Court Invalidates FTC Enforcement Action Related to Alleged Unfair Data Security Practices

JUNE 12, 2018

On June 6, the US 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.

Read more via our "Eleventh Circuit Concludes FTC Data Security Order Unenforceable Because Standards Not Specific Enough" client alert.