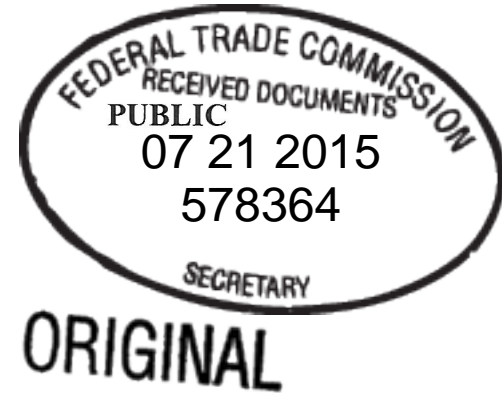


UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
OFFICE OF ADMINISTRATIVE LAW JUDGES



\_\_\_\_\_)  
In the Matter of )  
 )  
LabMD, Inc., )  
a corporation, )  
Respondent. )  
\_\_\_\_\_)

DOCKET NO. 9357

**ORDER DENYING RESPONDENT’S MOTION TO  
DISMISS AT THE CLOSE OF EVIDENCE OFFERED  
IN SUPPORT OF THE COMPLAINT**

**I.**

The Complaint in this matter charges Respondent LabMD, Inc. (“Respondent” or “LabMD”) with one count of unfair trade practices in violation of Section 5 of the Federal Trade Commission (“FTC”) Act. Specifically, the Complaint alleges that Respondent failed to use “reasonable” and “appropriate” data security practices, which practices caused, or are likely to cause, substantial consumer harm that is not reasonably avoidable by consumers or outweighed by countervailing competitive benefits. The Complaint further alleges that, no later than 2006, a LabMD billing manager downloaded and installed the “Limewire” peer-to-peer (“P2P”) file sharing application on her computer and that, in May 2008, a certain LabMD insurance aging report containing personal information of medical patients, referred to as the “1718 File,” was available on a P2P file sharing network. In addition, the Complaint alleges, in October 2012, certain LabMD “day sheets” and cancelled checks payable to LabMD, also containing personal information, were found among other documents in a Sacramento residence whose occupants subsequently pleaded “no contest” to identity theft charges.

Trial commenced on May 20, 2014. On May 23, 2014, FTC Complaint Counsel rested. On May 23, 2014, in open court at the conclusion of evidence presented by Complaint Counsel, Respondent moved to dismiss the Complaint for failure of Complaint Counsel’s evidence to establish a *prima facie* case of unfair trade practices. Thereafter, on May 27, 2014, in furtherance of the direction of the Administrative Law Judge, Respondent submitted its motion to dismiss in writing (“Motion”). Complaint Counsel filed an opposition to the Motion on June 6, 2014 (“Opposition”). Respondent filed a Reply in support of its Motion on June 13, 2014.<sup>1</sup>

<sup>1</sup> Rule 3.22(d) allows the filing of a reply, without advance leave of court, when filed in connection with a dispositive motion, such as the instant Motion to Dismiss. See 16 C.F.R. § 3.22(d) (“The moving party shall have no right to reply, except for dispositive motions or as otherwise permitted by the Administrative Law Judge or the Commission.”).

Rule 3.22(a) of the Commission's Rules of Practice states in pertinent part:

When a motion to dismiss is made at the close of the evidence offered in support of the complaint based upon an alleged failure to establish a *prima facie* case, the Administrative Law Judge shall defer ruling thereon until immediately after all evidence has been received and the hearing record is closed.

16 C.F.R. § 3.22(a).

Respondent rested its case on May 5, 2015 and the evidentiary hearing was concluded on July 15, 2015. Pursuant to Rule 3.44(c), the record was closed on July 20, 2015. *See* Order Closing Hearing Record, July 20, 2015. Accordingly, pursuant to Rule 3.22, the Motion is ripe for decision.

## II.

Respondent contends that Complaint Counsel's evidence fails to show any causal connection between Respondent's alleged unreasonable data-security practices and the exposure of the 1718 File or the day sheets. Respondent notes that Complaint Counsel's experts did not consider, and offered no opinions regarding, how these materials escaped LabMD's possession, and that the experts were instructed to assume that any resulting consumer harm was, or would be, the result of Respondent's data security practices. Respondent further argues that Complaint Counsel failed to offer evidence of likely "substantial" harm to consumers, and that any such conclusion of likely substantial harm would be speculative, because there is no proof that any consumer was actually harmed by Respondent's data security practices.


Complaint Counsel responds that it need not prove that Respondent's alleged unfair data security practices resulted in any particular data disclosure, or that any specific consumer has been harmed; rather, it is sufficient if substantial harm is likely to occur. Complaint Counsel further states that it has demonstrated that Respondent's alleged unreasonable data security practices are likely to harm consumers, because these practices expose consumers to the risk of substantial harm from identity theft, through the actual disclosure of personal information and through the increased risk of disclosure presented by the alleged unreasonable data security practices.

## III.

Having considered the positions of the parties, Respondent has failed to demonstrate that the evidence presented is insufficient as a matter of law, and that the Complaint must therefore be dismissed at this time. Accordingly, the Motion is DENIED. The issues raised by the Motion, to the extent they are material to the "issues of fact, law, or discretion presented on the record" (16 C.F.R. § 3.51(c)), and are properly briefed by the parties in their

post-hearing briefs, will be addressed in the initial decision. *See, e.g., In re McWane, Inc.*, 2012 FTC LEXIS 174, at \*4-5 (Nov. 7, 2012); *In re North Carolina Board of Dental Examiners*, 2011 FTC LEXIS 52, at \*7 (March 30, 2011).

ORDERED:

  
\_\_\_\_\_  
D. Michael Chappell  
Chief Administrative Law Judge

Date: July 21, 2015