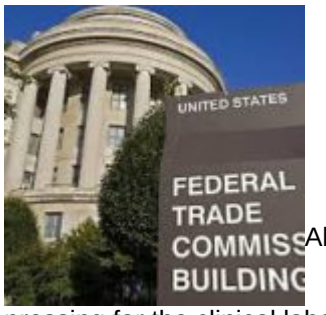
FTC Finds Lab Liable for Unfair Practices, Says It Put Consumers at Risk of Identity Theft



Although a recent decision by the Federal Trade Commission (FTC) is most immediately pressing for the clinical laboratory in question, some say it could directly impact healthcare providers overall in the long run.

The unanimous decision by the FTC commissioners determined that LabMD's security protocol failed to protect sensitive consumer medical information or personal information, thereby leaving people open to the risk of violations of privacy, malicious use of their information, or even identity theft. The decision determined that the lab's failure demonstrated an unfair practice under the FTC Act; it overturns a 2015 ruling by an FTC administrative law judge who was unconvinced that the lab had brought about harm to consumers.

Lab allegedly failed to safeguard sensitive consumer information

Edith Ramirez, FTC chairperson, wrote in this latest opinion: "LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer system." The commissioners decided that the administrative judge had used the incorrect legal standard when considering whether the lab's practices were unfair.

Ramirez noted several key faults in LabMD's behavior regarding data security:

- It failed to utilize a system for detecting intrusions;
- It failed to purge the consumer data it had gathered;
- It failed to monitor traffic that breached its firewalls;
- And it failed to adequately train its employees in data security.

Ramirez stated that those alleged oversights and missteps resulted in the prolonged exposure—of a period of nearly a year—of the medical and/or personal data of more than 9,000 unsuspecting individuals on a peer-to-peer network open to millions of users.

Head of the lab criticizes the FTC's "dirty system," says case has implications for all healthcare providers

Michael Daugherty is CEO of LabMD. He says that the lab was forced to close its doors two years ago (after 18 years in business) as a result of the demands of defending this case. He has announced plans to appeal the decision in federal court and expresses relief at taking the case out of what he calls the Commission's "dirty system."

He sees his case as an industry turning point and predicts a bleak ripple effect for the healthcare system on a wide

scale…if he loses his appeal. Daugherty claims that the FTC had no business in deciding the case but that it should have been the sole purview of the Health and Human Services' (HHS) Office for Civil Rights (OCR) in light of the fact that the OCR typically deals with HIPAA violations.

"If I lose, every healthcare facility in the country loses," Daugherty says. "They're going to push that they've got jurisdiction to come after healthcare facilities without standards, without notice and over and above Health and Human Services. That's terrifying."

The first FTC complaint against LabMD was filed in 2013, citing two breaches that allegedly occurred because of lax security on the lab's part. The first breach, in 2008, allegedly made personal data available on a peer-to-peer file-sharing network. The second, in 2012, was revealed when data originating from the lab was allegedly discovered in individuals' possession—individuals who were later charged with (and pleaded "no contest" to) identity theft.

The chronology of the complaint: sour grapes or appropriate, legal response?

The FTC began its investigation into LabMD's data security practices following notice sent to the FTC by Tiversa, a company specializing in intelligence services. LabMD chronicles the whistle-blowing in this order: Tiversa allegedly discovered a LabMD report (including personal information) on a peer-to-peer file-sharing network; Tiversa approached LabMD and offered its services to repair the security breach; LabMD declined to hire the company; Tiversa notified the FTC about the alleged breach.

Tiversa had this to say on the issue: "We have acted appropriately and legally in every way with respect to LabMD, despite their efforts to besmirch our reputation."

What's next for the defunct lab?

Section 5 of the FTC Act gives the Commission the authority to challenge "unfair or deceptive" practices relating to commerce. Section 5(n) states that an act or practice may be considered unfair if it "causes or is likely to cause substantial injury to consumers."

Now that the Commission has found LabMD liable for unfair data security practices and in violation of the FTC Act, the Commission's Final Order will require the lab to develop a thorough security protocol that protects the consumer data still in its possession. Further, once established, the lab's data security program will be required to undergo ongoing, independent, third-party assessments. LabMD must also inform affected consumers about the unauthorized disclosure of their personal information on the peer-to-peer network, as well as suggestions for how they can protect themselves against identity theft.

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.