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

(u)-8.3 anoci1

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

mepi272.2 (al)3.7 pee ofttn mma Tc 0 Tw 22. (m118)8.312.1 (nt)0.5 (

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

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

15. Defendant's security

18. Defendant failed to discover the unpatched vulnerability for more than four months. On or about July 29, 2017, Defendant

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 vpaea (c7m ( )]T -0

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 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-.572 0 Td [(r)22 a)

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

E.

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

DEFENDANT’S

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**

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.

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.

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