WILMERHALE

Eleventh Circuit Concludes FTC Data Security Order Unenforceable Because Standards Not Specific Enough

JUNE 12, 2018

On June 6, the U.S. Court of Appeals for the Eleventh Circuit vacated a cease-and-desist order by the Federal Trade Commission (FTC) issued against LabMD, Inc. (LabMD) arising from an FTC enforcement action alleging that LabMD's data security program was unreasonable and therefore constituted an unfair act or practice under the section 5 of the FTC Act, 15 U.S.C. § 45(a). The court held that the FTC's order had to be invalidated because it failed to direct LabMD to cease committing any specific unfair acts or practices and instead imposed only the general requirement that LabMD maintain a "comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." The court accepted, for purposes of its analysis, 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." But, analogizing to the standards of specificity required for injunctive relief in court, it held that "the prohibitions contained in cease and desist orders . . . must be specific."

Although the court seemed skeptical of the approach taken in the FTC's complaint, which viewed "all of LabMD's data security deficiencies as culminating in a single unfair act or practice," its decision leaves open the door for the FTC to continue using its Section 5 unfairness authority to bring data security enforcement actions. But the court's rejection of a general "reasonableness" standard means that, at least in the 11th Circuit, the FTC will have to define much more precisely the practices it alleges are unfair and their connection to consumer injury.

Background

The FTC alleged that a LabMD employee, in violation of company policy, had installed a peer-to-peer file-sharing application on the employee's computer in 2005, which allowed a third-party data security consulting company to acquire personal information from the company in 2008. Based on information provided to the FTC by the data security consulting company, the FTC issued an administrative complaint in 2013 against LabMD under the unfairness prong of Section 5 of the FTC Act. The FTC's administrative law judge (ALJ) dismissed the complaint in 2015 and concluded that the FTC had failed to allege that there was substantial injury or the likelihood of such for individuals

whose personal information had been exposed. The Commission overturned the ALJ's ruling in 2016, reasoning that the ALJ had applied an unduly stringent substantial injury standard and had failed to recognize that economic and physical harm are not the only forms of cognizable injury. The FTC issued a cease-and-desist order, requiring LabMD to establish a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.

Opinion

The Eleventh Circuit concluded that the FTC's order was unenforceable because "[i]t 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." The court noted that "[b]eing held in contempt and sanctioned pursuant to an insufficiently specific injunction is . . . a denial of due process."

The court held that the FTC's order failed this standard because it called for "vague items" to be included in LabMD's information security program and was "devoid of any meaningful standard informing the court of what constitutes a 'reasonably designed' data security program." The order would thus put the court in the position of managing LabMD's business in accordance with the Commission's wishes in future contempt proceedings to enforce the order.

FTC Reaction

An FTC spokeswoman said in a statement Wednesday that while the Commission was "disappointed by the appeals court's ruling, we will continue to do everything we can to protect consumer privacy." The agency is also "evaluating our next steps in response to this decision," the spokeswoman said.

Conclusion

The Eleventh Circuit's decision calls into question the FTC's ability to rely on a general standard of reasonableness in data security cases alleging unfairness, without more notice of what is and is not "reasonable." Companies facing FTC enforcement actions can now insist that the FTC limit its claims and the terms of any resulting orders to specific practices.