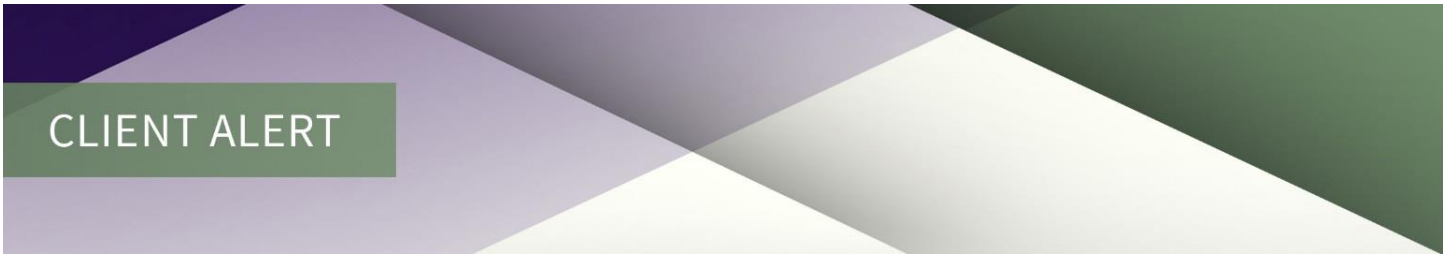
WILLKIE FARR & GALLAGHER LLP



Equifax Data Breach Consent Order Outlines Financial Regulators' Information Security Expectations

June 29, 2018

AUTHORS

Daniel K. Alvarez | Elizabeth J. Bower

On June 25, Equifax Inc., one of the three largest consumer credit reporting agencies, agreed to undertake a series of corrective actions to address financial regulators' concerns over Equifax's information security posture in light of its 2017 data breach that compromised the personal information of more than 140 million people. The agreement came in the form of a Consent Order between Equifax and financial regulators in eight states ("State Regulators"), led by the New York Department of Financial Services ("NYDFS").

The Consent Order confirms that NYDFS is prepared to enforce its new and rigorous Cyber Regulation,[1] as the Consent Order closely tracks the Cyber Regulation's information security compliance and reporting regime. The Consent Order identifies specific actions Equifax must take and, importantly, who within the company the State Regulators expect to take the specific steps. The Consent Order explicitly places accountability for these corrective actions with the Board of Directors (the "Board"). Equifax has just 90 days to improve its information-security defense systems and 30 days to create an internal auditing program. The key corrective actions include:

- **Information Security**: The Board must review and approve a **written risk assessment** to identify and evaluate the foreseeable vulnerabilities that threaten to compromise the confidentiality of personally identifiable

[1] Codified at 23 NYCRR § 500, NYDFS Cybersecurity Requirements for Financial Services Companies took effect March 1, 2017, with initial annual reporting obligations commencing February 15, 2018. For a more detailed discussion of the NYDFS Cyber Regulation, see our prior Client Alert.

information. The risk assessment must further identify the safeguards and controls in place to mitigate each threat and vulnerability.

- **Board and Management Oversight**: Equifax must improve the oversight of its **Information Security Program**. Under the new Program, the Board must review and approve the following information security policies:
    - Data Classification and Handling Standard;
    - End-User Policy;
    - Enterprise and Identity and Access Management process; and
    - all other IT and information security policies.

  Equifax must also ensure that its Security Incident Handling Procedure Guide includes up-to-date incident-related procedures and clarifies the roles and relationships of the groups involved in any incident response. The Board may delegate oversight of these corrective actions to the Technology Committee of the Board.

- **Vendor Management**: Equifax must better oversee and document its relationship with critical vendors, including outsourced technology services. The Board (or its Technology Committee) must develop controls that are consistent with the guidelines provided in both the Federal Financial Institutions Examination Council ("FFIEC") handbook entitled *Outsourcing Technology Services* and the Payment Card Industry Data Security Standards to better safeguard confidential information.

- **Patch Management**: Equifax must improve its software patch management system and develop a formal Patch Management Policy. The Policy must reduce the number of unpatched systems and minimize delayed patching. Equifax is expected to implement standards that are consistent with the FFIEC handbook entitled *Information Security*. Specifically, Equifax must develop:
    - a comprehensive IT asset inventory, which includes hardware, software, and asset location;
    - a formalized process to routinely identify what patches need to be updated and installed; and
    - an action plan for decommissioning legacy systems.

  The Board (or its Technology Committee) is expected to oversee these efforts.

- **Information Technology Operations**: The Board must enhance oversight of the company's IT operations to align with disaster recovery and business continuity plans.

- **Audit**: The Audit Committee of the Board is charged with overseeing the establishment of a robust Internal Audit Program, capable of effectively evaluating IT controls and ensuring timely remediation of critical risks. The Program must comply with Equifax's Internal Audit Charter based on the International Standards for the Practice of Internal Auditing. The Consent Order directs that this Internal Audit function be independent of the Enterprise Risk Management process.

Equifax must provide quarterly progress reports to the State Regulators, beginning July 31, 2018, updating them on remediation efforts taken as a result of the 2017 data breach and its compliance with the Consent Order.

The Consent Order does not impose any fines or penalties. However, its stringent requirements and imposition of Board-level responsibility confirm that the State Regulators are serious about holding financial services companies accountable for protecting the confidentiality of consumers' financial information. As the first information security enforcement proceeding since the NYDFS Cyber Regulation went into effect, the Consent Order provides a road map for the data protection standards state financial regulators are likely to impose on businesses to ensure better management of their cyber risks.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth J. Bower
202 303 1252
ebower@willkie.com

Copyright © 2018 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com