UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEDERAL TRADE COMMISSION, Plaintiff, v. EQUIFAX INC., Defendant.	Case No. ___________________ **COMPLAINT FOR PERMANENT INJUNCTION AND OTHER RELIEF**

Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §53(b), and the Standards for Safeguarding Customer Information ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Sections 501-504 of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. §§ 6801-6804, to obtain permanent injunctive relief, restitution, and other relief for Defendant's violations of the FTC Act, 15 U.S.C. § 45(a), and the Safeguards Rule, 16 C.F.R. Part 314.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

3. Venue is proper in this District under 28 U.S.C. § 1391(b)(1), (b)(2), (c)(2), and (d) and 15 U.S.C. § 53(b).

PLAINTIFF

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the Safeguards Rule, 16 C.F.R. Part 314, which requires financial institutions to protect the security, confidentiality, and integrity of customer information.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the Safeguards Rule and to secure such relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b) and 16 C.F.R. Part 314.

DEFENDANT

6. Equifax Inc. is a Georgia corporation with its principal place of business at 1550 Peachtree Street, NW, Atlanta, Georgia 30309. Defendant Equifax Inc., through certain of its subsidiaries, including Equifax Consumer Services LLC

and Equifax Information Services LLC, transacts or has transacted business in this District and throughout the United States.

COMMERCE

7. At all times material to this Complaint, Defendant has maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANT’S BUSINESS ACTIVITIES

8. Defendant, one of the three nationwide consumer reporting agencies in the United States, offers various credit reporting and information products and services to businesses and consumers. Defendant collects, processes, stores, and maintains vast quantities of personal information, including personal information about more than 200 million U.S. consumers.

9. Defendant stores much of this information in its main U.S. credit reporting database, known as Automated Credit Reporting Online (“ACRO”). Defendant uses ACRO to provide credit reports, credit scores, collections, and prescreening products, among other things.

10. Defendant also maintains on its network a system referred to as the Automated Consumer Interview System (“ACIS”). ACIS is a network of applications and automated processes that handles consumer questions, concerns,

and disputes regarding consumer credit data. Among other things, the ACIS network services an online dispute portal (the "ACIS Dispute Portal"), a web application where consumers can dispute items appearing on their consumer credit reports and upload supporting documentation. ACIS also services Defendant's platform for consumer credit freezes and fraud alerts, as well as all consumer requests for a free annual file disclosure through AnnualCreditReport.com ("ACR").

11. When a consumer disputes items on his or her credit report through the ACIS Dispute Portal or otherwise transacts with Defendant for a consumer product or service (such as a subscription to a credit monitoring product, a request to freeze the consumer's credit, or a request for a free credit report from ACR), the consumer must first submit sensitive personal information. For example, a consumer who requests a free credit report from ACR must submit, among other things, a name, date of birth, and Social Security number ("SSN"). A consumer who requests a security freeze or a copy of his or her credit score or credit report must submit similar personally identifiable information ("PII"), as well as a credit card number and expiration date if a purchase is being made. Defendant logs and stores consumers' PII in databases connected to ACIS. These databases thus contain hundreds of millions of records of sensitive personal information.

12. ACIS was originally built in the 1980s. It was designed to connect with ACRO and runs on old systems, many of which are no longer supported. Today, Defendant considers ACIS to be legacy infrastructure and its own documents describe the system as "archaic" and using "antiquated technology." As of 2016, about 25 million consumers interact with ACIS every year, with about 6.6 million of those consumers disputing transactions in their credit reports.

DEFENDANT'S 2017 DATA BREACH

13. On or about September 7, 2017, Defendant publicly disclosed a massive data breach (the "Breach") involving the theft of sensitive personal information from more than 147 million consumers. As described below, the Breach resulted from Defendant's failure to undertake numerous basic security measures to secure the PII stored in databases connected to the ACIS Dispute Portal.

14. On or about March 8, 2017, the United States Computer Emergency Readiness Team ("US-CERT") alerted Defendant to a new critical security vulnerability (referred to as 2017-CVE-5638) found in Apache Struts, an open source framework used to build Java web applications. The alert encouraged anyone using a vulnerable version of the software to update the software to a new version released by the Apache Software Foundation, which was available for free online to

all Apache software users. Within days, press reports indicated that attackers had already begun to exploit this critical vulnerability.

15. Defendant's security team received the US-CERT alert and, on or about March 9, 2017, disseminated the alert internally by a mass email to more than 400 employees. The mass email directed employees, "if [they were] responsible for an Apache Struts installation," to patch the vulnerability within 48 hours, as required by Defendant's Patch Management Policy.

16. The ACIS Dispute Portal contained a vulnerable version of Apache Struts. However, Defendant failed to apply the patch to the ACIS Dispute Portal for months. Although Defendant's security team issued an order to patch all vulnerable systems within 48 hours, Defendant failed to send the email ordering a patch to the employee responsible for maintaining the ACIS Dispute Portal. As a result, Defendant failed to notice or remediate the unpatched ACIS Dispute Portal.

17. On or about March 15, 2017, Defendant performed an automated vulnerability scan intended to search for vulnerable instances of Apache Struts that remained on Defendant's network. But Defendant used a scanner that was not configured to correctly search all of Defendant's potentially vulnerable assets. As a result, the automated scanner did not identify any systems vulnerable to 2017-CVE-5638 and the ACIS Dispute Portal remained unpatched.

18. Defendant failed to discover the unpatched vulnerability for more than four months. On or about July 29, 2017, Defendant's security team identified some suspicious traffic on the ACIS Dispute Portal after replacing expired security certificates. Defendant's security personnel blocked the suspicious traffic but identified additional suspicious traffic the next day, at which time Defendant took the ACIS Dispute Portal offline.

19. Defendant retained a forensic consultant who ultimately determined that between May 13, 2017, and July 30, 2017, multiple attackers were each able to separately exploit the 2017-CVE-5638 vulnerability in the ACIS Dispute Portal to gain unauthorized access to Defendant's network. Once inside, the attackers were able to crawl through dozens of unrelated databases containing information that went well beyond the ACIS Dispute Portal, in part because of a lack of network segmentation. The attackers also accessed an unsecured file share (or common storage space) connected to the ACIS databases where they discovered numerous administrative credentials, stored in plain text, that they used to obtain further access to Defendant's network. By August 11, 2017, Defendant had determined that the attack had likely compromised a large amount of consumer PII.

20. During the months that the attackers were able to operate undetected on Defendant's network, the attackers ran nearly ten thousand queries on

Defendant’s databases. Some of these queries were specifically designed to identify SSNs, dates of birth, and other sensitive personal information most valuable for identity theft.

21. According to Defendant’s forensic analysis, the attackers were able to steal approximately 147 million names and dates of birth, 145.5 million SSNs, 99 million physical addresses, 20.3 million telephone numbers, 17.6 million email addresses, and 209,000 payment card numbers and expiration dates, among other things. This data, in part, came from consumers who had previously obtained direct-to-consumer products from Defendant, such as credit scores, credit monitoring, and identity theft prevention products, as well as from consumers who had requested a free copy of their Equifax credit report through ACR.

22. The attackers were able to steal a staggering amount of personal information due to a series of basic security failures that Defendant failed to address, including:

A. Defendant failed to patch 2017-CVE-5638, a critical vulnerability. Defendant’s patch management policies and procedures, which did not require any of Defendant’s more than four hundred employees to acknowledge receipt of a critical patch directive or otherwise confirm that a critical patch was applied, directly contributed to this failure.

B. Defendant's reliance on an automated vulnerability scanner – without any other compensating controls to ensure that the vulnerability had been fully addressed – further contributed to Defendant's failure to patch the vulnerability. Although many companies use automated vulnerability scanners, Defendant (1) did not maintain an accurate inventory of public facing technology assets running Apache Struts (and therefore did not know where the scanner needed to run) and (2) relied on a scanner that was not configured to search through all potentially vulnerable public facing websites.

C. Defendant failed to segment the database servers connected to ACIS, a failure that permitted the attackers to easily gain access to vast amounts of information related to a broad variety of Equifax consumer products and services. The attackers did not need complex or advanced tools to pivot across Defendant's network.

D. Defendant left a file share connected to the ACIS databases where it was easily accessible by the attackers. The file share contained numerous administrative credentials and passwords in plain text. The file share also contained PII and was not protected by access controls. The attackers were able to leverage the credentials and passwords to access and comb through dozens of unrelated databases searching for sensitive personal information.

E. Defendant stored more than 145 million SSNs and other sensitive personal information in plain text, contrary to Defendant's own policies that require strong encryption and access controls for such PII.

F. Defendant had minimal protections for detecting intrusions on "legacy" technology systems such as ACIS, which contributed to Defendant's months-long failure to detect the attackers on its network. For instance, the ACIS system lacked any file integrity monitoring, which would have alerted Defendant to unauthorized activity within the ACIS environment. In addition, Defendant failed to update expired security certificates on the ACIS Dispute Portal, which prevented Defendant from using tools in its possession that would have decrypted suspicious traffic. The security certificate on the ACIS Dispute Portal had expired at least 10 months before the discovery of the Breach.

DEFENDANT'S DATA SECURITY PRACTICES

23. Defendant engaged in a number of practices that, taken together, failed to provide reasonable security for the massive quantities of sensitive personal information stored within Defendant's computer network. Among other things:

A. Defendant failed to implement reasonable procedures to detect, respond to, and timely correct critical and other high-risk security vulnerabilities across Defendant's systems, including:

i. Patch management policies and procedures that failed to ensure the timely remediation of critical security vulnerabilities;

ii. Widespread noncompliance with Defendant's patch management policy, including unpatched critical and high-risk vulnerabilities across Defendant's systems that persisted for months;

iii. A failure to implement reasonable intrusion protection controls in legacy systems; including:

a) Failures to implement host and network intrusion prevention or file integrity monitoring that could have identified unauthorized access to Defendant's network; and

b) Failures to maintain security certificates that would have allowed Defendant to examine traffic for suspicious activity;

iv. Failures to implement readily-available protections, including many low-cost protections, against well-known and reasonably foreseeable vulnerabilities, such as Cross-Site Scripting ("XSS"), Structured Query Language ("SQL") injection, security misconfigurations, and other common vulnerabilities, that could be exploited to gain unauthorized access to sensitive personal information and local networks;

B. Defendant failed to use readily available security measures to segment its servers and databases;

C. Defendant failed to implement or enforce reasonable access controls to prevent unauthorized access to sensitive personal information. For example,

i. Defendant stored numerous administrative credentials with access to sensitive personal information in plain text;

ii. Defendant copied sensitive personal information, including SSNs, to numerous systems for development and testing purposes, which were accessible by employees and contractors without any business need;

iii. Defendant failed to monitor or log privileged account activity across numerous systems; and

iv. Until at least 2017, Defendant failed to limit administrative rights for any of its employees on company-issued PCs and other devices, and allowed users to install any software or alter configurations;

D. Defendant stored sensitive personal information in plain text, including hundreds of millions of SSNs and payment card information, including credit card account numbers provided by consumers to purchase direct-to-consumer products; and

E. Defendant failed to provide adequate security training for engineers and other employees.

24. Defendant could have prevented or mitigated the failures described in **Paragraph 23** through cost-effective measures suitable for an organization of Defendant's size and complexity.

25. Internal company documents, since at least 2014, clearly demonstrate Defendant's awareness and actual knowledge of the failures described in **Paragraph 23**.

26. Defendant's failure to reasonably secure the sensitive personal information in their network, described in **Paragraphs 22-23**, has resulted in substantial injury to nearly 150 million consumers whose personal information was stolen by identity thieves. These injuries include wasted time and money to secure personal accounts and consumer reports from future identity theft, the cost of obtaining additional credit monitoring products or security freezes, and a significantly increased risk of becoming victims of identity theft in the future. Additionally, because information such as SSNs and dates of birth are immutable, identity thieves could wait years before capitalizing on the stolen information. Thus, Defendant's security failures are likely to continue to substantially injure consumers in the future. In addition to the injury to consumers by having to spend time and

money taking measures to protect their identities, Defendant's failures caused or are likely to cause consumers to experience identity theft.

DEFENDANT'S SECURITY REPRESENTATIONS TO CONSUMERS AND SMALL BUSINESSES

27. Since at least October 2013, Defendant has maintained a privacy policy for Defendant's direct-to-consumer offerings, including credit scores, credit monitoring and identity management services, provided by Equifax Consumer Services LLC, which states:

> We are committed to protecting the security of your information through procedures and technologies designed for this purpose by taking these steps: We limit access to your personal information to employees having a reasonable need to access this information to provide products and services to you . . . We have reasonable physical, technical, and procedural safeguards to help protect your personal information.

28. In fact, as described above in **Paragraphs 22-23,** Defendant's security practices did not live up to the representations contained in these privacy policies. First, as previously described, Defendant did not limit access to personal information only to employees having a reasonable need to access the information. In many

instances, Defendant stored sensitive personal information, obtained from consumers who purchased Defendant's direct-to-consumer products, in systems without any access controls where employees and contractors could access the sensitive personal information without any business need. Second, Defendant's many security failures described in **Paragraphs 22-23** failed to provide reasonable technical, physical, or procedural safeguards for consumer data on Defendant's network.

29. Equifax Small Business offers a variety of products, including Equifax ePort, which it describes as "an easy-to-use portal that streamlines access to Equifax consumer and commercial credit information and analytics tools." Approximately 142,000 records containing data collected by ePort were among the various database tables that attackers accessed in the Breach.

30. Since at least October 2013, Equifax Small Business has maintained a privacy policy that applies when consumers or small businesses purchase, access, or use U.S. Equifax Small Business Products for personal or business purposes through Equifax.com. That policy recites the same security statement set forth above in **Paragraph 27.** For the reasons previously set forth at **Paragraphs 22-23 and 28**, this statement was false or misleading.

31. Had consumers and/or small businesses known that the security statements set forth in **Paragraphs 27 and 30** were false or misleading, such knowledge would have affected the decisions of consumers and/or small businesses to purchase Defendant's products and services.

DEFENDANT VIOLATED THE GLB ACT'S SAFEGUARDS RULE

32. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A), and is subject to the GLB Act.

33. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including, among other things, (1) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (2) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; and (3) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the

business' operations or business arrangements, and any other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. Violations of the Safeguards Rule are enforced through the FTC Act. 15 U.S.C. § 6805(a)(7).

34. For the reasons previously described in **Paragraphs 22-23**, Defendant did not design and implement safeguards to address foreseeable internal and external risks, regularly test or monitor the effectiveness of the safeguards, or evaluate and adjust the information security program in light of the results of testing and monitoring and other relevant circumstances. Defendant has therefore violated the GLB Act Safeguards Rule.

VIOLATIONS OF THE FTC ACT

35. Section 5(a) of the FTC Act, 15 U.S.C. §45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce." Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

Unfair Acts or Practices Regarding Defendant's Data Security Practices

36. As described in **Paragraphs 23-26**, Defendant has failed to provide reasonable security for the sensitive personal information collected, processed, maintained, or stored within Defendant's computer networks.

37. Defendant's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

38. Defendant's acts or practices set forth in **Paragraph 36** constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

COUNT II

Deceptive Acts or Practices Regarding Defendant's Data Security to Consumers

39. Through the means described in **Paragraph 27**, Defendant has represented, directly or indirectly, expressly or by implication, that Defendant limits access to personal information to employees having a reasonable need to access this information to provide products and services to consumers, and that Defendant has reasonable physical, technical, and procedural safeguards to protect personal

information for Defendant's direct-to-consumer offerings, including credit monitoring and identity theft management services.

40. In truth and in fact, in numerous instances, Defendant failed to limit access to personal information to employees having a reasonable need to access this information and lacked reasonable physical, technical, or procedural safeguards to protect this information.

41. Defendant's representations as set forth in **Paragraph 39** are false or misleading and constitute a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C § 45(a).

COUNT III

Deceptive Acts or Practices Regarding Defendant's Data Security to Small Businesses

42. Through the means described in **Paragraph 30**, Defendant has represented, directly or indirectly, expressly or by implication, that Defendant limits access to personal information to employees having a reasonable need to access this information to provide products and services to consumers, and that Defendant has reasonable physical, technical, and procedural safeguards to protect personal information, for U.S. Equifax Small Business Products used for business or personal purposes.

43. In truth and in fact, in numerous instances, Defendant failed to limit access to personal information to employees having a reasonable need to access this information and lacked reasonable physical, technical, or procedural safeguards to protect this information.

44. Defendant's representations as set forth in **Paragraph 42** are false or misleading and constitute a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C § 45(a).

COUNT IV

VIOLATIONS OF THE GLB ACT SAFEGUARDS RULE

45. In numerous instances, Defendant failed to design and implement safeguards to address foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, has not regularly tested or monitored the effectiveness of the safeguards, and has not evaluated and adjusted Defendant's information security program in light of the results of testing and monitoring, and other relevant circumstances, as required by the Safeguards Rule, 16 C.F.R. Part 314.

46. Defendant's acts or practices, as described in **Paragraph 45** above, violate the Safeguards Rule, 16 C.F.R. Part 314.

CONSUMER INJURY

47. Consumers have suffered and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act and the GLB Act Safeguards Rule. In addition, Defendant has been unjustly enriched as a result of its unlawful acts or practices. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

48. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

PRAYER FOR RELIEF

49. Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. §§ 53(b), the Safeguards Rule, 16 C.F.R. Part 314, and the Court's own equitable powers, request that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act and the Safeguards Rule;

B. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendant's violations of the FTC Act and the Safeguards Rule, including but not limited to rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies;

C. Award Plaintiff the costs of bringing this action; and

D. Award additional relief as the Court may determine to be just and proper.

DATED: July 22, 2019

Respectfully Submitted,

/s/ Anna M. Burns

ANNA M. BURNS
GA Bar No. 558234
Federal Trade Commission
Southeast Region
225 Peachtree Street, N.E., Suite 1500
Atlanta, GA 30303
Telephone: (404) 656-1350
Facsimile: (404) 656-1379
E-mail: aburns@ftc.gov

JACQUELINE K. CONNOR
TIFFANY GEORGE
CATHLIN TULLY
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
Telephone: 202-326-2844 (Connor)
Telephone: 202-326-3040 (George)
Telephone: 202-326-3644 (Tully)
Facsimile: 202-326-3062
Email: jconnor@ftc.gov
tgeorge@ftc.gov
ctully@ftc.gov