to systems and information.

Attackers often use similar techniques and tools, making it difficult to distinguish one attacker from another. When custom-built tools are used, an attacker may rely on unique methods or display other telltale signs that can be used for identification; such tools are usually used when a target's defenses justify them. Off-the-shelf tools are usually enough to conduct a

⁴A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by an attacker.

successful attack that allows an attacker to steal data, bring systems down, or gain further access to systems and resources.

Attackers often begin with network-scanning programs, which are used to map the layout of a targeted network and determine the location of data repositories that may contain information of interest.⁵ Some scanners are designed to scan only a single networked computer, extracting as much data about that system as possible. Others can scan Internet addresses across the web to identify potential targets by determining whether they are using a version of software that is vulnerable to an attack.

Once a target has been identified, the attacker will generally attempt to gain access to the system or network without leaving any indication of who they are or from where they launched their attack. This is commonly accomplished using tools that mask the attacker's origin by using the Internet address of another computer from another location. While an investigator can sometimes use forensic tools to trace the original Internet address, often this leads to misleading information.

Attackers use additional tools and techniques to gain unauthorized access to systems and data on the target network and to transfer stolen data back to the attacker's own computer system. One such technique is to leverage the access rights gained on the originally compromised system to get further access into other servers on the network. To do this, an attacker can use standard, off-the-shelf tools for navigating systems and managing information that blend in with normal network activity. For example, encryption can be used to hide the transfer of sensitive information from one server to another or out of the network entirely. This enables the attacker to continue probing for more repositories of information and stealing copies of that information without being detected by the targeted network's system administrators.

⁵A scanner is a program that can identify active networked computers that are currently receiving and sending computer network communication to gain reconnaissance data about the type of operating system a computer is running (as well as the version), open system services (e-mail, servers, etc.), and a host of other data, depending on the capabilities of the scanning program.

Federal Agencies Oversee CRA Activities, Including Protection of Personally Identifiable Information

CRAs have been subject to federal regulation since the passage of the *Fair Credit Reporting Act* in 1970.⁶ Currently, FTC and BCFP are the two federal agencies with primary oversight responsibilities for CRAs. FTC was given responsibility for administratively enforcing CRAs' compliance with the *Fair Credit Reporting Act* at the time of enactment.⁷ As part of the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Dodd-Frank Act), BCFP was given authority to enforce a number of federal consumer financial laws, including the *Fair Credit Reporting Act*. BCFP also has begun exercising supervisory authority over certain larger participants in the credit reporting market.

FTC Has Enforcement Authority over CRAs

FTC has authority, subject to certain exceptions, to investigate any organization that maintains consumer data and to bring enforcement actions for violations of laws that concern the protection of consumer information.⁸ FTC also exercises enforcement authority over CRAs through the *Gramm-Leach-Bliley Act* and the related "Safeguards" and "Privacy Rules."⁹

- *The Fair Credit Reporting Act* promotes the accuracy, fairness, and privacy of information collected or used to help make decisions about individuals' eligibility for credit, insurance, employment, housing, or other benefits. CRAs that compile credit histories and other personal information into consumer reports must adhere to the act's provisions for ensuring the accuracy and permissible uses of such information.
- *The Gramm-Leach-Bliley Act* requires that federal financial regulators and FTC establish standards and protections to ensure the security

⁶Pub. L. No. 91-508, tit. VI, § 601, 84 Stat. 1114, 1127 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

⁷See 15 U.S.C. § 1681s(a). Federal agencies and the states have authority to bring injunctive actions under the *Fair Credit Reporting Act*, as well as actions for damages for violations of certain provisions. Under the *Fair Credit Reporting Act*, as amended by the *Fair and Accurate Credit Transactions Act*, there are also private rights of action. See 15 U.S.C. §§ 1681n, 1681o, 1681s-2(c). In addition, federally supervised banks that use consumer reports or furnish consumer report information are subject to enforcement by their respective federal banking regulators. See 15 U.S.C. §1681s.

⁸Certain entities, such as banks, credit unions, common carriers, and non-profit organizations, are excluded from FTC's authority under the *Federal Trade Commission Act*. See 15 U.S.C. § 45(a)(2).

⁹16 C.F.R. § 314.3. FTC's "Safeguards Rule" implements the *Gramm-Leach-Bliley Act*'s requirements for entities that fall under FTC jurisdiction, including check-cashing businesses, payday lenders, and mortgage brokers.

and confidentiality of customer information.¹⁰ These standards and protections must be implemented by companies of all sizes that are engaged in financial activities, including Equifax and all other CRAs. Further, the act requires financial institutions to protect the security of customers' personal information.

As part of its implementation of the *Gramm-Leach-Bliley Act*, FTC issued the "Safeguards Rule", which requires financial institutions develop, implement, and maintain a comprehensive information security program to keep information about a customer of a financial institution secure and confidential. In addition to developing their own safeguards, companies covered by the rule are responsible for requiring their affiliates and service providers to implement and maintain safeguards to protect customer information in their care.¹¹

In determining whether it should take enforcement action against a company for a violation of data security provisions, FTC considers a number of factors, including whether a company's data security measures are commensurate with the company's size. FTC does not have supervisory authority to examine CRAs for compliance with the *Federal Trade Commission Act*; therefore, the agency typically must rely on its enforcement authority after an incident has occurred.

Finally, FTC enforces Section 5 of the *Federal Trade Commission Act*, which prohibits "unfair or deceptive acts or practices in or affecting commerce."¹² FTC officials told us that failing to properly protect consumer data can be considered an unfair or deceptive act or practice.

BCFP Has Enforcement and Supervisory Authorities over CRAs

In 2010, the *Dodd-Frank Act* gave BCFP enforcement authority over all CRAs and certain other persons for violations of most provisions of the *Fair Credit Reporting Act*; certain provisions of the *Gramm-Leach-Bliley Act*; and for unfair, deceptive, or abusive acts or practices under sections

¹⁰Under the *Gramm-Leach-Bliley Act*, regulators must establish appropriate standards for financial institutions relating to administrative, technical, and physical safeguards 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 information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. Pub. L. No. 106-102, tit. V, § 501(b), 113 Stat. 1338, 1436 (1999) (codified as amended at 15 U.S.C. § 6801(b)).

¹¹16 C.F.R. § 314.4(d)(2).

¹²15 U.S.C. § 45.

1031 and 1036 of the *Dodd-Frank Act*.¹³ BCFP has taken enforcement actions against CRAs for violations of the *Fair Credit Reporting Act* and for deceptive practices.

In 2012, BCFP also extended its supervisory authority to include larger CRAs—that is, those with more than \$7 million in annual receipts from consumer reporting activities.¹⁴ BCFP staff review certain of these larger CRAs on an ongoing basis, and BCFP staff said that their recent examinations of CRAs have focused on compliance with *Fair Credit Reporting Act* requirements related to accuracy and resolving consumer disputes. BCFP has also examined CRAs subject to the BCFP’s supervisory authority for compliance with other *Fair Credit Reporting Act* requirements, including those related to ensuring the accuracy of information in consumer reports, furnishing information only to those with a permissible purpose, and compliance with the consumer dispute process.¹⁵

¹³For the *Fair Credit Reporting Act*, see Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x). For the relevant sections of the *Gramm-Leach-Bliley Act*, see Pub. L. No. 106-102, §§ 502-509, 113 Stat. 1338, 1437-1443 (1999) (codified as amended at 15 U.S.C. §§ 6802-6809). For the *Dodd-Frank Act*, see Pub. L. No. 111-203, §§ 1031, 1036, 124 Stat 1376, 2005, 2010 (2010) (codified at 12 U.S.C. §§ 5531, 5536).

¹⁴The *Dodd-Frank Act* gave BCFP authority to supervise nonbank “larger participant[s]” of markets for consumer financial products or services, as BCFP defines by rule. See § 1024(a)(1)(B), 124 Stat. at 1987 (codified at 12 U.S.C. § 5514(a)(1)(B)). Under BCFP’s 2012 rule, an entity with more than \$7 million in annual receipts resulting from relevant consumer reporting activities qualifies as a larger participant of the consumer reporting market subject to BCFP’s supervisory authority under 12 U.S.C. § 5514. See “Defining Larger Participants of the Consumer Reporting Market”, 77 Fed. Reg. 42874 (July 20, 2012). For the purposes of calculating “annual receipts,” the term “receipts” means “total income” plus “cost of goods sold” as these terms are defined and reported on IRS tax return forms. 12 C.F.R. § 1090.104(a). The term does not include net capital gains or losses. Annual receipts are measured as the average of a CRA’s most recently completed three fiscal years, or the average receipts for the entire period the person has been in business if it has less than three completed fiscal years. 77 Fed. Reg. at 42883.

¹⁵The *Fair Credit Reporting Act* promotes the accuracy, fairness, and privacy of information collected or used to help make decisions about individuals’ eligibility for credit, insurance, or employment, and applies to CRAs that compile credit histories and other personal information into consumer reports. Accordingly, the act applies to CRAs, including the three nationwide CRAs, and to any other entity that resells consumer reports, among other persons. See 15 U.S.C. §§ 1681-1681a. In addition to examining certain CRA’s compliance with federal consumer financial laws, including the *Fair Credit Reporting Act*, BCFP has also requested information about CRAs’ compliance management systems pursuant to Section 1024(b)(1)(B) of the *Dodd-Frank Act*.

BCFP also has supervisory authority over some aspects of the *Gramm-Leach-Bliley Act*. For example, BCFP examines larger CRAs for whether they restrict the sharing and disclosure of nonpublic personal information to third parties. BCFP does not have supervisory or enforcement authority over the “Safeguards Rule” enacted by FTC as part of the agency’s implementation of the *Gramm-Leach-Bliley Act*.

Finally, BCFP has authority to examine larger CRAs for any unfair, deceptive, or abusive acts or practices and to bring enforcement actions against CRAs of all sizes for such acts or practices. According to BCFP staff, in some cases, a CRA could commit an unfair, deceptive, or abusive act or practice or violation of other applicable law in connection with its data security practices.

GAO Has Previously Reported on Data Protection Issues

We have previously made recommendations to agencies regarding the protection of PII, and proposed Matters for Congressional Consideration in areas where laws could be enhanced. For example, in our recent report on data oversight at the Centers for Medicare and Medicaid Services (CMS),¹⁶ we recommended that the agency ensure that all third parties¹⁷ that receive CMS data have clear requirements for the protection of that data, that CMS properly oversee the implementation of those requirements, and that the agency ensure identified issues are remediated. Additionally, our recent report on the oversight of students’ PII at the Department of Education included seven recommendations for better protection of student PII and for improving department policies to meet federal privacy guidelines.¹⁸ All of these recommendations currently remain open while the agencies take actions to address them.

In addition to recommendations for agencies, we have proposed two Matters for Congressional Consideration related to data protection. In 2008, we reported that the *Privacy Act*¹⁹ and *E-Government Act of 2002*²⁰

¹⁶GAO, *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*, [GAO-18-210](#) (Washington, D.C.: Mar. 6, 2018).

¹⁷CMS shares Medicare beneficiary data with external entities primarily for processing Medicare claims, supporting medical research, and evaluating the performance of Medicare service and equipment providers.

¹⁸GAO, *Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information* [Reissued on December 15, 2017], [GAO-18-121](#) (Washington, D.C.: Nov. 27, 2017).

¹⁹Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

may not adequately ensure that consumers are notified in the event of a breach by federal agencies and that existing laws could better ensure that consumers are aware of what PII federal agencies collect and how they use it.²¹ Based on this finding, we suggested that Congress consider amending applicable laws to ensure that all PII collected by federal agencies is protected and that its use is limited to the stated purpose of the collection.

With regard to data collected by private entities, in 2013, we reported that existing federal laws provide consumers with only limited protection for data that is collected and used for marketing purposes.²² Consequently, we asked Congress to consider strengthening the current consumer privacy framework to reflect the effects of changes in technology and the marketplace while also ensuring that any limitations on data collection and sharing do not unduly inhibit the economic and other benefits to industry and consumers that data sharing can accord.

Attackers Exploited Vulnerabilities That Equifax Subsequently Reported Taking Actions to Address

In March 2017, unidentified individuals discovered the presence of a known vulnerability in software running on Equifax's online dispute portal that could be used to obtain access to the system. In May of that year, attackers exploited the vulnerability and began to extract data containing PII from Equifax's information systems. According to Equifax, the attackers used a number of techniques to disguise their exploit of the Equifax systems and the database queries they conducted. On July 29, 2017, Equifax discovered the breach and reported that it took actions to address the factors that allowed the attackers to successfully gain access to its network. Further, the company reported that it took steps to identify, notify, and provide support to individuals who were potentially impacted by the breach.

²⁰Pub. L. No. 107-347, 116 Stat. 2899.

²¹GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, [GAO-08-536](#) (Washington, D.C.: May 19, 2008).

²²GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, [GAO-13-663](#) (Washington, D.C.: Sept. 25, 2013).

Attackers Identified and Exploited Vulnerabilities to Steal Data

Equifax has stated that, on March 10, 2017, unidentified individuals scanned the company's systems to determine if the systems were susceptible to a specific vulnerability that the United States Computer Emergency Readiness Team²³ had publicly identified just 2 days earlier. The vulnerability involved the Apache Struts Web Framework and would allow an attacker to execute commands on affected systems.²⁴

Equifax officials stated that, as a result of this scanning, the unidentified individuals discovered a server housing Equifax's online dispute portal²⁵ that was running a version of the software that contained the vulnerability. Using software they obtained from an unknown source and that was designed to exploit the vulnerability, the unidentified individuals subsequently gained unauthorized access to the Equifax portal and confirmed that they could run commands. No data was taken at this time.

According to Equifax officials, beginning on May 13, 2017, in a separate incident following the initial unauthorized access, attackers gained access to the online dispute portal and used a number of techniques to disguise their activity. For example, the attackers leveraged existing encrypted communication channels connected to the online dispute portal to send queries and commands to other systems and to retrieve the PII residing on the systems. The use of encryption allowed the attackers to blend in their malicious actions with regular activity on the Equifax network and, thus, secretly maintain a presence on that network as they launched further attacks without being detected by Equifax's scanning software.

Equifax officials added that, after gaining the ability to issue system-level commands on the online dispute portal that was originally compromised, the attackers issued queries to other databases to search for sensitive data. This search led to a data repository containing PII, as well as unencrypted usernames and passwords that could provide the attackers access to several other Equifax databases. According to Equifax's interim Chief Security Officer, the attackers were able to leverage these

²³The United States Computer Emergency Readiness Team is an organization within the Department of Homeland Security's National Protection and Programs Directorate. It is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

²⁴The Apache Struts Web Framework is a commonly-used, open-source software suite for developing web applications.

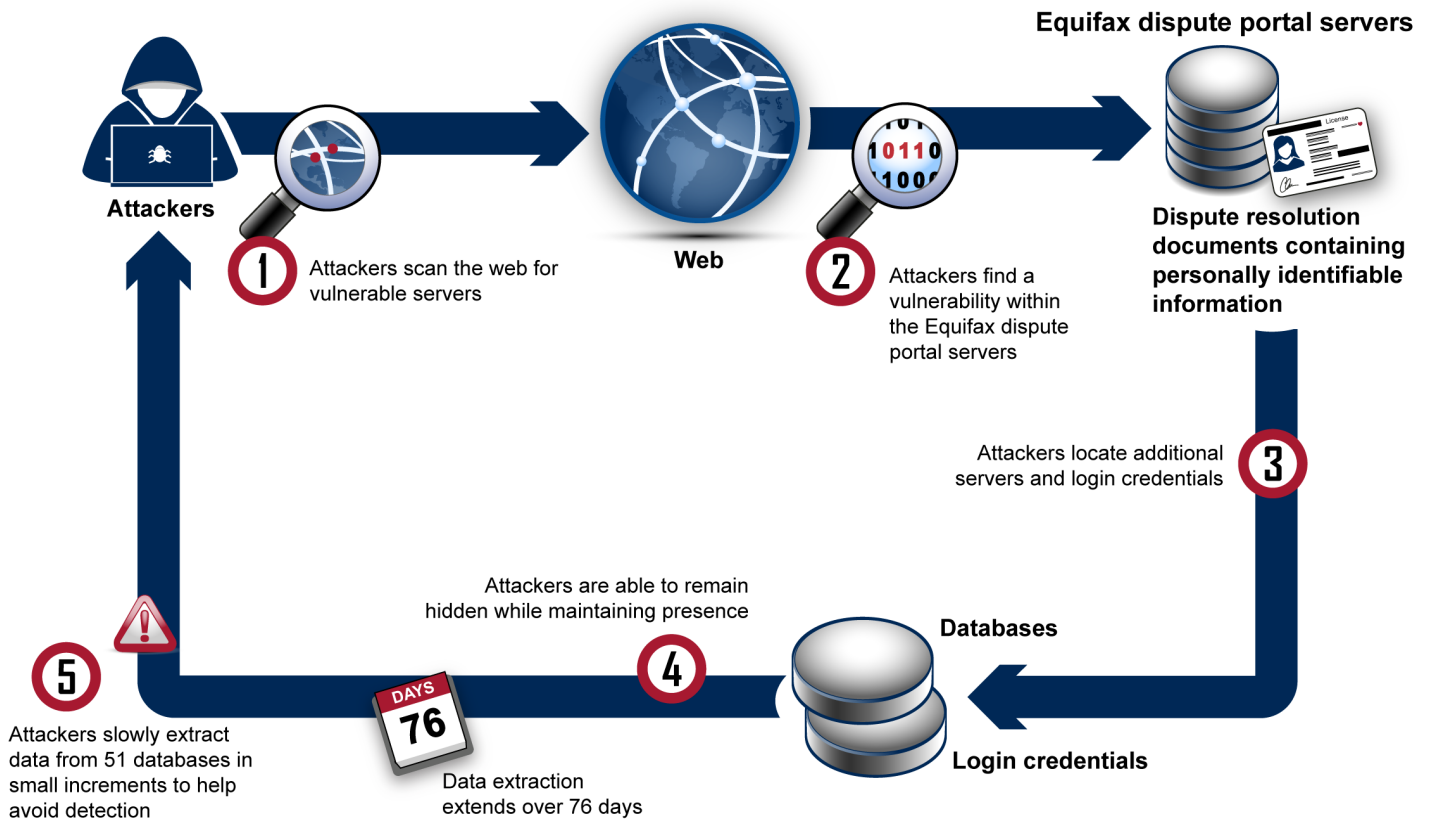
²⁵Equifax's online dispute portal is a web-based application that allows an individual to upload documents to research and dispute an inaccuracy in their Equifax credit report.

credentials to expand their access beyond the 3 databases associated with the online dispute portal, to include an additional 48 unrelated databases.

After reviewing system log files that recorded the attackers' actions, Equifax officials determined that the attackers then ran a series of queries in an effort to try to extract PII from the databases they had located. Altogether, the attackers ran approximately 9,000 queries, a portion of which successfully returned data containing PII. As before, Equifax officials stated that the attackers were able to disguise their presence by blending in with regular activity on the network.

After successfully extracting PII from Equifax databases, the attackers removed the data in small increments, using standard encrypted web protocols to disguise the exchanges as normal network traffic. The attack lasted for about 76 days before it was discovered. Figure 1 depicts an analysis of how the attackers gained access into Equifax's systems and exploited vulnerabilities.

Figure 1: Analysis of How Attackers Exploited Vulnerabilities



Source: GAO, based on information provided by Equifax. | GAO-18-559

After Becoming Aware of the Attack, Equifax Took Steps to Block the Attackers

Equifax’s assessment of the data breach began with actions it took to identify that it was being attacked as well as subsequent actions to block the intrusion. Equifax officials stated that, on July 29, 2017—approximately 2.5 months after the attackers began extracting sensitive information on May 13, 2017—security personnel conducting routine checks of the operating status and configuration of IT systems detected the intrusion on the online dispute portal.

As reported by Equifax, a network administrator conducting routine checks of the operating status and configuration of IT systems discovered that a misconfigured piece of equipment allowed attackers to communicate with compromised servers and steal data without detection. Specifically, while Equifax had installed a device to inspect network traffic

for evidence of malicious activity, a misconfiguration allowed encrypted traffic to pass through the network without being inspected. According to Equifax officials, the misconfiguration was due to an expired digital certificate.²⁶ The certificate had expired about 10 months before the breach occurred, meaning that encrypted traffic was not being inspected throughout that period. As a result, during that period, the attacker was able to run commands and remove stolen data over an encrypted connection without detection.

Equifax officials stated that, after the misconfiguration was corrected by updating the expired digital certificate and the inspection of network traffic had restarted, the administrator recognized signs of an intrusion, such as system commands being executed in ways that were not part of normal operations. Equifax then blocked several Internet addresses from which the requests were being executed to try to stop the attack.

Equifax reported that, on July 30, 2017, after its information security department observed additional suspicious activity continuing to occur, the online dispute portal was taken offline. The next day, the Chief Security Officer, in coordination with internal stakeholders, informed the Chief Executive Officer of the attack on the portal.

Equifax Identified Several Factors That the Attacker Exploited During the Breach

To further assess the scope of the breach and identify its causes, Equifax began an investigation to identify the vulnerabilities that had been exploited to steal PII from its systems. Concurrent with this effort, company officials stated that they also began examining the data repositories that had been accessed to try to determine how much data had been taken and how many individuals were potentially impacted. According to Equifax officials, the investigation took place between August 2 and October 2, 2017, with the help of an external cybersecurity consultant.

Equifax officials stated that the company's investigation was facilitated by the use of electronic logs that had not been damaged or erased by the

²⁶Equifax stated that the misconfiguration was the result of an expired digital certificate that had not been replaced with a new certificate. Digital certificates are encrypted electronic tokens that are used to authenticate servers and systems. Because this one was expired, the system was unable to inspect encrypted traffic. The network administrator replaced the expired certificate, allowing the system to resume inspection of traffic.

attackers on the affected systems. These logs recorded commands that were issued by the attackers throughout the attack, such as commands to retrieve or display the contents of data repositories. By examining the logs, Equifax worked to reconstruct the sequence of specific actions that the attackers had taken and, consequently, determine what specific data had been compromised. In addition to initiating its internal investigation, on August 2, 2017, the company notified the Federal Bureau of Investigation of the breach.

Based on its cybersecurity consultant's analysis and recommendations following the breach, Equifax determined that several major factors had facilitated the attackers' ability to successfully gain access to its network and extract information from databases containing PII. Specifically, Equifax officials told us that key factors that led to the breach were in the areas of identification, detection, segmentation²⁷, and data governance:

- **Identification.** According to Equifax officials, the Apache Struts vulnerability was not properly identified as being present on the online dispute portal when patches for the vulnerability were being installed throughout the company. After receiving a notice of the vulnerability from the United States Computer Emergency Readiness Team in March 2017, Equifax officials stated that they circulated the notice among their systems administrators. However, the recipient list for the notice was out-of-date and, as a result, the notice was not received by the individuals who would have been responsible for installing the necessary patch. In addition, Equifax officials stated that although the company scanned the network a week after the Apache Struts vulnerability was identified, the scan did not detect the vulnerability on the online dispute portal.
- **Detection.** As reported by Equifax officials, an expired digital certificate contributed to the attackers' ability to communicate with compromised servers and steal data without detection. Specifically, while Equifax had installed a tool to inspect network traffic for evidence of malicious activity, the expired certificate prevented that tool from performing its intended function of detecting malicious traffic.

²⁷Segmentation allows an organization to logically separate applications based on their sensitivity level or to keep unrelated applications from communicating with each other. In addition to allowing organizations to group applications and similar data for access by a specific group, it also limits the access provided to those inside the organization and third-parties.

The certificate had expired before May 2017, meaning that traffic was not being inspected throughout the breach.

- **Segmentation.** Because individual databases were not isolated or “segmented” from each other, the attackers were able to access additional databases beyond the ones related to the online dispute portal, according to Equifax officials. The lack of segmentation allowed the attackers to gain access to additional databases containing PII, and, in addition to an expired certificate, allowed the attackers to successfully remove large amounts of PII without triggering an alarm.
- **Data Governance.** Data governance includes setting limits on access to sensitive information, including credentials such as usernames and passwords. According to Equifax officials, the attackers gained access to a database that contained unencrypted credentials for accessing additional databases, such as usernames and passwords. This enabled the intruders to run queries on those additional databases.

In addition to these four broad categories, Equifax officials noted one other factor that also facilitated the breach. Specifically, the lack of restrictions on the frequency of database queries allowed the attackers to execute approximately 9,000 such queries—many more than would be needed for normal operations.

Equifax Reported Taking Steps to Strengthen its Cybersecurity Controls

According to Equifax’s public filings, including its annual 10-K filing submitted to the Securities and Exchange Commission in March 2018 and its notice of 2018 annual meeting and proxy statement, following the 2017 incident, Equifax undertook a variety of remediation efforts to address the factors identified in their investigation.²⁸ Equifax officials responsible for coordinating the response to the incident stated that, once the company identified how the attackers were able to gain unauthorized access to company systems and remove sensitive data, it took measures to address the internal factors that led to the breach. The measures were intended to better protect the company’s infrastructure from future disruptions, compromises, or failures. We did not independently assess Equifax’s efforts to address the identified factors.

²⁸According to the Securities and Exchange Commission, federal securities laws require domestic companies to submit annual reports on Form 10-K that provide a comprehensive overview of the company’s business and financial condition and include audited financial statements.

Specifically, Equifax officials stated that system-level remediation measures were implemented to address the factors that led to the breach. For example, to work toward addressing concerns about identifying vulnerable servers, Equifax reportedly is implementing a new management process to identify and patch software vulnerabilities and confirm that vulnerabilities have been addressed. Also, to help ensure that detection of malicious activity is not hindered in the future, Equifax officials said they have developed new policies to protect data and applications and implemented new tools for continuous monitoring of network traffic. Further, in an effort to improve segmentation between devices that do not need to communicate, Equifax officials stated that they have implemented additional controls to monitor communications at the external boundary of the company's networks and added restrictions on traffic between internal servers. Finally, to help address data governance issues, the officials said they were implementing a new security controls framework and tighter controls for accessing specific systems, applications, and networks.

In addition to these measures, Equifax stated that they implemented a new endpoint security tool to detect misconfigurations, evaluate potential indications of compromise, and automatically notify system administrators of identified vulnerabilities. Further, Equifax officials reported that the company has implemented a new governance structure to regularly communicate risk awareness to Equifax's board of directors and senior management. The new structure requires the company's Chief Information Security Officer to report directly to the Chief Executive Officer.²⁹ Officials said this should allow for greater visibility of cybersecurity risks at top management levels.

²⁹Prior to the 2017 data breach, the Chief Information Officer reported to the Chief Executive Officer and the Chief Security Officer reported to the company's Chief Legal Officer. Following the breach, Equifax created the position of Chief Information Security Officer, who reports to the Chief Executive Officer.

Equifax Reported Taking Steps to Identify Affected Individuals

Following the shutdown of its online dispute portal, Equifax took steps to identify what data had been lost and the number of individuals affected so that it could fulfill its responsibility to notify affected individuals.³⁰ To develop its estimate of the number of individuals affected by the data breach, Equifax stated that it recreated the attackers' database queries on a separate system that could run the queries at high speed, allowing Equifax to generate its estimate in a relatively short period of time. Equifax staff then worked to reconstruct queries against the data tables to identify which queries had successfully extracted data and which individuals were associated with that data.

However, as is commonly experienced with large breaches, Equifax faced challenges in determining exactly how many individuals were affected. According to Equifax officials, much of the stolen data consisted of incomplete records without full sets of identifying information. Some data sets included information that could be matched to more than one known individual. Subsequently, Equifax officials stated that they compared these data sets with information in the company's internal databases that were not impacted by the data breach to make matches with known identities.

For example, Equifax took partial records that did not include all fields and ran an analysis to determine whether Social Security numbers and names included in the records could be matched with those in Equifax's core credit reporting databases. In addition, Equifax performed analyses to remove duplicates and to determine whether a person could be linked to incomplete records based on Social Security numbers. After Equifax completed its initial analysis of the datasets, it estimated that approximately 143 million U.S. consumers had been affected by the breach.

Moreover, Equifax's initial analysis, reported on September 7, 2017, indicated that multiple types of PII had been compromised, including individuals' names, Social Security numbers, birth dates, addresses, and driver's license numbers. Because many of the records were incomplete,

³⁰There is no comprehensive federal law that dictates an organization's responsibility to notify affected individuals in the event of a data breach. However, some state laws require the entity that has been impacted by a data breach to notify its customers and other relevant parties about the breach in a timely fashion. Such notification is intended to allow the affected individuals the opportunity to take steps to protect themselves from identity theft or other misuse of personal information that may have been compromised in the breach.

not all of the types of PII had been compromised for all affected individuals.

In addition, Equifax determined that credit card numbers for approximately 209,000 consumers and certain dispute documents, which had included PII for approximately 182,000 consumers, had been accessed. These documents contained PII associated with specific items from dispute cases that were submitted to Equifax as evidence supporting disputes they filed about the accuracy of their credit reports, such as utility bills.

Equifax made two revisions over time to its estimate of affected individuals. First, in late September 2017, Equifax determined that it had incorrectly concluded that one of the attackers' queries had not returned any data. After additional analysis, including a determination that the query had, in fact, allowed the attackers to access PII from approximately 2.5 million additional U.S. consumers, Equifax revised the number of affected individuals from 143 million to 145.5 million on October 2, 2017.

Second, 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. The newly identified individuals were based on names and partial driver's license information contained in a data table that Equifax had not previously identified as including individuals compromised in the breach. According to Equifax officials, Equifax's original investigation had not identified these individuals because their names and partial driver's license information were not stolen together with their Social Security numbers.

To identify as many potentially affected individuals as possible, Equifax contracted with a third-party data source that had access to a driver's license database and mapped the partial driver's licenses to an Equifax database containing Social Security numbers. According to Equifax officials, some of the individuals within this group of 2.4 million were already included in the previous total of 145.5 million affected individuals, while others were not. As of August 2018, Equifax had not determined

exactly how many of the 2.4 million individuals were included in the previous total of 145.5 million.³¹

Equifax Notified Affected Individuals and Offered Monitoring Services

On September 7, 2017, after Equifax had determined the extent of the breach and developed a remediation plan for potentially impacted consumers, the company provided written notification to all U.S. state attorneys general regarding the approximate number of potentially affected residents in each state and its plans for consumer remediation. The notification included steps individuals could take to determine if they were affected by the breach and to help protect against misuse of their personal information.³² The company also issued a press release to the public providing information about the breach and the types of PII that had been compromised.

Further, the press release issued on September 7, 2017, stated that the company had set up a dedicated website to help individuals determine if their information might have been stolen in the breach. In addition, Equifax improved the search tool it had developed to help U.S. consumers determine if they were impacted and expanded its call center operations. However, the website experienced several technical issues, including excessive downtime and inaccurate data. Equifax officials acknowledged these shortcomings and said they took measures to address them, including improving the stability of the website and accuracy of the information it provided.

Additionally, Equifax reported that it would provide several services to all U.S. consumers, regardless of whether their information had been compromised, free of charge for one year. Those services included credit monitoring, individual copies of Equifax credit reports, notification of changes to credit reports, a credit “lock” allowing individuals to prevent

³¹Equifax officials stated that they have substantially completed the process of reaching out to all 2.4 million identified individuals regardless of whether they previously had been identified.

³²In addition to notification requirements, some states have laws requiring breached entities to assist affected individuals in mitigating potential adverse effects, such as identity theft. For example, some states require organizations to offer credit monitoring services, which alert consumers when new accounts are opened using their personal information. In addition, federal laws require CRAs to provide individuals the ability to request fraud alerts, which require businesses to verify a consumer’s identity before issuing credit, and, effective September 21, 2018, credit “freezes,” which restrict potential creditors from accessing a consumer’s credit report.

third-parties from accessing their Equifax credit report,³³ identity theft insurance covering certain expenses related to the process of recovering from identity theft, and a Social Security number monitoring service that would scan suspicious websites for an individual's Social Security number.

These services were offered to consumers from September 7, 2017, until January 31, 2018, when Equifax announced a new service called "Lock & Alert." This new service allows consumers to use their smartphone or computer to lock and unlock their Equifax credit report. Equifax announced that it was making this service available to all consumers at no cost.

Federal Agencies Took a Variety of Actions in Response to the Equifax Breach

After Equifax announced the data breach, federal customer agencies took a variety of actions based on their responsibilities and how the breach affected their operations. Specifically, the agencies that were customers of the company's services conducted independent assessments of the company's security controls, revised their own identity proofing processes, and made changes to their contracts with Equifax, among other activities. Equifax did not ask the Department of Homeland Security (DHS), which is the central agency that responds to cyber incidents across the federal government, to assist in responding to the breach. Nevertheless, the department took the step of reminding federal agencies of the importance of correcting the software vulnerability that led to the breach. In addition, the oversight agencies, BCFP and FTC, began taking actions to investigate the breach and inform the public.

³³A credit "lock" is similar to a credit freeze, but is not subject to the same regulations. While provisions for a credit freeze varies by state, they generally allow consumers to request a freeze on their credit report by contacting CRAs and sometimes paying a fee, typically \$5–\$10, to each CRA. Consumers are given a unique personal identification number or password that they can use to temporarily lift the freeze when they are applying for credit or employment. For more information about fraud alerts, credit freezes, and credit monitoring, see GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, [GAO-17-254](#) (Washington, D.C.: Mar. 30, 2017).

Major Federal Customers of Equifax Took Steps to Ensure Their Activities Were Not Adversely Affected by the Breach

IRS, SSA, and USPS—large agencies that were major customers of Equifax at the time of the breach—assessed the potential impact of the breach to their own operations as well as to the operations of their consumers. For example, these agencies assessed the technical impact of the breach on their own systems that rely on Equifax services to determine whether the breach could have compromised the integrity of their identity proofing processes. While there was no breach of agency systems or information, they also sought to determine which of their customers were directly affected by the breach, recognizing that those individuals could be at heightened risk of identity fraud. Information security officials we spoke to at IRS, SSA, USPS, and DHS expressed concern about how the breached data could be used to compromise sensitive information or fraudulently procure government services, even from agencies that are not direct customers of Equifax.

Representatives of IRS, SSA, and USPS noted that they responded to the breach independently of other agencies, because they said it was unclear whether any single federal agency had responsibility for coordinating government actions in response to a breach of this type in the private sector. According to the three agencies, their actions included the following:

- **Identified affected individuals.** Due to concerns about the potential for fraud using the stolen data, IRS and SSA both obtained from Equifax a list of the individuals affected by the Equifax breach. The agencies then used these lists to identify which of their own customers were affected and to look for potential instances of identity fraud affecting those customers.
- **Performed independent assessments of Equifax security controls.** According to information security officials at IRS, SSA, and USPS, the agencies independently conducted site visits at Equifax's data center in Alpharetta, Georgia, where they reviewed the company's security controls. According to SSA officials, their agency's review assessed compliance with the baseline set of controls required by the National Institute of Standards and Technology for systems determined to pose a moderate level of risk.³⁴ SSA officials stated that they shared the results of their assessment with IRS, the Office of Management and Budget, House Ways and Means Social Security Subcommittee, and the Senate Committee on Finance. USPS officials

³⁴A system's security impact level is categorized as low, moderate, or high impact.

said they reviewed both physical security and cybersecurity controls at Equifax's data centers in Alpharetta, Georgia and St. Louis, Missouri locations. IRS officials said they also conducted a security assessment at Equifax's Alpharetta data center, as well as a separate review of physical security and cybersecurity controls at the company's St. Louis, Missouri site. The officials of all three agencies said that their reviews did not uncover any major new problems, but did identify a number of lower-level technical concerns that they required Equifax to address.

- **Modified contracts with Equifax.** IRS and SSA made changes to contracts they had with Equifax to require prompt notification of any future breach, among other things. According to officials from both agencies, Equifax did not directly notify major federal customers of the 2017 breach prior to its public announcement because its contracts with these agencies required notification only of breaches directly involving the systems that provided services to the federal government. SSA officials stated that it was important to update the agency's contract to require Equifax to promptly notify SSA of any data breach, regardless of which of the company's systems it may affect. IRS officials stated that a similar change was made to their contract with Equifax for credit reporting services. The contract change also required the company to notify IRS within one hour after a breach is discovered, rather than within the previous time frame of 24 hours. In addition, according to the officials, cybersecurity language in the IRS's contract was modified to ensure better implementation and oversight of technical security controls.
- **Communicated with the public and affected individuals.** IRS made public announcements about the impact of the breach, noting that the agency did not expect the breach to have any impact on taxpayers' ability to securely file tax returns. SSA issued a public blog post reminding consumers about steps they could take to protect their Social Security numbers.³⁵
- **Made changes to agency identity-proofing procedures.** Following its assessment, IRS updated its internal cybersecurity contractor requirements and controls related to incident handling. Further, upon completing its assessment, USPS initiated discussions with the National Institute of Standards and Technology to determine risks associated with the knowledge-based verification questions it had been using with Equifax's identity-proofing service. USPS

³⁵See <https://blog.ssa.gov/protecting-your-social-security/>.

subsequently changed its process, removing certain knowledge-based verification questions and adding a procedure whereby customers receive a code in the mail that they can use to verify their mailing addresses.

- **Canceled a short-term contract with Equifax.** Before the Equifax breach, Equifax was the incumbent contractor at IRS for taxpayer identity and verification services.³⁶ In June 2017, prior to the discovery of the breach, IRS began a new acquisition for these services by issuing a request for quotations to three CRA vendors (including Equifax and Experian) holding contracts under the federal supply schedule. IRS selected Experian as offering the lowest-priced, technically acceptable quotation, for issuance of a fixed-price task order and establishment of a blanket purchase agreement.³⁷ Equifax filed a bid protest on July 5, 2017 with GAO challenging the IRS's evaluation of Experian's quotation.³⁸ As described elsewhere in this report, Equifax discovered the breach on July 29 and, after investigating it, announced the breach on September 7. On September 29, during GAO's consideration of the protest, IRS awarded Equifax a short-term, sole-source contract for \$7.25 million to cover its need for the identity and verification services during the time frame needed to resolve the protest. IRS considered these services "critical" that "cannot lapse." However, following the completion of its breach-related security assessments, IRS issued Equifax a stop-work order to suspend its performance under the short-term, sole-source order. GAO denied Equifax's protest on October 16, 2017 and IRS proceeded with the task order issued to Experian for the taxpayer identity and verification services.

DHS Offered Breach Response Services to Equifax

In its role as the center for federal information security incident prevention and response, DHS offers services to assist federal agencies in preparing for potential cyber incidents, maintaining awareness of the current threat environment, and dealing with ongoing breaches. Under a Presidential

³⁶This contract was separate from the IRS contract for credit reporting services, which was modified to require notification within one hour.

³⁷A blanket purchase agreement is a simplified method of filling anticipated repetitive needs for supplies or services by establishing "charge accounts" with qualified sources of supply.

³⁸GAO, *Equifax Information Services, LLC*, B-414907 (Washington, D.C.: October 16, 2017). GAO's statutory bid protest function is separate from its audit mission.

directive,³⁹ DHS is also responsible for assisting public- and private-sector critical infrastructure owners and operators in preparing for, preventing, protecting against, mitigating, responding to, and recovering from a cyber incident.⁴⁰

In September 2017, shortly after the Equifax breach was publicly announced, DHS contacted the company to offer its professional services related to forensic analysis and breach response. However, according to officials at both organizations, Equifax notified DHS officials that the company had already retained professional services from a private cybersecurity consultant and, thus, declined assistance from DHS.

Oversight Agencies Opened Investigations and Provided Information and General Advice to Consumers

According to Equifax officials, the company informed regulators about the data breach on September 7, 2017—when the general public was notified. FTC announced that it was investigating the Equifax breach, and Equifax stated in its annual report that several governmental agencies, including FTC and BCFP, were continuing to investigate events related to the breach.

BCFP staff told us that, immediately following notification of the breach, they participated in conference calls with Equifax to learn more about the breach. According to the officials, their calls with Equifax focused on ensuring consumers were provided with accurate information about the breach and what they could do to protect themselves. Equifax officials told us that they also informed FTC, the Securities and Exchange Commission, various states' attorneys' general, and the Financial

³⁹Presidential Policy Directive (PPD) 41 sets forth principles governing the federal government's response to any cyber incident, whether involving government or private-sector entities.

⁴⁰For more information, see GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, [GAO-14-354](#) (Washington, D.C.: Apr. 30, 2014).

Services Information Sharing and Analysis Center, that it had suffered a breach.⁴¹

Shortly after Equifax's public announcement of the breach, BCFP released a blog post on the top 10 ways that consumers could protect themselves in the wake of the breach.⁴² Suggestions included regularly reviewing credit reports, checking credit card statements, and changing passwords for all financial accounts. In addition, BCFP posted on its website actions consumers could take to protect themselves against fraud or identity theft, including freezing credit and placing fraud alerts.

BCFP staff told us that, while the agency posts information to its website, it does not provide individual legal assistance to consumers. Nevertheless, the staff said that consumers can file a complaint with BCFP if they are experiencing issues related to a CRA. BCFP staff added that they received a large volume of consumer complaints following the Equifax breach. BCFP staff said they use such complaints as one factor to prioritize future supervisory examinations, as well as investigations and enforcement actions.

In October 2017, BCFP also began conducting targeted data security and cybersecurity examinations. Specifically, in addition to assessing whether the CRAs' data security practices and policies constitute violations of federal consumer financial law, BCFP began assessing risks to consumers posed by potential cybersecurity lapses and to markets for consumer financial products and services. BCFP staff said that whether BCFP continues to conduct CRA cybersecurity examinations will depend on whether they identify the issue as a priority through future examination prioritization processes.

Similarly, FTC released a statement to consumers with information about the breach, such as when it occurred and the types of data

⁴¹The Financial Services Information Sharing and Analysis Center is a central resource for cyber threat information for institutions in the financial sector. It is one of a number of centers that was established within industry sectors identified as having critical infrastructure in response to Presidential Decision Directive 63 (issued in 1998). Within these centers, security specialists identify, analyze, and share information; collaborate on threats, incidents, vulnerabilities, and best practices; and work to protect their respective industries from cyber and physical threats. These centers also can provide risk mitigation and alerts.

⁴²See www.consumerfinance.gov/about-us/blog/top-10-ways-protect-yourself-wake-equifax-data-breach/.

compromised.⁴³ The statement also included guidance on steps consumers could take to help protect their information from being misused. For example, FTC encouraged individuals to visit Equifax's website to find out whether their information may have been exposed, provided links to obtain a free credit report, and offered other information about credit freezes and fraud alerts.

On June 25, 2018, eight state banking regulators issued a consent order requiring Equifax to address various data security issues. The order included several areas of concern, including general information security, internal audits, and board and management oversight. More specifically, the order required Equifax, the board, or its audit committee to, among other things:

- provide a written risk assessment that identifies foreseeable threats and vulnerabilities to the confidentiality of PII;
- establish a formal and documented internal audit program that is capable of effectively evaluating information technology controls;
- improve the oversight of its information security program;
- improve oversight and documentation of its critical vendors;
- improve standards and controls for supporting the patch management function; and
- enhance oversight of IT operations as it relates to disaster recovery and business continuity functions.

Under the consent order, Equifax was required to submit a list of all remediation projects planned, in process, or implemented to the state regulatory agencies by July 31, 2018.

Agency Comments and Third-Party Views

We provided a draft of this report to BCFP, DHS, FTC, IRS, SSA, USPS, and Equifax for comment. SSA and USPS provided written responses expressing appreciation for the opportunity to review the draft report. The SSA and USPS responses are reprinted in appendices II and III, respectively. In addition, BCFP, DHS, FTC, IRS, SSA, USPS, and Equifax provided technical comments orally and via email, which we have incorporated, as appropriate.

⁴³See <https://www.ftc.gov/equifax-data-breach>.

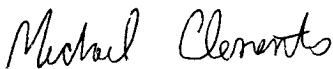
As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 29 days from the report date. At that time, we will send copies to the appropriate congressional committees, Equifax, and to the Acting Director of the Bureau of Consumer Financial Protection; the Chairman of the Federal Trade Commission; the Secretary of the Department of Homeland Security; the Commissioners of the Internal Revenue Service and Social Security Administration; and the Postmaster General of the United States. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>. We are sending copies of this report to In addition, the report is 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 Nick Marinos at (202) 512-9342 or marinosn@gao.gov, or Michael Clements at (202) 512-8678 or clementsm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Sincerely yours,



Nick Marinos
Director, Cybersecurity and Data Protection Issues



Michael Clements
Director, Financial Markets and Community Investment

List of Congressional Requesters

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

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

The Honorable Trey Gowdy
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) summarize the events regarding the 2017 Equifax breach and the steps taken by the company to assess, respond to, and recover from the incident and (2) describe the actions that federal customers and oversight agencies took in response to the breach.

To address the first objective, we obtained and assessed documentation generated in response to the breach. Specifically, we analyzed the results of security assessments conducted by Equifax and its cybersecurity consultant following the breach, which included information about how the attacker gained access to Equifax's systems and the specific vulnerabilities that were exploited. This documentation included the report summarizing the results of the consultant's forensic analysis of Equifax systems and the consultant's recommendations to Equifax to address the factors that led to the breach. We also reviewed Equifax's relevant public filings to the Securities and Exchange Commission and statements it provided to the public and shareholders, which included information about the data breach and the company's efforts for remediation.

Further, we conducted a site visit to the Equifax data center in Alpharetta, Georgia, to interview knowledgeable officials, such as the interim Chief Security Officer and other officials knowledgeable about how Equifax stores and processes data, and observed physical security measures. In addition, to clarify details of the breach and the steps that Equifax took, we interviewed officials at Equifax who were responsible for coordinating reviews conducted following the breach. Specifically, we interviewed the interim Chief Security Officer and government relations employees, who were responsible for coordinating Equifax's interaction with federal agencies in response to the incident.

We did not independently assess Equifax's information security controls or the steps the company took to address identified factors that contributed to the ineffective implementation of those controls. Specifically, the scope of our report was to report on actions taken by Equifax and agencies in response to the breach. Consequently, the information in this report is based on public filings and announcements as well as information provided to us by the company. We did not reach conclusions regarding the adequacy or efficacy of Equifax's security measures.

To address the second objective, we selected three major federal agencies, Internal Revenue Service (IRS), Social Security Administration (SSA), and United States Postal Service (USPS), which were Equifax's largest federal customers at the time of the breach. We initially identified

these customer agencies by reviewing public reports following the breach that identified federal agencies that were major Equifax customers at the time. We also interviewed Equifax officials responsible for managing government accounts to confirm that these three agencies were the only large-scale federal customer agencies that interacted with Equifax following the breach. Other federal agencies also have contracts with Equifax for a variety of services; we did not conduct audit work for this engagement at any other agencies because we narrowed our selection criteria to the largest federal agencies that used Equifax's services to conduct their identity-proofing processes.

Subsequently, we analyzed documentation from IRS, SSA, and USPS to describe the relevant actions these agencies took in response to the breach, as well as documentation regarding oversight by BCFP and FTC, which are the federal agencies with primary oversight responsibilities over CRAs. Specifically, we reviewed relevant laws and BCFP guidance on data security examinations. In addition, we spoke with BCFP and FTC officials about their actions in response to the data breach and reviewed their websites for information provided to consumers.

We also selected and reviewed contracts between Equifax and each of the three selected agencies—IRS, SSA, and USPS—to determine what changes were made to services, such as identity-proofing solutions, provided by Equifax to federal agencies as a result of the breach. The contracts we reviewed were the ones identified by IRS, SSA, and USPS as contracts with Equifax for credit reporting or identity-proofing services.

Further, we conducted interviews with agency officials at BCFP, FTC, DHS, IRS, SSA, and USPS to determine what actions customer and oversight agencies took in response to the breach. The officials we interviewed were responsible for conducting their agencies' security assessment of Equifax at the time of the data breach. These included officials at each agency that had a role in responding to the Equifax breach, such as investigators at the oversight agencies and information security officials at the federal customer agencies.

To address both objectives, and to identify how federal requirements apply to credit reporting agencies, we analyzed relevant federal laws to determine the responsibilities of agencies and their contractors. Specifically, we reviewed the following laws:

- *Dodd-Frank Wall Street Reform and Consumer Protection Act;*

- *Fair Credit Reporting Act;*
- *Gramm-Leach-Bliley Act;*
- *Privacy Act of 1974; and*
- *E-Government Act of 2002.*

We conducted this performance audit from November 2017 to August 2018 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.

Appendix II: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

July 30, 2018

Mr. Nick Marinos
Director, Cybersecurity and Data Protection Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to review the draft report, "DATA PROTECTION: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach" (GAO-18-559).

We appreciate that the report acknowledges our efforts regarding the breach of Equifax's systems. Maintaining the privacy and security of the public's data is of paramount importance to us. We will continue our efforts to keep our data systems secure.

Your staff may contact Trae Sommer, Acting Director, Audit Liaison Staff, at (410) 965-9102.

Sincerely,

A handwritten signature in blue ink that reads "Stephanie Hall".

Stephanie Hall
Acting Deputy Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix III: Comments from the United States Postal Service

GREGORY S. CRABB
VICE PRESIDENT
CHIEF INFORMATION SECURITY OFFICER



July 31, 2018

Nick Marinos
Director, Cybersecurity
and Data Protection Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0002

Dear Mr. Marinos:

This is in response to your August 2018 Government Accountability Office (GAO) Draft report titled, "Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach".

Thank you for the opportunity to review and comment on the above subject matter. Currently, we do not have comments to add beyond those reflected in the document or shared within the review process.

If you have any questions or concerns, please contact my office at 202-268-7666.

Sincerely,

A handwritten signature in black ink, appearing to read "G. Crabb".

Gregory S. Crabb

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4021
WWW.USPS.COM

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Staff Acknowledgments

In addition to the individuals named above, John de Ferrari and John Forrester (assistant directors); Tina Torabi (analyst-in-charge); Bethany Benitez, Chris Businsky, Kavita Daitnarayan, Nancy Glover, Andrea Harvey, Thomas Johnson, David Plocher, Tovah Rom, Rachel Siegel, and Winnie Tsen made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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



Please Print on Recycled Paper.