ROPES & GRAY

ALERT

Privacy & Cybersecurity

June 7, 2018

Eleventh Circuit Vacates FTC Cybersecurity Order against LabMD

Attorneys
Douglas H. Meal
Douglas Hallward-Driemeier
Michelle Visser
Deborah L. Gersh
David T. Cohen
Heather Egan Sussman
James S. DeGraw
Seth C. Harrington
Mark P. Szpak

On June 6, 2018, at the urging of Ropes & Gray, the U.S. Court of Appeals for the Eleventh Circuit vacated an order that the Federal Trade Commission (the "FTC") had imposed on LabMD, Inc. ("LabMD") to overhaul the cancer detection laboratory's data security program. The court ruled that the FTC's order is unenforceable because, rather than enjoining a specific act or practice, it mandates a complete overhaul of LabMD's data security program and says little about how this is to be accomplished, effectively charging a district court with managing the overhaul. The decision also recognizes important limitations on the agency's authority even to declare an act "unfair" in the first place. The Eleventh Circuit's rejection of the FTC's action against LabMD has significant implications both for the FTC's privacy and data security program and for other regulatory and private litigation contexts.

The LabMD Case

The origins of the LabMD matter date back more than a decade. In 2008, Tiversa Holding Corporation ("Tiversa") took from LabMD a file containing a limited amount of personal information of approximately 9,300 patients by exploiting a vulnerability in a peer-to-peer file-sharing application that, contrary to LabMD policy, was installed on one of LabMD's workstations. After LabMD rebuffed Tiversa's attempt to sell the laboratory its purported remediation services and instead remediated the vulnerability on its own, Tiversa turned over the file to the FTC.

Following an extensive investigation, on August 28, 2013, the FTC initiated enforcement proceedings against LabMD. The FTC's administrative complaint (the "Complaint") alleged that LabMD's data security practices were "unfair" in violation of Section 5 of the FTC Act because, "taken together," they "failed to provide reasonable and appropriate security for personal information on its computer networks."

An administrative law judge dismissed the Complaint but the FTC reversed on appeal, holding, as the Complaint charged, that LabMD's data security practices constituted an unfair act or practice in violation of Section 5 of the FTC Act. The FTC concurrently issued an order requiring LabMD to undertake various affirmative actions, such as establishing and maintaining a reasonable and comprehensive information security program (the "Order"). LabMD then retained Ropes & Gray to petition the Eleventh Circuit for review, seeking to have the Order vacated.

The Eleventh Circuit's Decision

In a unanimous opinion, the Eleventh Circuit agreed with and adopted LabMD's argument that the FTC's Order is unenforceable. The court reasoned that the remedy that the FTC seeks "must comport with th[e] requirement of reasonable definiteness." In that regard, the court held that a fundamental flaw with the Order entered against LabMD is that it "does not instruct LabMD to stop committing a specific act or practice." The FTC did not seek to address the one-off vulnerability of the patient file through a narrowly drawn, easily enforceable order, such as one commanding LabMD to eliminate the possibility that employees could install unauthorized programs. Instead, the Order mandates a complete overhaul of LabMD's data security program and says little about how this is to be

accomplished, effectively charging a district court with managing the overhaul. The Order's command to LabMD to "overhaul and replace its data-security program to meet an indeterminable standard of reasonableness" is, the Eleventh Circuit concluded, unenforceable.

The court also recognized important limitations on the agency's authority to declare an act "unfair" in the first place. The panel stated that an unfair act or practice "is one which meets the consumer-injury factors . . . and is grounded in well-established legal policy." That is, pursuant to Section 5(n) of the FTC Act, the FTC must allege and prove actual or likely substantial injury to consumers that is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits. And in addition, the FTC must also find that "[t]he act or practice alleged to have caused the injury [is] unfair under a well-established legal standard, whether grounded in statute, the common law, or the Constitution." The court thus rejected the FTC's recent position that it may "bring suit purely on the basis of" actual or likely "substantial consumer injury." The court did not need to, and therefore did not, assess the legality of LabMD's data security practices under this standard. But the court called out that LabMD did, in fact, maintain a data-security program that included a compliance program, training, firewalls, network monitoring, password controls, access controls, antivirus, and security-related inspections.

The Eleventh Circuit's decision has significant implications both for the FTC's privacy and data security program and for other regulatory and private litigation contexts, which in many instances borrow from the FTC regime. For more information regarding the impact of the LabMD decision, please feel free to contact a member of the Ropes & Gray team that represented LabMD, which includes privacy & cybersecurity co-head Douglas Meal, partners Doug Hallward-Driemeier, Michelle Visser and Debbie Gersh, and counsel David Cohen. Please also feel free to reach out to any other member of Ropes & Gray's leading privacy & cybersecurity team, including Heather Sussman, Jim DeGraw, Seth Harrington, and Mark Szpak.