

Lessons From Equifax on How to Mitigate Post-Breach Legal Liability

September 11, 2019 | Articles & Books

On July 22, 2019, the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB) and 50 state and territorial attorneys general settled their claims against Equifax Inc. related to a massive 2017 breach of Equifax data. That settlement also resolves hundreds of civil consumer-fraud class actions brought against Equifax, but it does not address a securities-fraud class action that Equifax's shareholders brought against the company in the wake of the breach, which could still result in significant recovery for Equifax shareholders.

The Equifax settlement and the progress of the securities-fraud class action are instructive as to how civil and regulatory liability will play out for companies imperiled by large cyber events. Aside from loss of consumer and employee confidence, reputational damage and other losses resulting directly from a successful cyber attack, there are three large buckets of legal liability that companies face: (1) federal and state regulators, (2) classes of consumers and (3) classes of shareholders (for public companies).

This article analyzes the Equifax decision and uses lessons from that case to examine strategies for minimizing risk of securities fraud class actions arising from data breaches.

Related materials

[lessonsfromequifax_cslr_reprint.pdf](#)