

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

	)	MDL Docket No. 2800
In re: Equifax, Inc. Customer	)	Case No.: 1:17-md-2800-TWT
Data Security Breach Litigation	)	
	)	CONSUMER CASES
	)	
	)	

**~~PROPOSED~~ CONSENT ORDER**

On July 22, 2019, the Consumer Plaintiffs, by and through the Settlement Class Representatives on behalf of themselves and the Settlement Class, entered into a Settlement Agreement with Defendants Equifax Inc., Equifax Information Services LLC, and Equifax Consumer Services LLC (collectively “Equifax”) to resolve the consumer track of the above-captioned litigation.

Pursuant to Sections 2.7, 4.1.1, and 4.1.2, and Exhibits 2 and 3 of the Settlement Agreement, Equifax is obligated to undertake certain Business Practice Commitments that are to be memorialized in a Consent Order entered by this Court in connection with the Judgment. The Court, having reviewed the Settlement Agreement, Exhibits, and Business Practices Commitments set forth therein, hereby ORDERS as follows:

Unless otherwise specified below, the following security measures or their equivalents will be deployed and maintained by Equifax for at least five (5) years from the date this Court grants final approval of the Settlement Agreement:

1. **Scope:** This Order shall apply to all networking equipment, databases or data stores, applications, servers, and endpoints that: (1) are capable of accessing, using or sharing software, data, and hardware resources; (2) are owned, operated, and/or controlled by Equifax; and (3) collect, process, store, have access, or grant access to Personal Information of consumers who reside in the United States, but excluding networking equipment, databases or data stores, applications, servers, or endpoints outside of the U.S. where access to Personal Information is restricted using a risk-based control (“Equifax Network”). For purposes of this Order, the following definitions apply:
  - a. “Personal Information” shall have the same meaning as set forth in the data privacy laws in the states in which Class Members reside, unless preempted by federal law.
  - b. The “NIST Standard” refers to the most recent applicable NIST guidance, beginning with NIST 800-53r4, as the primary set of standards, definitions, and controls. Where this Order requires

Equifax to test cyber resilience, Equifax will use an industry-recognized cybersecurity framework (for example, NIST CSF framework). Where this Order refers to “NIST or another comparable standard,” Equifax either will use the NIST standard indicated above or another industry-recognized cybersecurity standard that satisfies Regulator Requirements.

- c. “Regulator” means the Federal Trade Commission (“FTC”), the Consumer Financial Protection Bureau (“CFPB”), or the multi-state group of state Attorneys General investigating the 2017 Data Breach. If no Regulator is willing or able to make a determination under this Order, then one of the attorneys designated as Co-Lead Counsel for the Consumer Plaintiffs in this multi-district litigation, or their law firms, and Equifax’s CISO or their designee shall, in good faith, reach a determination.

2. **Information Security Program:** Within ninety (90) days of final approval of the Settlement Agreement, Equifax shall implement, and thereafter regularly maintain, review, and revise a comprehensive Information Security Program that is reasonably designed to protect the

confidentiality, integrity, and availability of the Personal Information that Equifax collects, processes, or stores on the Equifax Network.

3. **Managing Critical Assets:** Equifax shall identify and document a comprehensive IT asset inventory, using an automated tool(s) where practicable, that, consistent with NIST or another comparable standard, will inventory and classify, and issue reports on, all assets that comprise the Equifax Network, including but not limited to software, applications, network components, databases, data stores, tools, technology, and systems. The asset inventory required under this paragraph shall be regularly updated and, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the Equifax Network; and (e) the asset's criticality rating. Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process<sup>1</sup> establishing that hardware and software within the Equifax Network be rated based on criticality, factoring in whether such assets are used to collect, process, or store

---

<sup>1</sup> "Governance Process" shall mean any written policy, standard, procedure or process (or any combination thereof) designed to achieve a control objective with respect to the Equifax Network.

Personal Information. Equifax shall comply with this provision by June 30, 2020.

4. **Data Classification:** Equifax shall maintain and regularly review and revise as necessary a data classification and handling standard.
5. **Security Information and Event Management:** Consistent with NIST or another comparable standard, Equifax shall implement a comprehensive, continuous, risk-based SIEM solution (or equivalent). Equifax shall continuously monitor, and shall test on at least a monthly basis, any tool used pursuant to this paragraph, to properly configure, regularly update, and maintain the tool, to ensure that the Equifax Network is adequately monitored.
6. **Logging and Monitoring:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing:
  - (1) risk-based monitoring and logging of security events, operational activities, and transactions on the Equifax Network, (2) the reporting of anomalous activity through the use of appropriate platforms, and (3) requiring tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance. The Governance

Process shall include the classification of security events based on severity and appropriate remediation timelines based on classification.

7. **Vulnerability Scanning:** Equifax shall implement and maintain a risk-based vulnerability scanning program reasonably designed to identify and assess vulnerabilities within the Equifax Network.
8. **Penetration Testing:** Equifax shall implement and maintain a risk-based penetration-testing program reasonably designed to identify and assess security vulnerabilities within the Equifax Network.
9. **Vulnerability Planning:** Equifax shall rate and rank the criticality of all vulnerabilities within the Equifax Network. For each vulnerability that is ranked most critical, Equifax shall commence remediation planning within twenty-four (24) hours after the vulnerability has been rated as critical and shall apply the remediation within one (1) week after the vulnerability has received a critical rating. If the remediation cannot be applied within one (1) week after the vulnerability has received a critical rating, Equifax shall identify or implement compensating controls designed to protect Personal Information as soon as practicable but no later than one (1) week after the vulnerability received a critical rating.

- 10. Patch Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process to maintain, keep updated, and support the software on the Equifax Network. Equifax shall maintain reasonable controls to address the potential impact that security updates and patches may have on the Equifax Network and shall maintain a tool that includes an automated Common Vulnerabilities and Exposures (CVE) feed with regular updates regarding known CVEs.
- 11. Threat Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing a threat management program designed to appropriately monitor the Equifax Network for threats and assess whether monitoring tools are appropriately configured, tested, and updated.
- 12. Access Control and Account Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to appropriately manage Equifax Network accounts. This Governance Process shall include, at a minimum, (1) implementing appropriate password, multi-factor, or equivalent authentication protocols; (2) implementing and maintaining appropriate policies for the secure storage of Equifax Network account passwords, including policies based

on industry best practices; and (3) limiting access to Personal Information by persons accessing the Equifax Network on a least-privileged basis.

- 13. File Integrity Monitoring:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to provide prompt notification of unauthorized modifications to the Equifax Network.
- 14. Legacy Systems:** Equifax shall develop and implement a risk-based plan to remediate current legacy systems on a schedule that provides for remediation within five years following entry of this Order and which includes applying compensating controls until the systems are remediated. Equifax shall also maintain a Governance Process for active lifecycle management for replacing and deprecating legacy systems when they reach end of life.
- 15. Encryption:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process requiring Equifax either to encrypt Personal Information or otherwise implement adequate compensating controls.
- 16. Data Retention:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing a retention



schedule for Personal Information on the Equifax Network and a process for deletion or destruction of Personal Information when such information is no longer necessary for a business purpose, except where such information is otherwise required to be maintained by law.

17. **TrustedID Premier:** Equifax, including by or through any partner, affiliate, agent, or third party, shall not use any information provided by consumers (or the fact that the consumer provided information) to enroll in TrustedID Premier to sell, upsell, or directly market or advertise its fee-based products or services.
18. **Mandatory Training:** Equifax shall establish an information security training program that includes, at a minimum, at least annual information security training for all employees, with additional training to be provided as appropriate based on employees' job responsibilities.
19. **Vendor Management:** Equifax shall oversee its third party vendors who have access to the Equifax Network by maintaining and periodically reviewing and revising, as needed, a Governance Process for assessing vendor compliance in accordance with Equifax's Information Security Program to assess whether the vendor's security safeguards are appropriate for that business, which Governance Process requires vendors

by contract to implement and maintain such safeguards and to notify Equifax within seventy-two (72) hours of discovering a security event, where feasible.

20. **Incident Response Exercises:** Equifax shall conduct, at a minimum, biannual incident response plan exercises to test and assess its preparedness to respond to a security event.
21. **Breach Notification:** Equifax shall comply with the state data breach notification laws, as applicable, and unless preempted by federal law.
22. **Information Security Spending:** Equifax shall ensure that its Information Security Program receives the resources and support reasonably necessary for the Information Security Program to function as required by this Settlement. In addition, over a five-year period beginning January 1, 2019, Equifax shall spend a minimum of \$1,000,000,000 (\$1 billion) on data security and related technology.
23. **Third-Party Assessments:** Equifax shall engage a Third-Party Assessor meeting the criteria specified in this Order to conduct a SOC 2 Type 2 attestation, or to conduct an assessment using industry-recognized procedures and standards in satisfaction of Regulator requirements for this Order (the “Third-Party Assessments”). The Third-Party Assessments will

meet the following minimum standards, unless a Regulator expressly authorizes otherwise:

- a. The Third-Party Assessments will be conducted by an unbiased, independent, cybersecurity organization agreeable both to Equifax and a Regulator. Prior to selection, Equifax will disclose to the Regulator approving the Third-Party Assessor any compensated engagement by Equifax of the Third-Party Assessor in the 2 years prior to the assessment. The Third-Party Assessor shall be a Certified Information Systems Security Professional (“CISSP”) or a Certified Information Systems Auditor (“CISA”), or a similarly qualified organization; and have at least five (5) years of experience evaluating the effectiveness of computer system security or information system security.
- b. The scope of the Third-Party Assessments, including the assertion statements required, will be established by the Third-Party Assessor in consultation with Equifax.
- c. The Third-Party Assessments will evaluate Equifax’s Information Security Program, including its policies and practices, consistent with NIST or another comparable standard.

- d. The reporting periods for the Third-Party Assessments shall (1) cover the first 180 days following final approval of the Settlement Agreement for the initial Third-Party Assessment, and each two-year period thereafter for a total of seven (7) years. Provided, however, that the parties agree in good faith to adjust this timeline to align with Third-Party Assessments performed for Regulators to the extent that they are used to satisfy this Order.
- e. The Third-Party Assessor will confirm that Equifax has complied with the terms of this Order.
- f. The Third-Party Assessments will identify deficiencies in Equifax's Information Security Program and, in good faith cooperation with Equifax's CISO or their designee, prioritize and establish dates by which Equifax shall remediate the deficiencies identified or implement compensating controls.
- g. Within 30 days after the close of each reporting period in Paragraph 23(d) above, the Third-Party Assessor will provide to Consumer Plaintiffs' Co-Lead Counsel a verification of compliance with this Order, which includes the identification of material deficiencies and Equifax's corresponding plan pursuant to Paragraph 23(f).

h. Equifax may use a Third-Party Assessment performed in satisfaction of obligations to government entities to meet the Third-Party Assessment requirement here, provided that the assessment complies with Paragraph 23 of this Order.

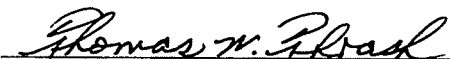
**24. Regulator Requirements:** The Parties and Court acknowledge that Equifax may be obligated to comply with requirements governing Equifax's Information Security Program and Third-Party Assessments as part of the resolution of claims stemming from the 2017 Data Breach and asserted against Equifax by certain government entities (the "Regulator Requirements"). In the event that any of the specific obligations set forth in the above provisions conflict with provisions set forth in the Regulator Requirements regarding the same or similar obligations, then the more restrictive Regulator provision shall apply and supersede the less restrictive provision in this Order.

**25. Miscellaneous:** In the event that technological or industry developments or intervening changes in law render any of the provisions set forth in this Order obsolete or make compliance by Equifax with any provision impossible or technically impractical, Equifax will provide notice to Consumer Plaintiffs Co-Lead Counsel. If the Parties reach a mutual

agreement that the elimination or modification of a provision is appropriate, they may jointly petition the Court to eliminate or modify such provision. If the Parties fail to reach an agreement, Equifax may petition the Court to eliminate or modify such provision. Under any circumstances, to the extent Consumer Plaintiffs believe that Equifax is not complying with any provision of this Order, they will first meet and confer with Equifax prior to seeking relief from the Court.

- 26. Continuing Jurisdiction and Enforcement:** The Court retains jurisdiction over this matter and the Parties for purposes of enforcing the terms of this Consent Order.

IT IS SO ORDERED this 13 day of January, 2020.

  
\_\_\_\_\_  
THOMAS W. THRASH, JR.  
United States District Judge