LabMD Beats FTC in Cybersecurity Appeal – What's Next for "Reasonableness"-Based Enforcement Cases?

June 26, 2018

One of the longest-running legal sagas in cybersecurity has ended, at least for now: the Eleventh Circuit Court of Appeals rejected the Federal Trade Commission's ("FTC") cease and desist order requiring LabMD to implement "reasonable" cybersecurity practices because it lacked the necessary specificity to permit court enforcement. The decision takes a scalpel to the FTC's cybersecurity authority, but not the ax that some had expected. It portends modest yet meaningful limits on the FTC's enforcement authority both in cybersecurity and, potentially, in other areas such as false advertising.

What happened? The case dates back to 2005, when a LabMD billing manager installed a peer-to-peer file-sharing application on her work computer, inadvertently making some medical records available online. The FTC challenged LabMD's allegedly poor cybersecurity practices as unfair in violation of Section 5 of the Federal Trade Commission Act ("FTC Act").

LabMD proved to be the unusual company that fought the FTC rather than settling. At the agency level, the FTC imposed a cease and desist order requiring LabMD to have "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." LabMD appealed.

In an interim ruling in 2016, the Eleventh Circuit stayed the FTC order—questioning whether, as a matter of law, any unfair business practice could occur without better proof of consumer harm. (The patient records were exposed, but the FTC lacked evidence of actual misuse.) In the final ruling, the Eleventh Circuit vacated the FTC order because "it does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data security program and says precious little about how this is to be accomplished."

Notably, the Eleventh Circuit stated that the *prohibitions* contained in an FTC cease and desist order must be specific—stated with clarity and precision. The LabMD order did not contain any prohibitions, only general directives to implement reasonable cybersecurity practices. The Court found that these order provisions were too ambiguous and therefore unenforceable.

Key Takeaways. After this long-awaited decision, what has changed and what has not?

- The FTC's basic authority to bring enforcement actions for "unreasonably" lax data security practices under the unfairness prong of Section 5 remains debatable but was not overturned by the Eleventh Circuit. This authority was specifically affirmed by the Third Circuit in the much-discussed Wyndham Hotels case. The Eleventh Circuit here sidestepped the issue. Rather, it assumed the FTC has authority to deem unreasonably poor security an unfair business practice, and instead focused on limitations associated with the FTC's injunctive remedies.

- Likewise, the court chose not to adopt a stringent requirement of substantial actual harm, which had been suggested in the interim decision. Proof of actual harm is often hard to come by in data breaches. Such a requirement thus would sharply reduce the number of cases in which the FTC could invoke its unfairness authority.

- For companies confronting a particular FTC enforcement action based upon a data breach or cybersecurity practices, there is now a clear new limit on remedies: the injunctive provisions in future FTC orders (whether imposed by the Commission or a court, or agreed to by settlement) will have to be more detailed about what amounts to "reasonable" security. Orders may also have to be more closely tied to the particular security practices at issue in a given case and may need to be drafted as "prohibitions." Time will tell how much detail, and how close a tie, are needed to pass legal muster. Many companies are under existing FTC settlement orders—most of which include similar requirements and many of which are applicable for periods up to 20 years (or longer). In the event that the FTC alleges that a company has violated one of these orders, that company may now have a basis to argue that portions of the order are unenforceable.

- Companies facing FTC false advertising challenges may also be able to use the *LabMD* decision to their benefit. When the FTC resolves a case based on allegedly false advertising, its orders frequently require a "reasonable basis" and "competent and reliable scientific evidence" in support of future claims. Arguably, that approach has many of the same weaknesses identified by the Eleventh Circuit related to ambiguity and lack of precision. The FTC may contend that its approach in advertising cases is more defensible because the meaning of these terms has become well settled across decades of enforcement matters. A "reasonableness" standard in cybersecurity is both newer and arguably more dynamic, and therefore harder for a court to enforce. Thus, it is uncertain whether the Eleventh Circuit *LabMD* decision will limit the FTC's remedial authority outside the cybersecurity realm.

- "Reasonable" security remains the basic legal standard for planning or assessing a corporate cybersecurity program. The Eleventh Circuit avoided a frontal attack on

the reasonableness standard, and more than a dozen states, notably including California, have enacted laws that require "reasonable" cybersecurity. Like the FTC, these state legislatures have not decreed specific benchmarks for what is reasonable (though California's attorney general has pointed to the Center for Internet Security's 20 Critical Security Controls.) Some courts also have let negligence-based challenges survive motions to dismiss in post-breach class action lawsuits.

Companies seeking legal compliance thus are still well-advised to adjust their cybersecurity practices, evaluating the latest best-practice responses and adopting them in a risk-based manner as the threat landscape evolves.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Paul D. Rubin
pdrubin@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Monisola Salaam
msalaam@debevoise.com