PUBLICATION

FTC Ordered to Testify Regarding Data Security Standards in LabMD Dispute

May 09, 2014

The Federal Trade Commission (FTC) has suffered a significant setback in its ongoing dispute with LabMD, a now-closed medical laboratory that the FTC charged with failing to adopt reasonable data security practices that resulted in the exposure of the data of 10,000 patients in 2010. In a decision that has far-reaching implications for companies caught in the snares of FTC proceedings regarding the adequacy of data security practices, an administrative law judge ruled on May 1, 2014, that the FTC must submit to a deposition and provide testimony regarding the specific data security standards the FTC has published or intends to use at trial to show that LabMD's data security was inadequate.

The FTC charged LabMD with engaging in unfair trade practices in violation of Section 5(a) of the Federal Trade Commission Act by engaging in a number of data security practices that, "taken together, failed to provide reasonable and appropriate security for personal information on LabMD's computer networks," which caused, or are likely to cause, substantial injuries to consumers. The FTC claimed that LabMD, among other things, failed to have a "comprehensive data security program," did not use readily-available measures to identify risks and vulnerabilities on its computer networks, did not use "adequate measures" to prevent employees from accessing personal information, did not maintain or update its computer operating system, and did not employ readily-available measures to prevent or detect unauthorized access to personal information on LabMD's networks.

LabMD answered the FTC's complaint and denied that it had violated the FTC Act or failed to provide reasonable and appropriate security for personal information on its computer networks. LabMD then noticed a deposition of the FTC seeking testimony of, among other things, the "data security standards that have been used by the [FTC] to enforce the law under Section 5 of the Federal Trade Commission Act since 2005." During the deposition, the FTC's counsel instructed the witness not to answer questions about the data security practices allegedly breached by LabMD, but the judge granted LabMD's motion to compel that testimony. While the judge held that the FTC did not have to disclose the legal reasoning behind its decision, the judge found that the data security standards the FTC intended to rely on are "factual matters, well within the scope of permissible discovery," and relevant to LabMD's defense that its data security practices were adequate, as well as its defense that the FTC failed to provide fair notice of the data security standards that LabMD was expected to meet.

The FTC frequently brings enforcement actions against companies for failing to have in place "reasonable" practices to safeguard personal information on their computer networks. Those cases have historically been resolved through consent agreements, with no legal challenge being made to the FTC's authority to bring such actions under Section 5 of the FTC Act, which prohibits "unfair or deceptive" trade practices. However, a federal court recently affirmed the FTC's authority to bring such enforcement actions under Section 5 of the FTC Act in *FTC v. Wyndham Worldwide Corp*.

The deposition of the FTC in the LabMD case is expected to be conducted within 10 days pursuant to the judge's ruling. The testimony should provide important insight into the FTC's decision-making process with respect to the reasonableness of data security practices under Section 5 of the FTC Act. If you have questions about this other data security issues, please contact a member of the Privacy and Information Security Team.