ORIGINAL

PUBLIC

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 GRANTING RESPONDENT'S MOTION TO COMPEL TESTIMONY

On April 22, 2014, Respondent LabMD, Inc. ("Respondent" or "LabMD") filed a Motion to Compel Testimony ("Motion"). Specifically, Respondent requests an order compelling testimony from the designated deponent for the Federal Trade Commission ("FTC") Bureau of Consumer Protection regarding "the data security standards" that the Bureau of Consumer Protection ("Bureau" or "BCP") "has published and intends to use at the [h]earing in this matter" to prove that Respondent's data security was inadequate. FTC Complaint Counsel filed an opposition to the Motion on April 29, 2014 ("Opposition").

Having fully reviewed and considered the Motion and the Opposition, and all assertions and arguments therein, the Motion is GRANTED, as explained below.

I.

The Complaint charges that Respondent, a lab that provides doctors with cancer detection services, engaged in an unfair trade practice 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 [Respondent's] computer networks," which conduct caused, or is likely to cause, substantial injury to consumers. Complaint ¶¶ 10, 22-23. The Complaint alleges, among other security failures, that Respondent: failed to have a "comprehensive information security program," *id.* ¶ 10(a); did not use readily available measures to identity risks and vulnerabilities on Respondent's computer networks, *id.* ¶ 10(b); did not use "adequate measures" to prevent employees and others from accessing personal information, *id.* ¶ 10 (c)-(e); *see also id.* at (a); did not maintain or update its computer operating system, *id.* ¶ 10(f); and did not employ readily available measures to prevent or detect unauthorized access to personal information on the networks. *Id.* ¶ 10(g). The Complaint also alleges that, since at least 2005, the Commission has warned that P2P applications present a risk that users will inadvertently share files on P2P networks. *Id.* ¶ 16.

Respondent's Answer denies that Respondent violated the FTC Act or that any consumer was injured by the alleged security breach. Answer ¶¶ 17-23. Respondent's Answer specifically denies that Respondent failed to provide reasonable and appropriate security for personal information on its computer networks. Answer ¶ 10. The Answer further avers that Respondent lacks information sufficient to form a belief as to whether, since at least 2005, the Commission has warned that P2P applications present a risk that users will inadvertently share files on P2P networks, as alleged in paragraph 16 of the Complaint. Answer ¶ 16.

On January 30, 2014, Respondent served a "Notice of Deposition of the Bureau of Consumer Protection," pursuant to FTC Rule 3.33, directing the Bureau to designate a representative to testify regarding four topics, including "Topic 2," which requested "[a]ll data-security standards that have been used by the Bureau to enforce the law under Section 5 of the Federal Trade Commission Act since 2005." On February 14, 2014, Complaint Counsel filed a Motion for Protective Order, seeking an order barring Respondent from taking the noticed deposition, which Respondent opposed on February 26, 2014. On March 10, 2014, an Order was issued that narrowed the scope of Topics 1 and 4, but which otherwise denied the relief requested by Complaint Counsel. Order Granting in Part and Denying in Part Complaint Counsel's Motion for Protective Order, March 10, 2014, at 8-9 ("March 10 Order").

As to Topic 2 of the deposition notice, the March 10 Order held that "the deposition will not be barred; however, consistent with prior rulings in this case, Respondent may not inquire generally into the legal standards the FTC used in the past and is currently using to determine whether an entity's data security practices are unfair under Section 5. In addition, to prevent improper inquiry into privileged matters, Respondent will also be barred from inquiring into the legal opinions, legal reasoning, mental processes or decision making of the Bureau, its directors, officers, or employees, or of the Commission, with respect to Section 5 enforcement standards." March 10 Order at 7. The March 10 Order concluded:

> Complaint Counsel has failed to demonstrate that the deposition of BCP should be barred in its entirety. Accordingly, to this extent, Complaint Counsel's Motion for a Protective Order is DENIED. However, to ensure compliance with prior discovery orders in this case, and to prevent improper inquiry into privileged matters, Complaint Counsel's Motion for Protective Order is GRANTED IN PART pursuant to Rule 3.31(d), and it is HEREBY ORDERED:
>
> . . .
>
> Notwithstanding the relief granted in this Order [narrowing Topics 1 and 4], Respondent is prohibited from inquiring into any privileged matters, including without limitation, the legal opinions or legal reasoning or mental impressions of any attorney involved in the investigation or prosecution of this case, and specifically including:
>
> > The decision making processes of the Bureau with respect to the investigation of Respondent or the prosecution of this case;
> >
> > The legal standards the Bureau used in the past and is currently

> using to determine whether an entity's data security practices are unfair under Section 5;
>
> The legal reasoning or mental processes of the Bureau with respect to the use of a reasonableness standard in the Complaint; and
>
> The legal reasoning or mental processes of the Bureau with respect to the contention that Respondent's practices caused, or are likely to cause, consumer harm.

March 10 Order at 8-9.

The deposition proceeded on April 14, 2014.

II.

Respondent asserts that Respondent's counsel attempted to question the designee about the data security standards that the Bureau published during the period 2005 to 2010, and which Complaint Counsel plans to use at the hearing in this matter to demonstrate that LabMD's security was inadequate, but that Complaint Counsel objected and instructed the witness not to answer. Respondent has not certified any particular question, but cites the following exchange as an example:

> Q: Based on the allegations in paragraph 10(a), my question is has the Bureau or the FTC published, and by published I mean made available to the public, the standard that it requires for a comprehensive information security program for companies like LabMD to have in place?
>
> MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10, 2014 protective order, and I am instructing [the witness] not to answer the question.

Motion, Exh. 1, Tr. 119-120. The deposition transcript shows other questions along the same line of inquiry, to which Complaint Counsel objected as beyond the scope of the March 10 Order, and instructed the witness not to answer. *See, e.g.*, Motion Exh. 1 at Tr. 132-133 ("Q: [W]here can a company like LabMD find the Bureau's or the FTC's data security standards which will inform a company like LabMD what the FTC or the Bureau expects with regard to that company's data security?"); Tr. 134-137 (regarding data security standards outlined in the report prepared by Complaint Counsel's proferred expert, "Q: My question is[,] is that the data security standard that LabMD will be held to . . . at the hearing?").

Respondent asserts that although the March 10 Order prohibits Respondent from inquiring into the *legal standards* that have been used in the past to determine that data security practices were unfair under Section 5, the Order did not prohibit Respondent from inquiring into the *data security standards* that the Bureau has published and intends to use at trial to show that Respondent's data security was inadequate. Thus, Respondent argues, Complaint Counsel's basis for objecting to this line of questioning is invalid. In addition, Respondent states, the data

security standards that the Bureau has published and intends to use at trial are relevant to Respondent's defense that its data security was in fact adequate, as well as to its defense that the FTC failed to provide fair notice of the data security standards that Respondent was expected to meet. Accordingly, Respondent asserts, it is entitled to take testimony on this line of questioning.

Complaint Counsel contends that Respondent seeks information that violates the March 10 Order, and certain other prior orders resolving previous motions in this case. According to Complaint Counsel, these prior orders stand for the proposition that "[t]he Commission's standards – whether 'legal' or otherwise – 'used in the past and . . . currently us[ed] to determine whether an entity's data-security practices violate Section 5' are 'outside the scope of permissible discovery in this case.'" Opposition at 4. Complaint Counsel further argues, based on the Commission's January 16, 2014 Order Denying Respondent's Motion to Dismiss, that the adequacy of the Commission's notice regarding data security standards is not at issue in this case, and that the issue to be tried is the factual question of whether LabMD's data security procedures were "unreasonable." Thus, Complaint Counsel argues, Respondent seeks information that is not relevant or material. *Id.* at 4-5.

III.

As noted above, Respondent's Notice Topic 2 asked for the Bureau's designee(s) to provide testimony regarding "all data-security standards that have been used by the [Bureau] to enforce the law under Section 5 of the Federal Trade Commission Act since 2005." In previously seeking a protective order barring testimony on this topic, Complaint Counsel made substantially the same arguments as made in the instant Motion. The March 10 Order acknowledged that "prior rulings in this case hold[] that Respondent may not discover the *legal standards* the FTC has used in the past and is currently using to enforce Section 5 in data security cases, *in order to discover and challenge the Commission's decision making processes in issuing the Complaint in this case. See, e.g.*, February 25 Order; February 21 Order; January 30 Order."[1] March 10 Order at 6 (emphasis added). Contrary to Complaint Counsel's

[1] The January 30, 2014 Order granted Complaint Counsel's motion to quash a subpoena served on Complaint Counsel attorney Alain Sheer, on numerous grounds, including that "[i]t is beyond dispute that Respondent's purpose in eliciting information concerning the pre-Complaint investigation and the Commission's decision making in issuing the Complaint is to challenge the bases for the Commission's commencement of this action. Precedent dictates that such matters are not relevant for purposes of discovery in an administrative adjudication." Jan. 30, 2014 Order at 6. The February 21, 2014 Order denied Respondent's motion for a Rule 3.36 subpoena to require the Commission and FTC Office of Public Affairs to produce "all documents sufficient to show the standards the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act." That Order rejected Respondent's argument that these documents are discoverable to "show the standards that the Commission utilized in determining to bring a complaint against LabMD . . . [and that these standards] are relevant to [Respondent's] defense that the Commission's behavior toward LabMD was 'arbitrary, capricious, an abuse of discretion, and otherwise not in accordance with the law.'" February 21, 2014 Order at 6. The February 25, 2014 Order granted Complaint Counsel's motion to quash Respondent's subpoena to FTC attorney Carl Settlemyer, which sought to discover, *inter alia*, the FTC's pre-Complaint communications with nonparty Tiversa, because Respondent failed to articulate relevance, and further stated: "To the extent that Respondent seeks to discover the FTC's communications with Tiversa in order to challenge the Commission's actions, processes, or decision making leading up to the issuance of the Complaint in this case, '[p]recedent dictates that such matters are not relevant for purposes of discovery in an administrative adjudication.'" February 25, 2014 Order at 4.

arguments, none of these prior orders on previous discovery motions held that Respondent was prohibited from discovering what *data security* standards have been published by the FTC or the Bureau, and upon which Complaint Counsel intends to rely at trial to demonstrate that Respondent's data security practices were inadequate, or in the words of the Complaint, not "reasonable and appropriate." *See* Complaint ¶ 10. These are factual matters, well within the scope of permissible discovery, that are readily distinguishable from Respondent's previous attempts to discover legal enforcement standards in order to challenge the reasoning and motives for the issuance of the Complaint in this matter. Therefore, Complaint Counsel's assertion that the information sought by Respondent has been barred by prior orders is incorrect.

Further, Respondent's effort to discover what data security standards have been published by the FTC or the Bureau, and upon which Complaint Counsel intends to rely at trial to demonstrate that Respondent's data security practices were inadequate, does not violate the March 10 Order. Complaint Counsel argues that the March 10 Order limited Topic 2 to the factual bases for the allegations of Paragraph 10 of the Complaint, summarized above, and prohibited any inquiry into "data security standards." This is incorrect. The March 10 Order *denied* Complaint Counsel's request for a protective order barring testimony on Topic 2, and did not limit the scope of Topic 2, except as to "any privileged matters, including without limitation, . . . [t]he legal standards the Bureau used in the past and is currently using to determine whether an entity's data security practices are unfair under Section 5." *Id.* at 8-9; *see also id.* at 7 (holding that Respondent may not inquire into why, or how, the Bureau or the Commission determined to use a reasonableness standard to enforce Section 5, which facts support which contentions, what inferences are being drawn from the evidence, or why the alleged facts justify a conclusion of unreasonableness, because such questioning amounts to a request for the mental impressions, conclusions, opinions or legal theories of attorneys, which are privileged). As stated above, Respondent's proffered inquiry is not fairly construed as an inquiry into the FTC's legal standards or an inquiry into the Commission's decision making processes in issuing the Complaint. Moreover, Respondent's proffered inquiry does not call for privileged information prohibited by the March 10 Order, such as legal theories, reasoning, or conclusions. Rather, the data security standards that have been published and that will be used at trial to show that Respondent's data security was inadequate are fairly within the scope of Topic 2, as to which Complaint Counsel's previous request for a protective order was denied, except as to the prohibitions described above. Accordingly, Complaint Counsel's contention that Respondent's inquiry into data security standards was barred by the March 10 Order is without merit.

Complaint Counsel's argument that Respondent's proffered line of inquiry is not relevant for purposes of discovery mirrors that presented in its previous Motion for Protective Order to bar any testimony on Topic 2, which was denied by the March 10 Order. In addition, as noted above, the data security standards that have been published by the FTC or the Bureau, and upon which Complaint Counsel intends to rely at trial to demonstrate that Respondent's data security practices were inadequate, or in the words of the Complaint, not "reasonable and appropriate," are factual matters well within the scope of discovery. Complaint ¶ 10; *see* FTC Rule 3.31(c)(1) ("Parties may obtain discovery to the extent that it may be reasonably expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses of any respondent").

IV.

For all the foregoing reasons, Respondent's motion to compel deposition testimony is GRANTED, and the Bureau shall provide deposition testimony as to what data security standards, if any, have been published by the FTC or the Bureau, upon which Complaint Counsel intends to rely at trial to demonstrate that Respondent's data security practices were not reasonable and appropriate.

The fact discovery deadline, which was extended under the March 10 Order to take the Rule 3.33 deposition of the Bureau, is hereby further extended by an additional ten days from the date of this Order to allow sufficient time to complete the deposition.

ORDERED:

D. Michael Chappell
Chief Administrative Law Judge

Date: May 1, 2014