FTC's Data Security Authority Curbed by 11th Circuit

The Federal Trade Commission ("FTC") has long been considered the agency best suited to regulate data security. The Eleventh Circuit dealt a serious setback to that authority yesterday in *LabMD v. FTC*, No. 16-16270, striking down its attempt to subject LabMD to proscriptive future data security measures. With the release of this opinion, companies now have a variety of new tools to push back against FTC enforcement actions and consent decrees.

The LabMD saga begins in 2013, when the FTC filed a complaint against LabMD alleging the company failed to reasonably protect certain data. The FTC noted a specific incident in 2008 wherein a third party illegally obtained data from a LabMD computer using the Limewire peer-to-peer network. The Limewire application had been installed on the computer by a LabMD employee *against company policy*, and was immediately removed by LabMD when it learned of the issue. The FTC, in filing its complaint against LabMD, however, did not allege a specific act or practice of LabMD that allowed the incident to occur. Rather, the FTC set forth a wish-list of data security measures that it alleged LabMD should have implemented, and issued a cease-and-desist order requiring the company to do so.

The Eleventh Circuit rejected the FTC's attempt to regulate prospectively LabMD's data security program through aspirational objectives: "In the case at hand, 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."

The *LabMD* opinion also pushed back against the FTC's heavy reliance on the Third Circuit's 2015 opinion in *FTC v. Wyndham*, No. 14-3514. The *Wyndham* opinion broadly upheld the FTC's authority to regulate companies' data security programs, which was one of the threshold appellate issues asserted as error by LabMD. When Wyndham's challenge to the FTC's authority was rejected by the Third Circuit, it was forced to enter

Related Capabilities

- Privacy & Social Media

into a consent order with the FTC that required Wyndham to establish a robust data security program. The FTC has imposed similar requirements in numerous other consent orders in recent years—the types of requirements which the Eleventh Circuit rejected in *LabMD*.

By narrowly limiting its reversal to the FTC's improper relief, the *LabMD* opinion implicitly calls into question the threshold issue of the extent to which the FTC can enforce its claimed data security authority. *LabMD* rejects the FTC's assertion that it has the authority to intervene when it generally perceives a company to have a deficient data security program and order the company to develop a program to the FTC's satisfaction. Instead, the Court ruled that FTC must act narrowly to remedy specific claimed deficiencies.

The *LabMD* opinion provides companies with at least some opportunity to challenge FTC overreach. Companies will still be expected to manage data efficiently, independently, and responsibly, but will now have some foundation to challenge aspirational, vague standards asserted in ongoing enforcement actions or negotiations with the FTC, and try to limit the FTC's enforcement action to specifically identified data security deficiencies. In light of the tension between the Third and Eleventh Circuit's opinions, the FTC's authority will be closely monitored in the coming months. Stay tuned for further developments.