UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS:	**Edith Ramirez, Chairwoman** **Julie Brill** **Maureen K. Ohlhausen** **Joshua D. Wright** **Terrell McSweeny**

In the Matter of	)	
	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**
	)	

ORDER DENYING RESPONDENT LABMD, INC.'S MOTION FOR SUMMARY DECISION

By Commissioner Joshua D. Wright, for a unanimous Commission:[1]

Respondent LabMD, Inc. ("LabMD") seeks a summary decision dismissing with prejudice the Complaint in this matter. Motion for Summary Decision, filed April 21, 2014 ("Motion"). It argues that there is "no genuine dispute as to any material fact regarding liability or relief" in this case, and that we should proceed to "issue a final decision and order" in LabMD's favor. Motion at 8 (quoting 16 C.F.R. § 3.24(a)(2)). Complaint Counsel opposes that request.[2] We find that there are genuine disputes about some of the facts asserted by LabMD in its Motion, and that other such facts are not material to the ultimate question of whether LabMD is liable for engaging in "unfair acts or practices" in violation of Section 5(a) of the Federal Trade Commission Act ("FTC Act), 15 U.S.C. § 45(a). That question must be resolved based on factual evidence presented at an evidentiary hearing. Accordingly, we deny LabMD's Motion for Summary Decision.

BACKGROUND

On August 28, 2013, the Commission issued an administrative Complaint commencing this adjudicatory proceeding. The Complaint alleges that LabMD's data security practices, "taken together, failed to provide reasonable and appropriate security for personal information

[1] Commissioner Brill did not take part in the consideration or decision herein.

[2] *See* Complaint Counsel's Response in Opposition to Respondent's Motion for Summary Decision, filed May 5, 2014 ("CC Opp."); Complaint Counsel's Separate and Concise Statement of Material Facts as to Which There Exist Genuine Issues for Trial, filed May 5, 2014 ("CC Stmt."). *See also* LabMD Reply in Support of Motion to Dismiss, filed May 12, 2013 ("LabMD Reply").

stored on its computer networks," even though LabMD "could have corrected its security failures at relatively low cost using readily available security measures." Complaint, ¶¶ 10, 11. The Commission thus found "reason to believe" that LabMD's conduct could constitute "unfair . . . acts or practices" in violation of 15 U.S.C. § 45(a), and determined that an adjudicatory proceeding would be "in the public interest." *Id.*, Preamble & ¶¶ 22-23 (quoting 15 U.S.C. § 45(b)).

The Complaint sets forth specific allegations of "reasonable and appropriate" data security measures that LabMD allegedly should have implemented, but failed to implement, to minimize the risk of security breaches. Complaint, ¶¶ 10(a)-(g), 11. The Complaint goes on to allege that LabMD experienced two security breach incidents. First, unauthorized third parties allegedly retrieved a June 2007 "insurance aging report" and possibly other files containing sensitive consumer information from LabMD's computer systems via Limewire, a peer-to-peer file-sharing application that was installed on the computer of LabMD's billing manager. *Id.*, ¶¶ 17-20. Second, the Sacramento Police Department discovered identity thieves in possession of LabMD "day sheets" containing personal information and consumer checks payable to LabMD. *Id.*, ¶ 21.

The Complaint charges (1) that LabMD's purported data security failures caused, or were likely to cause, harm to consumers, including "identity theft, medical identity theft, and . . . disclosure of sensitive, private medical information" and other personal information including addresses, telephone numbers, social security numbers, bank account and credit card numbers. *Id.*, ¶¶ 6, 9, 12, 19, 21, 22; (2) that consumers could not have learned about LabMD's data security practices or avoided these potential injuries independently, *id.*, ¶ 12; and (3) that LabMD's alleged data security failures did not substantially benefit LabMD or anyone else, *id.*, ¶¶ 11, 20, 22.

In its Answer to the Complaint and Affirmative Defenses, filed September 17, 2013 ("Answer"), and its Objections and Responses to Complaint Counsel's Requests for Admission pursuant to 16 C.F.R. § 3.32, filed March 3, 2014 ("LabMD Admissions/Denials"), LabMD admits most, but not all, of the Complaint's allegations regarding the nature of its business, the services it provides, and the types of consumer information stored on its computer systems. *See* Answer, ¶¶ 1, 3-6, 8-9; LabMD Admissions/Denials, ¶¶ 1-13, 16-28, 35-38.[3] LabMD admits that Limewire had been installed on a computer used by its billing manager and that a company called Tiversa, Inc. had obtained access to LabMD's June 2007 insurance aging report. But in other respects, LabMD either denies, or pleads insufficient knowledge to admit or deny, most of the charges concerning the Limewire and Sacramento data breach incidents. Answer, ¶¶ 17-20; LabMD Admissions/Denials, ¶¶ 39-49. LabMD denies the Complaint's allegations concerning the list of specific data security measures that it did not implement. Answer, ¶¶ 10-11. It also generally denies the allegations regarding the causal relationship between its conduct and actual or potential consumer injury, and whether such injury was avoidable by consumers or whether its conduct had any countervailing benefits. *Id.*, ¶¶ 11-12, 22-23.

[3] LabMD denies that it maintained electronic copies on its computer networks of patients' checks, Answer, ¶ 9(c); LabMD Admissions/Denials, ¶¶ 33-34; and it takes issue with the allegations concerning the number of laboratory tests and the number of affected consumers. Answer, ¶ 7; LabMD Admissions/Denials, ¶¶ 14-15, 19-20.

On November 12, 2013, LabMD filed a motion to dismiss the Complaint. It contended that (1) the Commission has no authority to address private companies' data security practices as "unfair . . . acts or practices" under Section 5(a)(1) of the FTC Act; (2) the Health Insurance Portability and Accountability Act ("HIPAA") and other statutes touching on data security implicitly strip the Commission of authority to enforce Section 5 in the field of data security; and (3) due process requires the Commission to adopt regulations governing data security before we may engage in an enforcement action. The Commission rejected those arguments and denied the motion. *See* Order Denying Respondent LabMD's Motion to Dismiss (issued January 16, 2014) ("MTD Denial Order").

From December 2013 through April 2014, LabMD and Complaint Counsel engaged in discovery concerning factual issues and expert testimony, including extensive document production, depositions, and requests for admissions. This Motion for Summary Decision followed.

STANDARD OF REVIEW

We review LabMD's Motion for Summary Decision pursuant to Rule 3.24 of our Rules of Practice, 16 C.F.R. § 3.24, whose "provisions are virtually identical to the provisions of Fed. R. Civ. P. 56, governing summary judgment in the federal courts." *N.C. Bd. of Dental Examiners*, 151 F.T.C. 607, 610-11 (2011); *see also Hearst Corp.*, 80 F.T.C. 1011, 1014 (1972). A party moving for summary decision must show that "there is no genuine dispute as to any material fact," and that it is "entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a).

"[T]he substantive law will identify which facts are material . . . . [*i.e.*, those] that might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby*, 477 U.S. 242, 248 (1986). Here, the applicable substantive law is Section 5(n) of the FTC Act, which deems an act or practice to be "unfair" if it [1] "causes or is likely to cause substantial injury to consumers"; [2] such injury "is not reasonably avoidable by consumers themselves"; and [3] such injury "is not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n). Facts are "material" for present purposes only if they tend to prove or disprove that LabMD's data security practices satisfy one or more of these criteria. Facts that have no bearing on these dispositive questions "are irrelevant or unnecessary [and] will not be counted." *Anderson*, 477 U.S. at 248.

There is no "genuine" dispute over material facts where the "evidence favoring the non-moving party . . . is merely colorable, [but] not significantly probative." *Id.* at 249. The "party seeking summary judgment always bears the initial responsibility of . . . identifying" factual information in the record that "it believes demonstrate[s] the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). Where, as here, the party opposing the motion bears the ultimate burden of proof, *see* 16 C.F.R. § 3.43(a) (imposing burden of proof on Complaint Counsel), the moving party may "discharge this initial responsibility" either by showing that "there is an absence of evidence to support the non-moving party's case" or by supplying "affirmative evidence demonstrating that the non-moving party will be unable to prove its case at trial." *Fitzpatrick v. City of Atlanta*, 2 F.3d 1112, 1115-

16 (11th Cir. 1993). "Only when that burden has been met does the burden shift to the non-moving party to demonstrate that there is indeed a material issue of fact that precludes summary judgment." *Clark v. Coats & Clark, Inc.*, 929 F.2d, 604, 608 (11th Cir. 1991); *see also* 16 C.F.R. § 3.24(a)(3) ("When a motion for summary decision is made and *supported as provided in this rule*, a party opposing the motion . . . must set forth specific facts showing that there is a genuine issue of material fact for trial.") (emphasis added). "On summary judgment the inferences to be drawn from the underlying facts must be viewed in the light most favorable to the party opposing the motion." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986) (citation omitted).

ANALYSIS

I. GENUINE ISSUES OF MATERIAL FACT

In a section of its Motion entitled "Statement of Facts," LabMD sets forth facts that it contends are both "material" and not subject to "genuine" dispute. *See* Motion at 4-8 ("LabMD Stmt."); *cf.* 16 C.F.R. § 3.24(a). We consider the assertions in each of the 24 paragraphs in this Statement,[4] as well as factual assertions set forth in other sections of LabMD's Motion, to determine (1) whether they constitute "material" facts; (2) if so, whether there is no "genuine" dispute about them; and (3) whether, on that basis, LabMD is entitled to a summary decision in its favor as a matter of law.

A. HIPAA Data Security Standards

LabMD asserts that "[a]ll information received, utilized, maintained and transmitted by LabMD is protected health information ('PHI') as defined by the Health Insurance Portability and Accountability Act of 1996 ('HIPAA')." Motion at 1 (citing 45 C.F.R. § 160.103).[5] LabMD's Statement of Facts includes five paragraphs relating to the data security requirements imposed by HIPAA and related statutes and rules (collectively, "HIPAA Standards"), and characterizes that text as a set of "material" facts that are not in "genuine" dispute.[6]

[4] We refer to each of these paragraphs using the convention "[X.Y]," where X refers to the page number of the Motion and Y refers to the position of the paragraph in sequence of the paragraphs beginning on that page. Thus, "LabMD Stmt. 5.2" refers to the second full paragraph on page 5 of the Motion.

[5] Significantly, LabMD does not assert that the scope of personal health information included in the definition of "PHI" is co-extensive with the scope of the "personal information" at issue here, as defined in the Complaint (¶ 6), nor does it refer to any evidence or legal authority that would support that proposition.

[6] *See* LabMD Stmt. 4.2 ("LabMD is a "Covered Entity" that receives, maintains and transmits PHI during the normal course of its business."); *id.* 5.5 ("LabMD is a HIPAA-covered entity. . . . It must comply with HHS's HIPAA and Health Information Technology for Economic and Clinical Health Act ("HITECH") regulations . . . ."); *id.*, 5.6 ("HIPAA's Security Rule establishes substantive data-security standards involving PHI with which HIPAA-covered entities, like LabMD, must comply."); *id.* 5.7 ("HHS exclusively enforces HIPAA and HITECH. . . ."); *id.*, 6.1 ("The FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations. . . .").

LabMD further contends that Complaint Counsel's expert witness, Dr. Raquel Hill, articulated data security standards pursuant to Section 5 "that are difficult to reconcile with," and are "far more stringent" than, the HIPAA Security Rule and other HIPAA Standards. Motion at 3, 20. For example, LabMD asserts that Dr. Hill's proposed standards "do not account, as required by HIPAA, for the needs and capabilities of small health care providers and rural health care providers," improperly "presume a level of technical knowledge generally not available to small health care providers," and are "inconsistent with HHS guidance that the risk assessment can be a qualitative and manual process." *Id.* at 21. From those asserted facts, LabMD contends that its "compliance with the HIPAA [Standards]" should not be deemed "irrelevant to . . . Section 5 unfairness claims," but rather should be a complete "defense" to such claims. *Id.* at 20.

Complaint Counsel responds that LabMD's asserted facts relating to HIPAA "are irrelevant or immaterial" and that it need not "demonstrate that [LabMD's] conduct violated other laws in order to establish that [LabMD's] practices were unfair under Section 5." CC Opp. at 4. Complaint Counsel contends that "the Commission [has] already rejected the argument that the FTC Act and HIPAA are at odds," *id.* at 12 (citing MTD Denial Order at 12), and asserts that LabMD's arguments "that the FTC's data security 'standards' are not scalable or presume too high a level of technical knowledge for small health care providers should be addressed at trial and do not support a summary decision." *Id.*

We conclude that LabMD's factual contentions regarding HIPAA data security standards do not justify a summary decision in LabMD's favor. As LabMD concedes, "[t]he FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations," Motion at 6 (LabMD Stmt. 6.1), and "this case has nothing to do with HIPAA." *Id.* at 10 (quoting MTD Denial Order at 12). Rather, this case concerns LabMD's compliance with Section 5 of the FTC Act. Thus, the facts that LabMD alleges about HIPAA could be "material" for purposes of this Motion for Summary Decision only if LabMD were correct that, as a matter of law, the Commission could not hold LabMD liable under Section 5 if its data security practices complied with HIPAA Standards. Motion at 1. But that legal argument is now foreclosed. We held in the Order denying LabMD's Motion to Dismiss that HIPAA does not "trump" Section 5, and that LabMD therefore "cannot plausibly assert that, because it complies with [HIPAA], it is free to violate" requirements imposed independently by Section 5 of the FTC Act. MTD Denial Order at 11, 13; *see infra*, Part II.[7]

In any event, LabMD's statements of fact regarding HIPAA Standards would be insufficient to merit summary decision in its favor even if, counterfactually, those Standards *did* define the scope of Section 5 liability as a matter of law. LabMD points to no record evidence regarding what measures, if any, it implemented to prevent data breaches. It does not explain which HIPAA Standards apply to LabMD's actions or why LabMD's conduct satisfied them. Indeed, LabMD does not even assert that it *complied* with the applicable HIPAA Standards; it merely avers that the Commission has not accused it of *violating* those requirements. *See, e.g.,*

[7] Consistently, HHS, in adopting regulations implementing HIPAA, recognized that entities subject to HIPAA "may be required by other Federal law to adhere to additional or more stringent security measures," and consequently, that "[s]ecurity standards in [HHS's] final rule establish a minimum level of security that covered entities must meet." Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8355 (Feb. 20, 2003).

LabMD Stmt. 6.1. The "party seeking summary judgment bears the initial responsibility of informing the [adjudicator] of the basis for its motion, and identifying those portions of the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, which it believes demonstrate the absence of a genuine issue of material fact." *Celotex*, 477 U.S. at 323 (quotation marks omitted). LabMD has not carried this burden.[8]

In sum, because we conclude that LabMD's HIPAA-related factual assertions are not "material" to the violations of law alleged in the complaint and, in any event, are not supported by any evidence, we need not determine whether they are in "genuine" dispute.

B. Alleged Limewire and Sacramento Security Breaches

LabMD identifies what it characterizes as "material" facts regarding the two specific security breaches alleged in the Complaint – *i.e.*, the alleged breach relating to the installation of Limewire on a billing computer,[9] and the alleged breach discovered by the Sacramento Police Department.[10]

We conclude that these factual claims, even if undisputed, are not material and would not support a summary decision in LabMD's favor. LabMD has not attempted to show how its factual assertions regarding the Limewire and Sacramento incidents are material to its liability as alleged in the Complaint. For example, even if we accepted as true the claims that Tiversa retrieved the Insurance Aging File without LabMD's knowledge or consent (LabMD Stmt. 4.3), that Tiversa improperly passed on that file to Professor Johnson or others (*id.*, 4.5), and that Tiversa touted its unique technology (*id.*, 4.3 n.2), these facts would not resolve the ultimate questions we must decide in this case. In particular, they would not compel us, as a matter of

[8] We cannot determine, on the present record, whether, in fact, LabMD *has* complied with or violated HIPAA Standards. For purposes of the present Motion, we must draw all reasonable inferences in support of the party opposing the Motion—*i.e.*, Complaint Counsel—and consequently, we cannot infer from LabMD's unsupported assertions that it complied with applicable HIPAA Standards. Moreover, we express no view on whether and to what extent such compliance or noncompliance might be a relevant factor in our assessment of whether LabMD violated Section 5. We agree with Complaint Counsel that any such arguments "should be addressed at trial." CC Opp. at 12.

[9] *See* LabMD Stmt. 4.3 ("On or about February 5, 2008, without LabMD's knowledge or consent, Tiversa, Inc. ('Tiversa'), took possession of a single LabMD insurance aging file (the 'Insurance Aging File')."); *id.* n.2 ("Tiversa has testified before Congress that it possesses unique technology which among other things allows it to download computer files from unsuspecting third persons inadvertently sharing computer files via peer to peer ('P2P') networks."); *id.*, 4.4 ("The Insurance Aging File contained PHI for over 9,000 patients of LabMD's physician clients."); *id.*, 4.5 ("Subsequently, Tiversa made the Insurance Aging File available to Professor Eric Johnson, of Dartmouth College, who was conducting research under a government contract for his article entitled, 'Data Hemorrhages in the Health Care Sector'."); *id.*, 4.6 ("In January 2010, the FTC began a three year full investigation of LabMD's data security practices based upon the disclosure of the PHI contained in the Insurance Aging File.").

[10] *See* LabMD Stmt. 5.1, 5.2, and 5.3 ("In October 2012, during a raid of a house of suspected identity thieves, the Sacramento Police Department found LabMD 'day sheets' and copies of checks made payable to LabMD. Again, the day sheets and checks contained PHI from patients of LabMD's physician clients."); *id.* 5.2 ("In an attempt to notify LabMD of its find, the Sacramento police 'googled' LabMD, and discovered that LabMD was under investigation by the FTC."); *id.*, 5.3 ("The Sacramento police then notified the FTC of its find, but did not notify LabMD, despite Sacramento's awareness of LabMD's duty to notify under HIPAA.").

law, to dismiss the allegations in the Complaint that LabMD failed to implement reasonable and appropriate data security and that such failure caused, or was likely to cause, unavoidable and unjustified harm to consumers. To the contrary, LabMD's factual contentions concerning Tiversa and the Sacramento Police Department are fully consistent with the Complaint's allegations that LabMD failed to implement reasonable and appropriate data security procedures.

C. Genuine Disputes Over Reasonable and Appropriate Data Security Practices

LabMD raises a number of contentions that could be construed as addressing issues of material fact, but it fails to demonstrate that there is no "genuine dispute" over these issues. For example, LabMD criticizes the opinions of Complaint Counsel's expert witness concerning appropriate data security measures. *See* Motion at 13, 16, 18, 20-22; *id.*, Exh. 5. The issues addressed by this expert report are undoubtedly material. But there is plainly also a genuine dispute about them. Indeed, LabMD submitted the declaration of its own expert witness, whose report conflicts with that of Complaint Counsel's expert witness.[11] *See* Motion, Exh. 12; *see also* Motion at 22; LabMD Reply at 11-13. Such conflicting expert opinion is precisely the type of dispute that evidentiary hearings are held to resolve.

Similarly, LabMD's Statement asserts, "The FTC has never specified what data security standards were in place at any given point during the relevant time period or when LabMD specifically violated them." LabMD Stmt. 6.4. This contention could be read as encompassing both factual and legal issues,[12] of which at least some are genuinely disputed.[13] We cannot resolve such disputes on the present record, and LabMD has not shown, with respect to this contention, that it is entitled to judgment as a matter of law.

---

[11] We decline to address Complaint Counsel's request that we strike Mr. Baker's declaration on the grounds that LabMD "did not timely designate Mr. Baker [as an expert] in this proceeding and its use of his declaration contravenes the Scheduling Order." CC Opp. at 4 n.2. The Commission (or the ALJ) may consider a Motion to Strike if submitted as a stand-alone pleading, rather than as a footnote to a brief regarding another motion.

[12] It is unclear whether LabMD, in using the term "the FTC" in Stmt. 6.4, intends to refer to Complaint Counsel or to the Commission. To the extent LabMD is contending that Complaint Counsel, in the course of this adjudication, has yet to identify with specificity what data security standards it alleges LabMD violated, this contention is not a material fact because the adjudication is still underway and, as discussed below, the Commission is not bound by Complaint Counsel's arguments or characterizations. *See infra* notes 15-18 and accompanying text. To the extent LabMD's statement is simply an alternative formulation of its legal argument that the Commission infringed its Constitutional due process rights by providing inadequate advance notice, the statement is unavailing because we have already rejected that legal argument. *See infra* Section II; *see also* MTD Denial Order at 14-17 (rejecting LabMD's due process/fair notice argument); Motion at 11-18 (rearguing the same legal claim); LabMD Reply at 3-12 (same). We recognize that there may be other ways to interpret LabMD's statement that might implicate unresolved legal questions or material issues of fact; but for present purposes, we cannot draw inferences in LabMD's favor.

[13] *Compare* LabMD Stmt. 6.4, 6.5, and 7.1 *with* CC Stmt. ¶¶ 1-10 (and evidence cited therein) (genuine factual disputes over applicable standards and LabMD's conduct). *See also* LabMD Reply at 6-9 (citing and disputing legal arguments in Complaint Counsel's Pre-Trial Brief (filed May 6, 2014)).

D. Other Immaterial Matters

We conclude that the remaining factual assertions in LabMD's Statement of Facts are immaterial. First, the procedural history of this case, even if undisputed, does not support any particular conclusion on whether LabMD's conduct violated the FTC Act.[14]

In addition, the propositions cited in LabMD's Statement of Facts characterizing the Commission's positions on the basis of Complaint Counsel's statements to the Administrative Law Judge during an Initial Pretrial Conference,[15] Complaint Counsel's responses to LabMD's discovery demands[16] and requests for admissions,[17] and Complaint Counsel's objections to questions posed during a deposition,[18] do not constitute facts at all, let alone material facts. Just because Complaint Counsel has made particular statements or taken certain positions does not necessarily mean *the Commission* has adopted those positions. To the contrary, the Commission is not bound by characterizations employed by Complaint Counsel, and is free to reject Complaint Counsel's arguments or reject its evidence. Moreover, the statements of counsel cited by LabMD are not contained in sworn affidavits or testimony, as required under 16 C.F.R.

---

[14] *See, e.g.*, LabMD Stmt. 4.6 ("In January 2010, the FTC began a three year full investigation of LabMD's data security practices . . . ."); *id.*, 5.4 ("In August, 2013, FTC filed an Administrative Complaint."); *id.*, 6.2 ("The FTC alleges that LabMD's data-security is inadequate to protect the PHI it possesses and that this failure to adequately protect PHI is an unfair practice affecting consumers in violation of Section 5 of the Federal Trade Commission Act.").

[15] *See* LabMD Stmt. 6.6 ("When asked by the ALJ whether 'the Commission issued guidelines for companies to utilize to protect...[sensitive] information or is there something out there for a company to look to,' the FTC admitted that '[t]here is nothing out there for a company to look to.'"); *id.*, 7.1 ("The FTC admits that it has never promulgated data-security regulations, guidance, or standards under Section 5: '[T]here is no rulemaking, and no rules have been issued . . . .'"); *id.*, 7.2 ("When asked about other sources of data-security standards, FTC said, the 'Commission has entered into almost 57 negotiations and consent agreements that set out . . . the method by which the Commission assesses reasonableness.' . . . . And finally the FTC argued that 'the IT industry has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology . . .,' except that the 'Commission's process' involves 'calculation of the potential consumer harm from unauthorized disclosure of information.'"); *id.*, 8.1 ("At the hearing, the ALJ asked: 'Are there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?' The FTC responded 'No.'"); *id.*, 8.2 ("The FTC also admits that '[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward.'") (quoting colloquy between Complaint Counsel Alain Sheer and Chief Administrative Law Judge D. Michael Chappell, Transcript of Initial Pretrial Conference, September 25, 2013).

[16] *See* LabMD Stmt. 7.3 ("In response to LabMD's written discovery requesting documents relating to the standards the FTC enforces regarding data-security, the FTC produced thousands of pages of consent decrees, reports, PowerPoint presentations, and articles from the FTC's website, including many in Spanish.") (citing attachments to letters from Complaint Counsel transmitting responses to LabMD document requests).

[17] *See* LabMD Stmt. 6.5 ("The FTC claims it need not 'allege the specific industry standards Respondent failed to meet or specific hardware or software Respondent failed to use.'") (quoting Complaint Counsel's Amended Response to LabMD's First Set of Requests for Admission (filed as Exh. B to Complaint Counsel's Motion to Amend Complaint Counsel's Response to Respondent's First Set of Requests for Admission)).

[18] *See* Motion at 14 ("Respondent's counsel asked [FTC Bureau of Consumer Protection Deputy Director Daniel] Kaufman a series of questions related to published standards that the Bureau sought to enforce against LabMD; however, Complaint Counsel instructed the witness not to respond to any of these questions.") (citing Deposition of Daniel Kaufman, April 14, 2014).

§ 3.24(a)(3) & (4), and thus are little more than "mere allegations or denials," 16 C.F.R. § 3.24(a)(3), which can neither support nor defeat a Motion for Summary Decision.

Most significantly, even if these statements or arguments of Complaint Counsel could be construed as facts, and even if they were not genuinely in dispute, they still would not be material to this case. The statements and arguments of Complaint Counsel that LabMD lists in its Statement of Facts relate primarily to LabMD's legal arguments concerning due process, jurisdiction, and related matters, which we already rejected in our Order denying LabMD's Motion to Dismiss. *See infra*, part II. They appear to have little, if any, bearing on the open issues affecting our decision on whether LabMD's data security practices violated Section 5.

Finally, LabMD's contention that it "owns" the consumer information at issue also is immaterial. *See* Motion at 9-10. LabMD contends that "the PHI in LabMD's possession is information that patients voluntarily gave to their doctors, who in turn, voluntarily provided this information to LabMD," and thus, that the information at issue is LabMD's "own property." *Id.*[19] The central questions to be decided here are whether LabMD's data security practices were reasonable and whether they caused, or were likely to cause, significant injury to consumers that was unavoidable and unjustified by offsetting benefits. Those questions do not turn on the "ownership" of the data. It is quite possible that a company could use (or misuse) its "own property" in a manner that causes, or is likely to cause, significant harm to others. If such misuse satisfies the criteria of Section 5, it may constitute an "unfair act or practice."

II. LABMD'S RENEWED DUE PROCESS AND JURISDICTIONAL CHALLENGES

LabMD asserts that we wrongly denied its Motion to Dismiss, Motion at 8, and implicitly asks us to reconsider the issues raised in that Motion. We decline to do so. We have already carefully addressed and disposed of LabMD's arguments that (1) its due process rights were infringed and that it lacked adequate notice of what conduct is prohibited (*compare* Motion at 11-12, 15-16, and LabMD Reply at 4-6, *with* MTD Denial Order at 16-17); (2) the Commission cannot bring enforcement actions to address statutory violations unless it has adopted specific rules or announced detailed compliance standards in advance (*compare* Motion at 13-18 and LabMD Reply at 6-10, *with* MTD Denial Order at 14-17); and (3) HIPAA supersedes any FTC authority over unfair data security practices and that HIPAA and the FTC Act are in irreconcilable conflict (*compare* Motion at 18-20, and LabMD Reply at 13-15, *with* MTD Denial Order at 10-13).

[19] In support of this assertion, LabMD contends that, as a matter of law, "consumers who voluntarily provide personal information to third parties lose their privacy rights because the information in question once given, belongs to the receiver and not the consumer." Motion at 9. LabMD therefore rejects what it characterizes as "FTC's foundational premise"—that "consumers who voluntarily give PHI to medical providers have some protectable privacy or other interest in that information beyond that which Congress authorized HHS to carve out under HIPAA." *Id.* at 10. *See also* CC Opp. at 8 & n.3 (opposing argument). For present purposes, we need not resolve the merits of this novel legal proposition.

We need not reiterate the legal analysis set forth in our earlier Order. LabMD identifies no "new questions raised by the decision . . . upon which [it] had no opportunity to argue," *see* 16 U.S.C. § 3.55; and even if it had done so, it failed to submit a Petition for Reconsideration within 14 days of the service of our Order. *Id.* To the extent LabMD continues to disagree with the legal conclusions set forth in that interlocutory decision, it may seek judicial review pursuant to 15 U.S.C. § 45(c)-(d)—but *only* if and when we issue a final order against LabMD at the conclusion of this adjudicatory proceeding. *See, e.g., FTC v. Standard Oil Co. of Cal.*, 449 U.S. 232 (1980).[20] We express no view on the open legal questions at issue in this proceeding, or on the numerous, genuinely disputed issues of material fact that have not yet been resolved.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s Motion for Summary Decision **IS DENIED.**

By the Commission, Commissioner Brill not participating.

Donald S. Clark
Secretary

SEAL:
ISSUED: May 19, 2014

[20] *See also LabMD, Inc. v. FTC*, No. 13-15267-F (11th Cir. Feb. 18, 2014) (*per curiam*) (dismissing challenge to adjudicatory proceeding for lack of jurisdiction, because no cease and desist order had been issued); *LabMD, Inc. v. FTC*, No. 1:14-cv-00810-WSD (N.D. Ga. May 12, 2014) (same), *appeal pending*.