CONSENT ORDER

The purpose of this Consent Order (ORDER) is to require certain corrective actions in response to criticisms noted in the Multi-State Regulatory Agencies' Examination that are outlined below. The following terms are used in this ORDER:

Company:	Equifax Inc.
Board:	The Board of Directors of Equifax Inc.
Multi-State Regulatory Agencies:	Includes the Alabama State Banking Department, California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York State Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking.

The Company, by and through its duly elected and acting Board, has consented to the issuance of this ORDER without admitting or denying any charges of unsafe or unsound information security practices.

NOW, THEREFORE, The Multi-State Regulatory Agencies, acting under statutory authority and with consent of the Company, hereby order that the undersigned representatives take, on behalf of the Company, the following steps in furtherance of alleviating the regulatory concerns of the Multi-State Regulatory Agencies.

INFORMATION SECURITY

1) Within 90 days from the effective date of this ORDER, the Board shall review and approve the written risk assessment that identifies:

   (a) foreseeable threats and vulnerabilities to the confidentiality of personally identifiable information (PII)[1];

   (b) the likelihood of threats;

   (c) the potential damage to the Company's business operations; and

   (d) the safeguards and mitigating controls that address each threat and vulnerability.

[1] "PII" shall mean as defined in 23 NYCRR 500.01(g)(2).

AUDIT

2) Within 30 days from the effective date of this ORDER, the Board or Audit Committee shall improve the oversight of the Audit function. Accordingly, the Audit Committee must oversee the establishment of a formal and documented Internal Audit Program that is capable of effectively evaluating IT controls and that complies with the Internal Audit Charter, which requires compliance with International Standards for the Professional Practice of Internal Auditing. The program must document and include:

(a) A defined audit universe, covering all auditable areas, and formal risk analysis process that is used to set the scope and frequency of the IT audits;

(b) An audit schedule that is prepared on a multi-year basis to ensure that critical, high- and medium-risk areas are audited with an appropriate frequency;

(c) Audit of critical and high-risk areas at least annually;

(d) Presentation of an issue tracking report and an issue aging report, containing all open issues, to the Audit Committee on at least a quarterly basis;

(e) Audit Committee monitoring of all findings identified by Internal Audit, regulators, and third party consultants that the Company retained to advise on breach remediation efforts until the issues are resolved;

(f) Validation by Internal Audit that critical, high-risk and medium-risk issues have been resolved on a timely basis; and

(g) Guidelines for ensuring that Internal Audit is not involved in the daily operations of the Enterprise Risk Management process.

BOARD AND MANAGEMENT OVERSIGHT

3) Within 90 days from the effective date of this ORDER, the Company shall improve the oversight of the Information Security Program. Accordingly, the Board or, if appropriately authorized, the Technology Committee of the Board (TC) shall:

(a) Approve a consolidated written Information Security Program and Information Security Policy and annually thereafter;

(b) Review an annual report from management on the adequacy of the Company's Information Security Program;

(c) Enhance the level of detail within the TC and Board minutes, or respective meeting package, by documenting relevant internal management reports (i.e. approval of a formal, written information security risk assessment). Reports to be reviewed should be documented in policy or charter document as appropriate;

(d) Review and approve the following IT and information security policies and ensure they are up-to-date and applicable:

a. the Data Classification and Handling Standard;

b. the End-User Security Policy;

c. the Enterprise Identity and Access Management process; and

d. by December 31, 2018, all other IT and information security policies.

(e) Ensure that the Security Incident Handling Procedure Guide includes up-to-date incident related procedures and clarifies the roles and relationships of the groups involved with incident response, especially:

a. Cyber Threat Center;

b. Fusion Center for physical and environmental events;

c. Network Operations Center for network and server operational events;

d. Security Operations Center for security monitoring and security incident detection; and

e. Security Incident Response Team.

VENDOR MANAGEMENT

4) Within 90 days from the effective date of this ORDER, the Company must improve oversight and documentation of critical vendors and ensure that sufficient controls are developed to safeguard information, consistent with guidance provided in both the FFIEC's "Outsourcing Technology Services" IT Examination Handbook, as further described below, and in the Payment Card Industry Data Security Standards (PCI DSS). Accordingly, the Board or TC must:

(a) Monitor management's documentation of its efforts to comply with PCI DSS;

(b) Review and approve all policies and procedures related to Outsourcing Technology Services/Vendor Management[2] and ensure they incorporate provisions regarding oversight and controls of critical third-party service providers. In addition, interrelated policies should be cross-referenced;

(c) Oversee management's development of a definition of "cloud service" for policies related to cloud-based services;

(d) Oversee management's development of policies that provide guidance for when the use of cloud-based services is permissible and the types of cloud services that are acceptable.

a. The definition and guidance should address security standards, service level agreements, and integration/linking with company systems and networks; and

b. If acceptable cloud services involve PCI data and/or PII, management must ensure appropriate levels of security and encryption are defined within the policy(s) for data at rest and in transit.

PATCH MANAGEMENT

5) The Company must improve standards and controls for supporting the patch management function, consistent with guidance provided in the FFIEC's "Information Security" IT Examination Handbook, within 90 days from the effective date of this ORDER, unless stated otherwise. An effective patch management program must be implemented to reduce the number of unpatched systems and instances of extended patching time frames. Accordingly, the Board or TC is expected to oversee the Company's efforts to:

(a) Identify and document a comprehensive IT asset inventory that includes hardware (including infrastructure devices), software (including applications and operating systems), and location of the assets;

(b) Formalize a process that can routinely identify what patches need to be updated and installed;

(c) Develop an action plan for decommissioning legacy systems, which includes compensating controls until the systems are removed and providing status update reports to the Board or the TC;

(d) Formalize the Patch Management Policy to reflect the personnel and procedural changes supporting the Company's current patch management

[2] This means, specifically, the Third Party Compliance Policy and the External Party Information Security Policy.

initiatives. The Board must oversee management's efforts to apply patch management procedures consistently throughout the Company;

(e) By December 31, 2018, ensure the process described in 5(b) is implemented;

(f) By December 31, 2018, populate with current metrics and data the dynamic patch dashboard that is being implemented;

(g) By December 31, 2018, prioritize and address any outstanding critical, high- and medium-risk patch management audit findings;

(h) By December 31, 2018 provide programmers job-specific training covering secure coding; and

(i) By December 31, 2018, conclude the process of removing system access of development staff (programmers) to the production environment, or implement compensating controls.

INFORMATION TECHNOLOGY OPERATIONS

6) The Company must enhance oversight of IT operations as it relates to disaster recovery and business continuity function within 90 days from the effective date of this ORDER, unless stated otherwise. Accordingly, the Board, or if appropriately authorized, an appropriate committee of the Board, shall oversee the Company's efforts to:

(a) Ensure that key processes of the business continuity plan are independently reviewed by Internal Audit at least annually; and

(b) Formalize emergency change standards and ensure they are expanded to provide for quick changes that are implemented in a well-controlled manner.

VALIDATION

7) By July 31, 2018, the Board or TC shall submit to the Multi-State Regulatory Agencies for review a list of all remediation projects planned, in process or implemented in response to the 2017 breach, along with the Company's prioritization of those projects. These projects will be designed to include developing a strategy for network segmentation, enhancing controls for protecting PII, and appropriately addressing the recommendations noted in the report of the third-party forensic firm that investigated the breach. Further, the Board or TC shall require management to have an independent party (which may be the Company's Internal Audit function) to test controls relating to all such remediation projects and report to the Multi-State Agencies whether such controls are functioning effectively by December 31, 2018.

PROGRESS REPORTS

8) The Board shall provide written reports to the Multi-State Regulatory Agencies outlining its progress toward complying with each provision of this ORDER and make such reports a part of the Board minutes. The Board shall provide these reports within 30 days after each calendar quarter end, with the first report due by July 31, 2018. Correspondence to the Multi-State Regulatory Agencies should be sent to Commissioner Charles G. Cooper, Texas Department of Banking, 2601 N. Lamar Blvd., Austin, Texas, 78705.

ADDITIONAL PROVISIONS

9) This ORDER is effective on the date of issuance, and will remain effective and enforceable except to the extent that, and until such time as, any provision or the ORDER itself has been modified, terminated, suspended, or set aside in writing by the Multi-State Regulatory Agencies. The provisions of this ORDER shall be binding upon the Company and any successors and assigns thereof.

10) The provisions of this ORDER do not bar, estop, or otherwise prevent any of the Multi-State Regulatory Agencies or any other federal or state agency or department from taking any other action against the Company that is authorized by law.

11) Except with regard to the enforcement of this ORDER, the Company's consent to the provisions of this ORDER does not bar, estop, waive, or otherwise prevent the Company from raising any defenses to any action taken by any federal or state agency or department, or any private action against the Company. In addition, this ORDER is intended to apply to those Equifax businesses that serve U.S. business and consumer customers or that hold U.S. consumer PII.

12) To facilitate execution, this ORDER may be executed by the parties in as many counterparts as may be convenient or required. It shall not be necessary that the signature of each party, or that the signature of all persons required to bind any party, appear on each counterpart. All counterparts shall collectively constitute a single instrument.

This ORDER is issued to be effective on June 25, 2018.

/s/ Mike Hill
Mike Hill
Superintendent of Banks
Alabama State Banking Department

/s/ Jan Lynn Owen
Jan Lynn Owen
Commissioner
California Department of Business Oversight

/s/ Kevin Hagler
Kevin Hagler
Commissioner
Georgia Department of Banking & Finance

/s/ Will Lund
Will Lund
Superintendent
Maine Bureau of Consumer Credit Protection

/s/ Terence McGinnis
Terence McGinnis
Commissioner
Massachusetts Division of Banks

/s/ Maria Vullo
Maria Vullo
Superintendent
New York State Department of Financial Services

/s/ Ray Grace
Ray Grace
Commissioner
North Carolina Office of Commissioner of Banks

/s/ Charles G. Cooper
Charles G. Cooper
Commissioner
Texas Department of Banking

Equifax Inc.

In their capacity as directors of the Company, the undersigned hereby accept and agree to the provisions of this ORDER on behalf of the Company:

/s/ Mark W. Begor	/s/ Mark L. Feidler
Mark. W. Begor	Mark. L. Feidler
/s/ Thomas Hough	/s/ Robert D. Marcus
G. Thomas Hough	Robert D. Marcus
/s/ Siri S. Marshall	/s/ Scott A. McGregor
Siri S. Marshall	Scott A. McGregor
/s/ John A. McKinley	/s/ Robert W. Selander
John A. McKinley	Robert W. Selander
/s/ Elane B. Stock	/s/ Mark B. Templeton
Elane B. Stock	Mark. B. Templeton