On the WLF Legal Pulse

Timely commentary from WLF's blog

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

August 7, 2019

Taking Stock of FTC Cybersecurity Enforcement after the Equifax Settlement

by M. Sean Royall, Richard H. Cunningham, and Bennett Rawicki

If the Northern District of Georgia approves its proposed settlement with the Federal Trade Commission, Equifax will pay at least $575 million to resolve allegations that its cybersecurity measures violated Section 5 of the FTC Act in the wake of one of the most significant data breaches on record. The settlement reflects that the agency remains committed to enforcing the Federal Trade Commission Act in the context of commercial data breaches, and entering into consent order settlements, notwithstanding that the Eleventh Circuit last year in *LabMD v. FTC* rejected an FTC consent order as being unenforceably vague.

Equifax Data Breach Settlement

On July 22, 2019, the FTC announced that Equifax had agreed to settle suits brought by the FTC, a consolidated class of consumers, the Consumer Financial Protection Bureau ("CFPB"), and 48 states, Puerto Rico, and the District of Columbia. Lawsuits filed by Indiana and Massachusetts remain unresolved.

As a result of the settlement, the FTC projects Equifax will pay between $575 million and $700 million: (i) at least $300 million to a fund for consumers affected by the breach (and up to an additional $125 million more); (ii) $175 million to the states and territories that were party to the settlement; and (iii) $100 million in penalties to the CFPB.

The settlement amount is the largest FTC cybersecurity remedy to date, and undoubtedly this is due in significant part to the seriousness of the data breach. The FTC's complaint alleges that, for three months in mid-2017, hackers exploited vulnerabilities in Equifax's cybersecurity to steal sensitive personal information of more than 145 million individuals, including names, dates of birth, social security numbers, and payment card numbers. Moreover, Equifax allegedly received an alert about a new critical threat two months before the breach. According to the FTC, Equifax ran an automated scan to identify gaps within its network, but the scan overlooked key vulnerabilities, and hackers had been stealing data for three months before Equifax detected suspicious traffic. The FTC also alleges that Equifax did not announce the data breach until September 2017, several more months after detecting the anomalous activity on its systems.

M. Sean Royall and **Richard H. Cunningham** are Partners with Gibson, Dunn & Crutcher LLP, and **Bennett Rawicki** is an associate with the firm. The authors would like to thank **Bryan Sohn**, summer associate, with Gibson Dunn for his contributions to this article.

The complaint faulted Equifax for numerous security failures, including:

- Failing to patch the vulnerability detected two months prior to the hack, which allowed the hack to occur;
- Storing administrative log-in credentials, and personal information of more than 145 million individuals, in unencrypted text;
- Failing to segment the database servers containing personal information, which allowed hackers to move more easily through Equifax's network;
- Failing to implement sufficient protections to detect the hack; and
- Failing to provide adequate cybersecurity training to employees.

Compl. at 8-14.

In addition to the monetary remedy, as part of the settlement, Equifax is required to maintain a comprehensive information security program for twenty years. The prescribed program requires, among other things, annual assessments of security risks and written documentation of those risks and the safeguards Equifax designs and implements to control for them. Equifax must also obtain initial and biennial assessments of its information security program, submit timely reports to the FTC of future data breaches, and provide the FTC with an annual certification from the board of directors or senior company officer stating that Equifax has complied with the information security program.

Taking Stock of the FTC's Post-*LabMD* Approach to Cybersecurity Enforcement

In June 2018, the Eleventh Circuit vacated an FTC cybersecurity consent order in *LabMD, Inc. v. FTC*. The Commission had found that LabMD's "data security practices were unfair under Section 5" and ordered LabMD to implement and maintain a data security program "reasonably designed" to protect the security of personal information. *LabMD* at 7 & App'x § I. As noted previously on this blog, the *LabMD* court held the FTC's order unenforceable because enforcing an order requires clear and convincing evidence that the defendant violated the order, and the "reasonableness" standard used in the FTC's order was too vague for the FTC ever to be able to prove that a practice was unreasonable by clear and convincing evidence. *LabMD* at 28-29.

That decision also called into question the FTC's interpretation of what constitutes "unfair" data security practices under Section 5 of the FTC Act. The FTC had argued in *LabMD* that the Commission need only show that the challenged conduct satisfies Section 5(n) in order to prove "unfair" conduct., Section 5(n) prohibits the FTC from finding conduct unfair unless it causes substantial injury that was not reasonably avoidable by consumers or outweighed by countervailing benefits. The Eleventh Circuit expressly rejected the FTC's position, explaining that "[t]he act or practice alleged to have caused the injury must still be unfair under a well-established legal standard, whether grounded in statute, the common law, or the Constitution." *LabMD* at 13, n.24. The court presumed that the "well-established legal standard" for determining whether data security practices were unfair "is the common law of negligence." *Id.* at 16-17. The FTC has not litigated this issue in another matter to date, and the *Equifax* litigation is unlikely to yield a judicial decision addressing this issue given that the parties are jointly proposing the settlement to the court.

Since *LabMD*, the FTC has not pulled back from bringing cases challenging cybersecurity practices it views as inadequate under Section 5. Instead, the FTC has pursued seven enforcement actions that mandated information security programs. And the *Equifax* matter and the recent

proposed $5 billion settlement with Facebook reflect that the agency is now ratcheting up the monetary component of its settlement demands.

One clear change, however, in the agency's post-*LabMD* practices is the notable removal of the word "reasonable" in the provisions of its cybersecurity consent orders. Most of the FTC's post-*LabMD* orders in this area require the respondent to maintain an information security program "that is designed" to protect the security of personal information, rather than "reasonably designed" to do so. *See Equifax*; *Facebook*; *D-Link*; *ClixSense.com*; and *Unixiz*.

How the FTC will police this standard in practice remains to be seen, but the current language is arguably more lenient to companies than the "reasonableness" requirement that the FTC used before *LabMD*. Although the orders pre- and post-*LabMD* prescribe similar detail for the information security program—such as assessing and documenting cybersecurity risks and the safeguards implemented to control those risks—now the orders say only that such programs must be designed to protect security, not *reasonably* designed to protect security. Thus, post-*LabMD*, a company can defend against claims it violated a consent order by arguing that it designed an information-security program that included the FTC-prescribed criteria, without further consideration of whether the company's design was "reasonable."

At the same time, if a company's design of its information security program were shown by a breach (or otherwise) to be so ineffective as being tantamount to negligence, we strongly suspect that the FTC would take the position that the program was not "designed" to protect sensitive data, and the FTC, in addition to pursuing *de novo* Section 5 claims, could bring an action alleging that the program constituted unfair cybersecurity practices under the order.

