wiley

ALERT

FTC Rebuked in LabMD Case: What's Next for Data Security?

June 7, 2018

On June 6, the U.S. Court of Appeals for the Eleventh Circuit decided the long-awaited LabMD saga. As Wiley Rein attorneys recently explained in a webinar on agency priorities, this case is an important milestone and inflection point for the new Federal Trade Commission (FTC) leadership. The FTC's authority and role in data security has been key to ongoing debates over federal privacy and security policy domestically and globally. This case raised issues going to FTC power and practice, but ultimately turned on the remedy imposed by the agency which was found to be so vague as to be unenforceable. The court did not address the key substantive questions:

- First, in a data breach case, what type of consumer injury gives rise to "unfairness" under Section 5 of the FTC Act, an issue sometimes identified as the "informational injury" question?
- Second what type of notice is the FTC required to provide regarding reasonable data security measures?

Despite its failure to answer these questions, the decision has implications for those issues and the agency's overall approach to data security. In particular the Eleventh Circuit's decision was a rebuke to the agency's remedial efforts, which lean heavily on consent decrees to prod action the agency could not otherwise mandate.

The Court found that the FTC's cease and desist order "mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished." According to three appeals court judges, "[t]his is a scheme that Congress could not have envisioned."

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Scott D. Delacourt
Partner
202.719.7459
sdelacourt@wiley.law

Practice Areas

FTC Regulation

Telecom, Media & Technology

How did we get here?

LabMD was a cancer detection facility that had personal information regarding its patients. Some of that informative was stored on a workstation where an employee was using peer-to-peer file-sharing application called LimeWire, contrary to LabMD policy. This inadvertently made information on the workstation accessible to third parties. A firm called Tiversa – which was either a security firm or a hacker depending on your perspective, accessed a document containing sensitive information of around 9000 patients. After unsuccessfully seeking to be hired by LabMD, in 2009, Tiversa arranged for the delivery of the 1718 File to the FTC which commenced an investigation.

Notably, it was never shown that anyone other than Tiversa accessed the data or that any misuse was made of the data. The FTC investigated and brought administrative complaint asserting that LabMD's data security practices were unreasonably lax and therefore "unfair" under Section 5 of the FTC which prohibits "Unfair acts or practices that **cause** or are **likely to cause** substantial injury to consumers."

The Commission rejected LabMD's substantive and procedural objections. Indeed, after the ALJ originally dismissed the complaint, the Commission reversed the ALJ's decision, finding that LabMD "failed to implement reasonable security measures to protect the sensitive consumer information on its computer network" and thus that its practices were unfair under Section 5. The FTC entered an order vacating the ALJ's decision and enjoining LabMD to install a data-security program that comported with the FTC's standard of reasonableness.

LabMD sought judicial review and asked the Eleventh Circuit to vacate the order, arguing that the order is unenforceable because it does not direct LabMD to cease committing an unfair act or practice within the meaning of Section 5(a). The Eleventh Circuit agreed and vacated the Order.

The case attracted interest from amici all across industry who backed LabMD's view, arguing that they need a better idea of what they need to do in terms of security to stay of the right side of the FTC.

What did the Eleventh Circuit decide?

The Eleventh Circuit saw the FTC's approach as overreach. The FTC could have rested on the failure of LabMD to prevent the unauthorized installation of the filesharing software. "Had the complaint stopped there, a narrowly drawn and easily enforceable order might have followed, commanding LabMD to eliminate the possibility that employees could install unauthorized programs on their computers." The Eleventh Circuit, with some seeming dismay, noted that "the complaint continues past this single allegation of wrongdoing" and lists a litany of practices that it claims fail to provide reasonable and appropriate security. It is here that the FTC lost the Court. Unfortunately for the FTC, "the complaint alleges no specific unfair acts or practices engaged in by LabMD. Rather, it was LabMD's multiple, unspecified failures" that gave rise to a Section 5 problem.

The Eleventh Circuit invokes negligence to animate the FTC's theory:

"The Commission's decision in this case does not explicitly cite the source of the standard of unfairness it used in holding that LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice. It is apparent to us, though, that the source is the common law of negligence."

The Eleventh Circuit cites the Restatement of Torts, among other sources, and assumes "arguendo" that "the Commission is correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice." While that is not the outcome many were hoping for, having so assumed, the Eleventh Circuit finds that the FTC's "cease and desist order, founded upon LabMD's general negligent failure to act" is not enforceable.

Why? The Court examined in detail the remedial measures and procedural options available to the FTC, and found that the cease and desist order, not being tied to any specific violation or behavior was void.

"the cease and desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable."

What is Next for the FTC?

Though LabMD has since ceased operations, the decision has implications far beyond the day-to-day data security decisions of health sector companies and providers. The decision—and its silences—will inform calls for federal data breach legislation, national privacy policy, and international debates over consumer privacy and data security. Each of these issues will be addressed by a new FTC, populated by some new Commissioners and staff that are generally expert in competition policy but relatively unfamiliar with these issues.

This decision could affect a variety of issues that touch the FTC and the private sector:

- **Harmonization with non-U.S. approaches**. The FTC is the leading consumer protection agency in the United States, but its actions are sometimes judged inadequate by other countries who take a more regulatory approach than the United States. Some call for the United States to emulate Europe in its approach to consumer privacy. The new FTC leadership will have to develop positions, defend U.S. approaches, and explain how this decision does not curtail its power to police business practices for unfair and unreasonable practices that could harm consumers.
- **Regulatory power**. Some have long called for the FTC to have rulemaking power and to set general, affirmative policies on data security. Will this decision increase calls for FTC to have direct regulatory and rulemaking power over consumer privacy and security interests? Note that the current FTC, unlike its predecessor, is likely loathe to have such powers. Prospectively defining reasonable data security standards in precise technical terms is an unenviable task given the pace of innovation.

- **Federal data breach and privacy legislation**. Many remain frustrated that the federal government has not adopted a uniform approach to federal data security and breaches, but the political stakes remain challenging so long as the states insist on an independent and strong enforcement role. Will this decision provide fuel to those to promote a national privacy regime that is enforceable by the FTC and has a clearer Congressional mandate than Section 5?
- **FTC enforcement philosophy**. Many are looking at how the FTC will prioritize cases in a high tech era, and what remedial tools it will use. Will this decision trim the sails of FTC enforcement actions, namely the 60+ consent decrees that the agency touts as providing ample notice to the private sector of what is expected to comply with Section 5?
- **State activity.** Will politicians looking to bolster state privacy and cybersecurity legislation seize this decision as a reason to encourage state by state activity to fill perceived gaps?
- **Informational injury**. The FTC has been looking at what sort of non-economic informational injury should be legally cognizable. This decision avoided that issue, but the FTC cannot. What will come of the agency's efforts to bring rigor to this inquiry and provide expert guidance to other agencies and courts about federal privacy policy?

The FTC will now face the decision of whether to appeal the 11th Circuit's decision. In light of the narrow scope of the 11th Circuit's holding, such further appeal may be unattractive to the FTC.