IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LabMD, INC., Plaintiff, v. FEDERAL TRADE COMMISSION, Defendant.	))))))))))	Civil Action No.: _____ *Related Case*: FTC v. LabMD et al., 1:12-cv-3005-WSD

VERIFIED COMPLAINT
FOR DECLARATORY AND INJUNCTIVE RELIEF

Plaintiff LabMD, INC. ("LabMD") hereby states its complaint for declaratory and injunctive relief against the unconstitutional abuse of government power and ultra vires actions by Defendant Federal Trade Commission (the "FTC" or "Commission") as follows:

PARTIES, JURISDICTION, AND VENUE

1. LabMD, 1250 Parkwood Circle, Unit 2201, Atlanta, GA 30339, is a small medical cancer diagnostics business.

2. The FTC, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580, is a federal agency for purposes of the Administrative Procedure Act ("APA"), 5 U.S.C. § 551 et seq.

3. This Court has subject-matter jurisdiction under 28 U.S.C. § 1331, 28 U.S.C. § 2201, and 5 U.S.C. § 702. In LabMD v. FTC, Case No. 13-15267-F, at 2 (11th Cir. Feb. 18, 2014), the United States Court of Appeals for the Eleventh Circuit examined whether it had jurisdiction to entertain LabMD's claims against the FTC under the APA, as codified in relevant part at 5 U.S.C. §§ 701-06, under the federal Constitution, and under 28 U.S.C. § 1331, which allows for "nonstatutory" review of ultra vires agency actions. The Court held:

> [J]urisdiction to hear suits under the APA is conferred by 28 U.S.C. § 1331, which provides district courts original jurisdiction of all civil actions arising under the laws of the United States. Any APA, *ultra vires*, and constitutional claims, to the extent they can be asserted [by LabMD] at this stage, first must be asserted and considered in a district court.

(internal citations omitted). A true and correct copy of the foregoing Order is attached hereto as Exhibit 1 and is incorporated herein by reference. See also Sackett v. E.P.A., 132 S. Ct. 1367, 1373 (2012) (". . . the APA provides for judicial review of all *final* agency actions . . . ."); id. at 1374 ("The Court holds that the Sacketts may immediately litigate their jurisdictional challenge in federal court. I agree, for the Agency has ruled definitively on that question.") (Ginsburg, J. concurring). The grounds for the relief requested include the due process clause of the United States Constitution, 5 U.S.C. §§ 701-706 (APA's judicial review provisions), 28 U.S.C. §

1651 (the All Writs Act), 28 U.S.C. § 2201 (the Declaratory Judgment Act), and 28 U.S.C. § 2202 (further relief).

4. The FTC has finally determined that it has jurisdiction over LabMD and that it has complied with constitutional due process fair-notice requirements: In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Jan. 16, 2014). A true and correct copy of the foregoing order is attached hereto as Exhibit 2 and is incorporated herein by reference.

5. The FTC claims the foregoing decision marks the consummation of its decisionmaking process, has the force of law, and is entitled to deference under "Chevron." See Supplemental Letter Brief, FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-JAD, Dkt. 152-1, at 6 (Jan. 21, 2014). A true and correct copy of the foregoing brief is attached hereto as Exhibit 3 and is incorporated herein by reference.

6. Venue is proper under 28 U.S.C. §1391(e).

NATURE OF THE CASE

7. LabMD, at all relevant times a small medical laboratory providing doctors with cancer-detection services, is now on the verge of ceasing all operations after being trapped in a paralyzing web of government investigations, subpoenas, and administrative litigation.

8. At some unknown point between 2005 and August 2013, the FTC, through enforcement activities and/or internet postings on the FTC's website, rather than through administrative rulemaking, guidance or known standards, declared for the first time that certain unspecified patient-information data-security practices employed by LabMD were inadequate and thus an "unfair" trade practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("Section 5").

9. The FTC still has yet to issue any rule or statement with legal force and effect describing the specific patient-information data-security practices it believes Section 5 prohibits or permits.

10. Between 2005 and the present, the FTC never specified in a rule or statement with legal force and effect how LabMD's patient-information practices fell short or described what, exactly, it should have done differently at any given point. In fact, the FTC commenced an investigation of LabMD in January 2010, filed its administrative complaint in August 2013, and still today, LabMD has yet to be told what, exactly, it did wrong at any point during the relevant period of years.

11. The FTC's actions and a campaign of disparagement, including conclusory statements by an FTC Commissioner that LabMD had mishandled sensitive patient information made shortly after the administrative complaint had been filed, have eviscerated LabMD's business and destroyed its professional reputation.

12. In October, 2013, LabMD lost its directors and officers (D&O) liability insurance as a result of the pending enforcement action and has been unable to obtain D&O insurance because of the pending action.

13. Further, LabMD and its doctors were denied "tail" medical malpractice insurance because of the FTC's actions, which will, unless this matter is resolved favorably in the near future, severely limit LabMD's prospects for obtaining medical malpractice insurance going forward and thus hiring qualified physicians.

14. The company's insurance carrier has advised that it will not renew LabMD's general liability insurance policy effective May 6, 2014, so that the policy will terminate effective October, 2014. This means that LabMD cannot rent office space.

15. The FTC's actions have forced LabMD, a company that once employed more than forty people and provided diagnostic services to more than one hundred doctors, to stop accepting samples.

16. At all times relevant, LabMD's Protected Health Information ("PHI"), or patient-information, data-security practices were subject to comprehensive regulation by the U.S. Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 U.S.C. § 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act

("HITECH"), 42 U.S.C. §§ 300jj et seq., 17901 et seq. See http://www.healthit.gov/providers-professionals/ehr-privacy-security/practice-integration .

17. Neither the HHS nor the FTC has accused LabMD of violating HIPAA or HITECH. See Complaint, In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Aug. 28, 2013). A true and correct copy of the foregoing complaint is attached hereto as Exhibit 4.

18. Even if Section 5 does empower the FTC to broadly regulate data-security, which it does not, Congress delegated sole authority to regulate PHI data-security to the HHS. And even if Section 5 does empower the FTC to regulate PHI data-security concurrently with HHS and/or to "overfile" HHS using a "common law" of consent orders and internet posts to impose requirements in excess of those set through HHS rulemaking, which it does not, the Commission's refusal to promulgate rules or regulations and provide the public with proper notice and comment violates LabMD's due process rights by failing to give fair notice of what the FTC believes Section 5 forbids or requires.

19. Not only does the FTC lack the statutory authority to regulate PHI and/or cyber-security, it also lacks the expertise to do so. For example, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 78 Fed. Reg. 11739 (Feb.

19, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed Mar. 18, 2014), directed the Department of Commerce to set data-security standards, not the FTC.

20. To stop the abuse, LabMD seeks a declaration that the FTC lacks jurisdiction under Section 5 over PHI data-security practices and that the FTC has violated LabMD's due process and First Amendment rights. It also seeks preliminary and permanent injunctive relief staying the administrative proceedings in In the Matter of LabMD, Inc., FTC Dkt. No. 9357. Finally, LabMD asks that the FTC pay all of LabMD's attorneys' fees and litigation costs.

FACTS

21. Section 5 authorizes the FTC to prohibit "unfair or deceptive acts or practices in or affecting commerce."

22. The FTC in this case claims Section 5 "unfairness" authority to regulate LabMD's PHI data-security practices, even absent a claim of "deception," by way of administrative "common law" established through consent orders and Internet postings.

I. The FTC Targets LabMD.

23. In or about 2008, Tiversa Holding Corp. ("Tiversa"), a self-described "cyber-intelligence company" specializing in searching for and copying medical,

financial, and other sensitive files on peer-to-peer networks using patented technology, obtained a LabMD accounts-receivable computer file containing PHI without LabMD's knowledge or consent.

24. On May 13, 2008, Tiversa contacted LabMD, advised it that Tiversa had taken its property, and refused to provide information on the procurement of the file unless LabMD entered into a contract for Internet security services. LabMD turned down this offer. See Dissenting Statement of Commissioner J. Thomas Rosch, Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands, FTC File No. 1023099 (June 21, 2012). A true and correct copy of the foregoing dissent is attached hereto as Exhibit 5 and is incorporated herein by reference.

25. In 2009, Tiversa gave LabMD's PHI accounts-receivable file to the FTC under highly irregular circumstances. See id. Recent deposition testimony of Tiversa's CEO, Robert Boback, suggests the FTC and Tiversa met on multiple occasions and ultimately conspired and agreed to transfer LabMD's file via a FTC civil investigative demand (CID) to a third company (the "Privacy Institute") that, upon information and belief, is a company that has a relationship with a Tiversa advisory board member.

26. Beginning in January 2010, the FTC requested and LabMD voluntarily provided thousands of pages of documents and submitted to multiple meetings and interviews.

27. Then, on December 21, 2011, the FTC issued formal civil investigative demands (the "CIDs") to LabMD.

28. LabMD filed a Petition to Limit or Quash the CIDs on January 10, 2012, explaining, among other things, that LabMD's PHI data security was exclusively regulated by HHS and solely subject to HHS rules and regulations establishing data-security standards for PHI under HIPAA and HITECH.

29. Commissioner Julie Brill denied LabMD's petition on April 20, 2012. Commission Letter Denying LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand, in File No. 1023099, at 13 (April 20, 2012). A true and correct copy of the foregoing correspondence is attached hereto as Exhibit 6 and is incorporated herein by reference.

30. Commissioner Brill acknowledged that LabMD's PHI accounts-receivable spreadsheet file "can be considered" protected health information regulated under HIPAA and HITECH but claimed that the FTC jurisdiction under Section 5 was "overlapping and concurrent." Id.

31. On April 25, 2012, LabMD appealed Commissioner Brill's ruling, arguing, as the Commission recently admitted, that the FTC "does not enforce HIPAA or HITECH." See Ex. 2 at 12 & n.19. LabMD also challenged the FTC's reliance on the PHI accounts-receivable file obtained from Tiversa.

32. Nonetheless, on June 21, 2012, three Commissioners (including Commissioner Brill) affirmed Commission Brill's ruling, "finding its conclusions to be valid and correct." See Commission Letter Affirming the Ruling, By Commissioner Brill, Denying the Petitions To Limit or Quash Filed by LabMD and Michael J. Daugherty (June 21, 2012). A true and correct copy of the foregoing order is attached hereto as Exhibit 7 and is incorporated herein by reference. Then-Commissioner Thomas Rosch dissented. Ex. 5.

33. The FTC then filed a petition to enforce the CIDs in this Court. LabMD opposed the petition, arguing, among other things, that the FTC lacked jurisdiction to regulate data-security.

34. The Hon. William S. Duffey upheld the CIDs, but said "there is significant merit" to LabMD's argument that Section 5 does not justify an investigation into data-security practices and consumer privacy issues. See Opinion and Order, FTC v. LabMD et al., 1:12-cv-3005-WSD, Dkt. No. 23, at 4 (N.D. Ga.

Nov. 26, 2012) (Duffy, J.). A true and correct copy of the foregoing order is attached hereto as Exhibit 8.

II. LabMD Publicly Criticizes The FTC And The FTC Retaliates.

35. LabMD's owner, Michael Daugherty decided to warn the public about the FTC's abuses through the press, social media, and a book. Mr. Daugherty used, and continues to use, his website, http://michaeljdaugherty.com/, to criticize the government.

36. For example, Mr. Daugherty was quoted in a September 7, 2012, Atlanta Business Chronicle article as follows: "'We are guilty until proven innocent with these people . . . . They are on a fishing expedition. We feel like they are beating up on small business.'" Amy Wenk, "Atlanta Medical Lab Facing Off Against FTC," Atlanta Business Chronicle (September 5, 2012). Ms. Wenk wrote that "Daugherty contends his company is being unreasonably persecuted by FTC. He said he's already spent about $500,000 fighting the investigation." Id.

37. On information and belief, FTC attorney Alain Sheer, who would later serve as lead counsel for the FTC in an enforcement action against Plaintiff, monitored Mr. Daugherty's political speech and retaliated against him for it.

38. For example, on July 19, 2013, Mr. Daugherty posted the trailer to his book, "The Devil Inside the Beltway," on his website,

http://michaeljdaugherty.com/2013/07/19/the-devil-inside-the-beltway-book-trailer/. The trailer called the FTC's actions against LabMD an "abusive government shakedown" and explained that his book would "blow the whistle" about how "the Federal Trade Commission began overwhelming . . . [LabMD, a] small business, a cancer detection center, with their abusive beltway tactics." It criticized Commission staff, including Mr. Sheer.

39. On July 22, 2013, Mr. Sheer told LabMD that Commission staff had recommended that the FTC commence enforcement proceedings against LabMD.

40. On July 30, 2013, Janis Claire Kestenbaum, the Senior Legal Advisor to the Chairwoman of the FTC, provided LabMD a draft complaint.

41. On August 28, 2013, the Commission commenced an enforcement action (the "Enforcement Action") by issuing a complaint and notice order. The gravamen of its claim at that time was about the PHI accounts-receivable file purloined by Tiversa. Mr. Sheer, who met with Tiversa and who was responsible for the shell-game through which the FTC obtained the file, is lead Complaint Counsel.

42. The FTC's Complaint in the Enforcement Action makes clear that LabMD was a "health care provider" and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things.

43. The FTC did not allege that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing those statutes.

44. Instead, the FTC's Complaint solely alleged that LabMD violated Section 5's proscription against "unfair" trade practices. It said LabMD's "information security program" was not "comprehensive" and that LabMD did not use "readily available measures" or "adequate measures" but did not specify what those terms actually mean. See Ex. 4 ¶¶ 10-11.

45. The FTC did not name an individual complainant or allege direct harm to any person.

46. The FTC did not cite any regulations, guidance, or standards for what was "adequate," "readily available," "reasonably foreseeable," "commonly known," or "relatively low cost."

47. The FTC did not cite any regulations, guidance, or standards that LabMD supposedly failed to comply with, or specify the combination of LabMD's alleged failures to meet the unspecified regulations, guidance, or standards that, "taken together," allegedly violated Section 5.

48. The FTC did not allege that LabMD's data-security practices fell short of meeting medical-industry data-security standards, such as those established by HIPAA and HITECH for PHI data security.

49. Mr. Sheer of the FTC has admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Initial Pretrial Conference Transcript, In the Matter of LabMD, Inc., Dkt. No. 9357, 10:11-15 (Sept. 25, 2013) ("Initial Pretrial Conf. Trans."). He also acknowledged that the FTC brought this action without any complaining witnesses who say their data was released or disclosed. Id. 33:3-5. A true and correct copy of that transcript is attached hereto as Exhibit 9.

50. No court has ever held the FTC may require firms to adopt information-practice policies under Section 5's "unfairness" prong. Hearing Trans. 16: 22-25, FTC v. LabMD, Inc. et al., Case No. 1:12-cv-3005-WSD (Sept. 19, 2012) (Duffy, J.) (emphasis added). A true and correct copy is attached hereto as Exhibit 10.

51. On September 17, 2013, LabMD filed an answer challenging the FTC's jurisdiction and violations of LabMD's federal constitutional due process rights, among other things.

52. In September 2013, HHS said that it decided against even investigating LabMD's alleged PHI data-security practices, noting that it had not received any complaints.

53. On October 24, 2013, Mr. Sheer of the FTC served a subpoena duces tecum on Mr. Daugherty, LabMD's CEO and President, requesting the following documents concerning Mr. Daugherty's book:

- "All drafts of . . . [Mr. Daugherty's book about the FTC] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" Mr. Daugherty's book about the FTC.
- "All documents related to the source material for drafts of" Mr. Daugherty's book about the FTC, "including documents referenced or quoted in the" book.
- "All promotional materials related to" Mr. Daugherty's book criticizing the FTC, "including, but not limited to, documents posted on social media, commercials featuring . . . [Mr. Daugherty], and presentations or interviews given by" Mr. Daugherty.

54. After over four years of investigation and litigation, LabMD still does not know when or what it did "wrong" and cannot even determine what the elements of a data-security "unfairness" offense are in this case.

55. For example, FTC enforcement staff have refused to substantively respond to LabMD's interrogatories regarding PHI data-security standards—including "data-security standards, regulations, and guidelines the FTC seeks to enforce against LabMD"—except to cross-reference their response to LabMD's request that they produce "[a]ll documents sufficient to show the standards or criteria 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 from 2005 to the present."

56. Indeed, Complaint Counsel even objected to LabMD's interrogatory inquiring what "data-security standards, regulations, and guidelines the FTC will use to determine whether LabMD's data-security practices were not reasonable and appropriate" on the ground that it seeks opinions by undisclosed nontestifying experts and "calls for expert opinions."

57. The thousands of pages of materials that FTC enforcement staff have produced to LabMD in response to the foregoing document request (most of which was produced on March 3, 2014, two days before the close of fact discovery) consist almost exclusively of: Power Point presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of

FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials. Some of these materials are of very recent vintage and dated after the events described in the FTC's August 2013 administrative complaint allegedly occurred. Some of these materials are dated after August 28, 2013, when the FTC issued this complaint. The only regulations that FTC enforcement staff produced to LabMD do not apply to LabMD and implement statutes that also do not apply to LabMD.

58. On March 3, 2014, FTC enforcement staff refused to admit, among other things, that the FTC's administrative complaint does not specifically reference any industry standards for data-security practices, hardware or software necessary to avoid a violation of Section 5, instead claiming that LabMD was asking for "an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside of the scope of discovery" and, in the alternative, denying that they were required to allege this.

59. FTC enforcement staff have even argued that "STANDARDS USED TO ENFORCE SECTION 5 ARE OUTSIDE THE SCOPE OF DISCOVERY," saying that "[t]he orders and opinions of the Commission and of th[e ALJ] …

preclude such discovery." Complaint Counsel's Motion for Protective Order Regarding Rule 3.33 Notice of Deposition, *In the Matter of LabMD*, FTC Dkt. No. 9357, at 7 (Feb. 14, 2014).

60. More recently, on March 18, 2014, FTC enforcement staff produced an expert witness report that for the first time—after more than four years of investigation and litigation—gave LabMD some notice as to what a FTC expert thinks LabMD did wrong. But that report did not even purport to assess LabMD's PHI data-security practices against any objective, applicable medical-industry data-security statute, regulation, custom, or standard.

III. <u>LabMD Challenges The FTC's Jurisdiction.</u>

61. On November 12, 2013, LabMD filed a dispositive Motion to Dismiss raising pure issues of law and questions of statutory interpretation in the FTC's administrative case. A true and correct copy is attached hereto as Exhibit 11. LabMD requested oral argument. Under the FTC's Rules of Practice, Commissioners (and not the ALJ) rule on dispositive motions to dismiss complaints they recently voted to issue in the first instance.

62. On November 14, 2014, LabMD also filed a Verified Complaint in the U.S. District Court for the District of Columbia seeking solely injunctive and

declaratory relief. LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 1 (D.D.C. Nov. 14, 2013).

63. On November 18, 2013, LabMD filed a petition for review in the U.S. Court of Appeals for the Eleventh Circuit, LabMD, Inc. v. FTC, Case No. 13-14267-F (11th Cir. Nov. 18, 2013). Ex. 1.

64. On November 25, 2013, LabMD filed an administrative stay motion in the FTC enforcement action.

65. On December 2, 2013, LabMD filed a reply in support of its administrative motion to dismiss. A true and correct copy is attached hereto as Exhibit 12.

66. On December 13, 2013, the FTC issued an order denying LabMD's stay motion ("December 13 Order"). A true and correct copy is attached hereto as Exhibit 13. The December 13 Order states that no Article III court has jurisdiction over LabMD's claims until the FTC gives its permission.

67. On December 16, 2013, the Eleventh Circuit issued two jurisdictional questions to the parties. Jurisdictional Questions, LabMD v. FTC, Case No. 13-15267-F (Dec. 16, 2013).

68. On December 23, 2013, LabMD filed a stay motion in in the Eleventh Circuit. Petitioner's Motion for Stay Pending Review, LabMD v. FTC, Case No. 13-15267-F (Dec. 23, 2013).

69. On January 16, 2014, the FTC denied LabMD's administrative Motion to Dismiss, rejecting LabMD's jurisdictional and fair-notice due process challenges without oral argument, thereby denying LabMD an opportunity to create a record (the "January 16 Order"). Ex. 2.

70. On January 17, 2014, the FTC submitted the January 16 Order to the Eleventh Circuit, via what it called a "notice of supplemental authority."

71. FTC did the exact same thing on the exact same day in FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-SCM, Dkt. No. 151 (D. N.J. Jan. 17, 2014). The FTC claimed its order had the force of law and should be given deference under "Chevron." Ex. 3 at 6.

72. The FTC admits that it cannot and does not enforce HIPAA or HITECH. Ex. 2 at 12 & n.19.

73. The FTC admits that its case against LabMD solely alleges statutory Section 5 statutory "unfairness" violations, not "violations of the FTC's Health Breach Notification Rule." Id. at 20 n.20.

74. The FTC admits that it has failed to establish any data-security standards with the force of law that give notice as to what PHI data-security practices the Commission and its enforcement staff believes Section 5 forbids or requires. Ex. 2 at 15.

75. The FTC admits that it did not claim data-security regulatory authority until years after 1994, when Section 5 was last amended to add subsection (n). 15 U.S.C. § 45(n). Ex. 2 at 4, 8-9. Subsection (n) does not mention "data security," let alone explain what data-security practices the FTC believes Section 5 to forbid or require.

76. Yet the FTC claims subsection (n) gives fair notice: "Here, the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n) [15 U.S.C. § 45], should dispel LabMD's concern about whether the statutory prohibition of 'unfair . . . acts or practices' is sufficient to give fair notice of what conduct is prohibited." Ex. 2 at 16.

77. The FTC's January 16 Order essentially asserts that constitutional fair-notice due process requirements are somehow inapplicable here because, according to the Defendant, the FTC is not pursuing "criminal punishment or civil penalties for past conduct." Ex. 2 at 16.

78. The FTC also claims it is not obligated to provide any fair notice at all of the PHI data-security practices it believes Section 5 to forbid or require because agencies have broad "discretion" to "address an issue by rulemaking or adjudication." Ex. 2 at 15.

79. For that matter, the FTC effectively claims that the standard for Section 5 "unfairness" PHI data-security liability is whether a company's practices are "unreasonable" according to it, while acknowledging that this is a case of first impression as to what is "unreasonable."

80. Elsewhere, the FTC admitted that there is no process through which businesses could have obtained guidance or an advisory opinion from the Commission regarding data-security practices. See Hearing Trans., FTC v. Wyndham et al., Case No. 2:13-cv-01887-ES-SCM, 52:10-11 (Nov. 7, 2012). A true and correct copy of an excerpt of the foregoing transcript is attached hereto as Exhibit 14 and is incorporated herein by reference.

81. On February 18, 2014, the Eleventh Circuit dismissed LabMD's Petition for Review and denied all pending motions as moot because there was no cease and desist order reviewable under 15 U.S.C. § 45(c). Instead, it ruled this Court has original jurisdiction over LabMD's ultra vires, statutory, and constitutional claims to

the extent that such claims could be asserted before a cease and desist order is entered. Ex. 1.

82. Therefore, on February 19, 2014, LabMD filed a Notice of Voluntary Dismissal Without Prejudice of LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 20 (D.D.C.), because under D.C. Circuit law, which is different from the law of this Circuit, only the U.S. Court of Appeals for the D.C. Circuit has jurisdiction over those claims, yet the D.C. Circuit will never have jurisdiction under 15 U.S.C. § 45(c) because LabMD has not done business there.

83. The FTC has issued a final agency decision regarding jurisdiction, and LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional fair-notice due process arguments.

IV. The FTC Denies LabMD Procedural Due Process.

84. To begin with, the FTC has never specified the PHI data-security standards LabMD failed to meet, thereby denying LabMD an opportunity to effectively defend itself and granting the Commission, Mr. Sheer, and other federal bureaucrats unlimited discretion to decide what is "unreasonable" after the fact and to regulate the entire health care industry based on their idiosyncratic whim, caprice, and fancy.

85. In 2009, the FTC modified its Rules of Practice to deny respondents a fair defense and to render motion practice futile. 74 Fed. Reg. 20,205 (May 1, 2009).

86. At the initial pretrial conference, the ALJ told LabMD's counsel:

> [L]et me talk about dispositive motions . . . . There is a rule that covers that, if you intend to file a summary judgment, and if you don't know, I'll tell you. Summary judgments will be ruled on by the Commission, the same body that voted to issue the complaint in this case. With respect to motion to dismiss or other substantive motion, the rules provide that if they are filed before the start of the evidentiary hearing, they will be ruled on by that same Commission . . . .

Ex. 9 at 18:11-15. The ALJ lacks power to even grant a continuance of the evidentiary hearing or stay the proceedings pending adjudication of dispositive motions before the Commission. See 16 C.F.R. §§ 3.22(b), 3.41(b).

87. The FTC was extensively warned about the constitutional implications of its power-grab during the comment period.

88. The American Bar Association (ABA) Section of Antitrust Law ("Antitrust Section") said the revisions forced respondents to address prehearing issues to the FTC without the benefit of a prior opinion authored by a party who was not involved in crafting and approving a complaint. Comments of the ABA Section of Antitrust Law in Response to the Federal Trade Commission's Request for Public Comment Regarding Parts 3 and 4 Rules of Practice Rulemaking—P072194, at 4 (Nov. 6, 2008).

89. The Antitrust Section explained that its "primary concern is that by 'codifying' the Commission's right to interject itself into prehearing case management, it may undermine the integrity of the process, compromise the ALJ, and create an appearance of unfairness." Id. at 12. The Antitrust Section also said the FTC's amendments "could reduce the quality of decision making, and may color the perception of the fairness and impartiality of Commission proceedings—a particularly important issue considering that when hearing an appeal, federal courts will give deference to a final FTC decision." Id. at 11.

90. The U.S. Chamber of Commerce added that "it appears that the proposed changes are being rushed into place and for the purpose of giving the FTC material, tactical, and procedural advantage . . . ." U.S. Chamber of Commerce, Comment, Re: Parts 3 and 4 Rules of Practice Rulemaking—P072104, at 1 (Nov. 6, 2008). In fact:

> The FTC's proposed regulations work to effectively eliminate the role of the independent Administrative Law Judge (ALJ) to manage and prepare an initial decision for a case. This results in the elimination of a vital check on potential unfairness inherent in the FTC's administrative procedure. Under the FTC's process, the Commissioners act as both prosecutor and judge in administrative trials. Thus, the same individuals who decide to issue the complaint also decide the final appeal of the administrative trial. With such a clear potential for unfairness or conflict of interest at the forefront of FTC administrative adjudication, it is necessary to preserve some sort of fairness check.

Id. at 2.

91. Under current Commission Rule 3.22(a), "[m]otions to dismiss filed before the evidentiary hearing, motions to strike, and motions for summary decision shall be directly referred to the Commission and shall be ruled on by the Commission unless the Commission in its discretion refers the motion to the Administrative Law Judge."

92. In excess of their authority and in violation of the Constitution's guarantee of due process, the FTC has assumed for itself the power to legislate, to prosecute, and to judge LabMD without even specifying in advance the elements of the data-security offense LabMD has allegedly committed.

93. The empirical evidence demonstrates that the FTC's administrative process is a rigged exercise in futility for LabMD and others similarly situated.

94. According to Commissioner Wright:

> The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed.

Joshua D. Wright, Comm'r, Fed. Trade Comm., Recalibrating Section 5: A Response to the CPI Symposium, CPI Antitrust Symposium, at 4 (November 2013), available at

http://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf (last visited Mar. 18, 2014).

95. Further administrative proceedings are exhausted and futile.

V. <u>The Irreparable Harm Done By The FTC To LabMD.</u>

96. FTC's power-grab has destroyed LabMD's customer relationships and, in large measure, driven LabMD to cease accepting new specimen samples. But for all of the time, attention, and money LabMD has been forced to devote to addressing the FTC's actions, the company would almost certainly be accepting new specimen samples and providing cancer-diagnostic services to doctors to this day.

97. LabMD, and its doctors, have been denied insurance coverage as a direct result of the FTC's ongoing persecution of the company. For example, One Beacon (a medical malpractice insurance company) recently denied LabMD, and its doctors, coverage, saying: "[W]e are unable to offer ERP terms for the entity [LabMD], and as a result, the individual physicians so I will be closing the file. The potential volatility due to the FTC investigation is something we want to stay away from particularly because it pertains to medical records."

98. LabMD's general liability insurance carrier is planning to non-renew its insurance policy effective May 6, 2014.

99. The FTC's personnel have intentionally interfered with LabMD's customer relationships and effectively engaged in a campaign of commercial disparagement.

100. The FTC's actions have caused, and continue to cause, irreparable injury to LabMD's business reputation and good will in the marketplace.

101. The FTC, Mr. Sheer, and other FTC employees have intentionally set out to destroy LabMD's commercial brand, reputation, and good will.

102. The FTC, Mr. Sheer, and others have caused and continue to cause LabMD irreparable harm far beyond mere litigation expenses and threaten the viability of LabMD's business operations. Much of this harm cannot be quantified in monetary terms, and cannot be remedied by monetary damages. For example, on January 6, 2014, LabMD notified its customers that it would no longer be accepting new specimen samples for testing for the foreseeable future, effective January 11, 2014.

CLAIMS FOR RELIEF

First Claim for Relief
(For Violation of the APA)

103. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 54-61, 64-66, 69-81, 84, and 93-95.

104. The FTC's action against LabMD is arbitrary, capricious, an abuse of discretion and power, in excess of statutory authority and short of statutory right, and contrary to law and constitutional right, in violation of 5 U.S.C. § 706.

105. The FTC does not have jurisdiction to regulate LabMD's patient-information data-security and thus its actions are ultra vires.

106. The Commission's orders denying the jurisdictional, ultra vires, and due process claims raised in LabMD's motion to dismiss and LabMD's motion for a stay are both "final agency actions" within the meaning of 5 U.S.C. § 704 and thus LabMD's APA claims are ripe and reviewable now. TVA v. Whitman, 336 F.3d 1236, 1248 (11th Cir. 2004); see, e.g., CSI Aviation Servs. v. DOT, 637 F.3d 408, 411-14 (D.C. Cir. 2011); see Sackett, 132 S. Ct. at 1371-72; see also Athlone Indus., Inc. v. CPSC, 707 F.2d 1485, 1487-88 (D.C. Cir. 1983).

107. LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional due-process arguments, which the Commission formally rejected on January 16, 2014.

108. In addition, only administrative remedies providing a genuine opportunity for adequate relief need be exhausted, and here exhaustion is also independently not required because the administrative process is futile and inadequate and LabMD will continue to suffer irreparable harm unless its claims are reviewed by

an Article III Court now. See N.B. by D.G. v. Alachua Cnty. Sch. Bd., 84 F.3d 1376, 1379 (11th Cir. 1996); Porter v. Schweiker, 692 F.2d 740, 742-43 (11th Cir. 1982); Randolph-Sheppard Vendors of Am. v. Weinberger, 795 F.2d 90, 107-08 (D.C. Cir. 1986) (irreparable harm excuses exhaustion).

109. Therefore, the FTC's enforcement action against LabMD should be enjoined and a declaration issued that it lacks authority to regulate patient information data-security.

Second Claim for Relief
(For Ultra Vires Agency Action)

110. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 61, 70-81, and 93-96.

111. Regardless of the presence vel non of "final agency action" under 5 U.S.C. § 704, this Court has jurisdiction to adjudicate LabMD's nonstatutory ultra vires and constitutional claims, for the presence or absence of "final agency action" has no jurisdictional effect. See, e.g., Trudeau v. FTC, 456 F.3d 178 (D.C. Cir. 2006); Muniz-Muniz v. U.S. Border Patrol, No. 12-4419, 2013 U.S. App. LEXIS 25400, at *11 (6th Cir. Dec. 20, 2013) (noting that "all of our sister circuits" have concluded 5 U.S.C. § 704 has no effect on a federal-question jurisdiction to adjudicate non-APA claims); see also Arbaugh v. Y & H Corp., 546 U.S. 500, 511, 516-17 (2006).

112. Thus, the FTC's ultra vires actions are ripe for judicial review now regardless of the reviewability of LabMD's APA claims.

113. Exhaustion is not required for these claims under any circumstances. See XYZ Law Firm v. FTC, 525 F. Supp. 1235, 1237 (N.D. Ga. 1981).

114. The FTC's actions against LabMD exceed the power given to it in Section 5 and are thus ultra vires.

115. Judicial review of this claim is available because the Defendant's ultra vires actions exceed the authority conferred on it by Congress and the United States Constitution.

116. Moreover, inter alia, the FTC has effectively violated three specific and mandatory restraints on its Section 5 "unfairness" power.

117. First, the FTC's abuse exceeds its delegated powers and is contrary to specific the FTC Act's prohibitions on the use of consent orders and speeches to create a binding "common law" of data security. 15 U.S.C. § 45(m)(1)(B).

118. Second, in addition to the fact that Congress has not given the FTC Section 5 "unfairness" authority to regulate data security, let alone authority to over-file HHS and regulate PHI data security, the FTC has also independently violated 15 U.S.C. § 45(n)'s specific limits on its Section 5 "unfairness" authority. 15 U.S.C. § 45(n) explicitly states that the Defendant "shall have no authority under this section

or section 18 [15 U.S.C. § 57a] to declare unlawful an act or practice on the grounds that such act or practice is unfair" under the circumstances of this case. 15 U.S.C. § 45(n) further explicitly bars the FTC from using its public policy views as a primary basis for exercising its unfairness authority.

119. Third, the FTC's sworn responses to LabMD's discovery requests demonstrate it is seeking to enforce against LabMD random Internet postings, e-mail alerts, Commission staff reports, and congressional testimony they say establish data-security standards LabMD should have followed, even those these documents do not have the force of law and were not even published in the Federal Register, and they do not allege that LabMD had actual knowledge of any of these Internet postings and other materials. 5 U.S.C. § 552(a)(1).

120. FTC's unauthorized actions are the direct and proximate cause of LabMD's injuries, as described above. Therefore, LabMD is entitled to the declaratory and injunctive relief requested herein.

Third Claim for Relief
(For Fair-Notice Due Process Violations)

121. LabMD repeats paragraphs 4-5, 7-10, 46-49, 74-80, 84-85, and 118-119.

122. This Court has jurisdiction over LabMD's fair-notice due process claim now. Exhaustion is not required for these claims under any circumstances.

123. The Fifth Amendment to the United States Constitution states that "[n]o person shall be . . . deprived of life, liberty, or property, without due process of law." U.S. Const. amend. V.

124. The draft notice order ("Commission Notice Order") if made effective, will be in place for twenty (20) years and, inter alia, require LabMD to (1) "establish and implement, and thereafter maintain, a . . . security program"; (2) "obtain initial and biennial assessment and reports" from third parties for a period of twenty (20) years; (3) provide Commission-approved notice to the individuals listed in the accounts-receivable file and their health insurance companies of Tiversa's actions via first-class mail; (4) deliver copies of the Commission Notice Order to "current and future principals, officers, directors, and mangers," as well as deliver copies to many current and future employees, agents, representatives, and business entities; (5) notify the FTC in writing at least thirty (30) days before making numerous changes, such as change in corporate name or address; and (6) prepare and file detailed reports with the FTC.

125. Additionally, the FTC has reserved the right to order such other relief as it finds necessary and appropriate if it decides that the Commission Notice Order is insufficient, including seeking "restitution" and other types of relief authorized by Section 19 of the Federal Trade Commission Act, 15 U.S.C. § 57b (civil actions for

violations of rules and cease and desist orders respecting unfair or deceptive acts or practices), including but not limited to rescission or reformation of contracts and payment of monetary damages.

126. Under 15 U.S.C. § 45(l), each violation of the FTC cease and desist orders carries up to a $10,000 civil penalty.

127. FTC's actions, January 16 Order, December 13 Order, and the Commission Complaint and Notice Order, thus implicate LabMD's property rights, which are protected by the Due Process Clause of the Fifth Amendment.

128. FTC's refusal to promulgate any regulations or to issue any other guidelines clarifying and providing any notice, let alone constitutionally adequate notice, of what data-security practices they believe Section 5 forbids or requires, or to otherwise establish any meaningful standards, violates LabMD's due process rights.

129. Due process requires that laws that regulate persons or entities must give fair notice of conduct that is forbidden or required. FCC v. Fox TV Stations, Inc., 132 S. Ct. 2307, 2317 (2012); Connally v. Gen. Constr. Co., 269 U.S. 385, 391-95 (1926).

130. This constitutional fair-notice requirement has been thoroughly incorporated into administrative law to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. Georgia Pac. Corp. v. OSHRC, 25 F.3d 999, 1005 (11th Cir. 1994). Fair-notice due process requirements thus apply to the

FTC administrative enforcement actions seeking to impose cease and desist orders for alleged violations of Section 5.

131. The FTC has failed to meet its burden of establishing reasonably ascertainable standards for what data-security practices it believes Section 5 to either forbid or to require. See Georgia Pac. Corp., 25 F.3d at 1005; Trinity Broad. of Fla., Inc. v. FCC, 211 F.3d 618, 628-32 (D.C. Cir. 2000).

132. Basic principles of due process limit the FTC's "discretion" to enforce Section 5 through administrative adjudications; specifically, the FTC can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires. The FTC has failed to provide LabMD the baseline level of fair notice of the data-security practices it believes to be required or forbidden by Section 5's "unfairness" language.

133. Because the FTC's Section 5 PHI data-security regulatory scheme forbids or requires the doing of an act in terms so vague that men and women of common intelligence must necessarily guess at its meaning and differ as to its application, it violates due process.

134. In addition, even if the FTC's "reasonableness" standard for PHI data security otherwise passed constitutional muster, the FTC's failure to link its data-security standards to medical-industry standards independently violates due process.

135. FTC's pattern and practice of fair-notice due process violations, as applied to LabMD and all similarly situated, including the defendants in FTC v. Wyndham, violates due process.

Fourth Claim for Relief
(For Facial, Structural Due Process Violations)

136. LabMD repeats paragraphs 4-5, 7-10, 17-19, 23-34, and 84-96.

137. Exhaustion of administrative remedies is not required for facial and structural due process challenges. See, e.g., Matthews v. Eldridge, 424 U.S. 319, 329-32 (1976); Amos Treat & Co. v. SEC, 306 F.2d 260, 267 (D.C. Cir. 1963).

138. The substantial private interests affected by the FTC's actions, the high risk of erroneous deprivation of LabMD's property interests, and the high value of additional procedural safeguards outweigh the FTC's de minimis interest in the existing procedures. Therefore, LabMD has not been provided the procedural safeguards that it is constitutionally entitled to have.

139. Due process minimally requires a fair trial in a fair tribunal and "this applies to administrative agencies which adjudicate as well as to courts." Withrow v. Larkin, 421 U.S. 35, 46-47 (1975).

140. FTC's modifications to its Rules of Practices transgress constitutional limits on blending of prosecutorial, legislative, and adjudicative functions and deprive

all respondents of a fair administrative hearing. Therefore, the Commission's Rules facially and structurally violate due process.

141. Furthermore, the FTC's ex post facto enforcement action against LabMD for alleged violations of unspecified data-security standards in a proceeding in which the FTC acts in a legislative, prosecutorial, and adjudicative capacity further violates due process.

142. Finally, the FTC has predetermined this matter, denying LabMD its right to a fair and level review, including a fair hearing on its Motion to Dismiss before an impartial ALJ.

143. FTC's intentional violations of LabMD's due process rights has caused LabMD hundreds of thousands of dollars in actual damages, harmed its business reputation, caused it to lose good will and business opportunities, and brought the company to the brink of ruin.

Fifth Claim for Relief

(For Retaliation Against LabMD for Protected First Amendment Speech)

144. LabMD repeats paragraphs 4-5, 7-11, 23-49, and 53.

145. The First Amendment to the United States Constitution guarantees LabMD freedom of speech.

146. Mr. Daugherty's book, his webpage about the book, and his speeches and statements about the FTC's actions are political speech and speech about matters of public concern and thus protected by the First Amendment.

147. On information and belief, the FTC's actions against LabMD were retaliation for protected speech by Mr. Daugherty.

148. The FTC's actions against LabMD, as set forth herein, will likely chill a person of ordinary firmness from engaging in the protected First Amendment activity.

149. On information and belief, the FTC's conduct herein was precisely intended and designed, at least in part, to punish LabMD and chill government criticism by LabMD and others targeted by the government.

150. Even if the FTC, Complaint Counsel, and other FTC employees disagree with and find Mr. Daugherty's statements about their actions to be patently offensive, they are not allowed retaliate by bringing an enforcement action against LabMD.

RELIEF REQUESTED

WHEREFORE LabMD requests the following relief:

A. That the Court enter a declaratory judgment that (1) the FTC lacks statutory authority to regulate patient-information data-security practices under Section 5; (2) the FTC's efforts to regulate patient information are ultra vires; (3) the FTC violated LabMD's due process rights by failing to provide constitutionally

adequate notice of what data-security practices the Commission believed Section 5 to forbid or require before the Complaint was filed; (4) the FTC violated LabMD's due process rights by unconstitutionally combining legislative, prosecutorial, investigative, and adjudicatory functions by, among other things, allowing FTC Commissioners to rule on dispositive motions concerning complaints they recently voted to issue; and (5) the FTC unconstitutionally retaliated against LabMD for engaging in constitutionally protected speech.

B. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall take no further actions in connection with administrative proceedings known as In the Matter of LabMD, FTC Dkt. No. 9357, including but not limited to issuing orders, holding hearings, taking discovery, and filing motions.

C. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall not (1) initiate any civil or administrative enforcement action against LabMD or any other person on the ground that their patient information data-security practices are "unfair" in violation of Section 5; (2) investigate whether LabMD's or any other person's patient

information data-security practices violate Section 5 for "unfairness"; (3) attempt to establish substantive data-security standards under Section 5 and/or enforce Section 5 in civil or administrative proceedings; or (4) undertake or pursue any administrative enforcement proceedings until the Commission amends its Rules of Practice to provide constitutionally adequate due process.

D. That the Court award LabMD its attorneys' fees and litigation costs under the Equal Access to Justice Act and/or such other applicable law.

E. Such other and further relief as this Court deems just and proper.

Respectfully submitted, this 20th day of March, 2014.

/s/ Ronald L. Raider

Ronald L. Raider
Georgia Bar No. 592192
Burleigh L. Singleton
Georgia Bar No. 649084
William D. Meyer
Georgia Bar No. 950008

KILPATRICK TOWNSEND
& STOCKTON LLP
1100 Peachtree Street, NE
Suite 2800
Atlanta, Georgia 30309
Telephone (404) 815-6500
Facsimile (404) 815-6555
rraider@kilpatricktownsend.com
bsingleton@kilpatricktownsend.com
bmeyer@kilpatricktownsend.com

Counsel for Plaintiff

OF COUNSEL:

Reed D. Rubinstein
(applying for admission pro hac vice)
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
reed.rubinstein@dinsmore.com

Senior Vice President for Litigation and
Counsel to Cause of Action

Michael D. Pepson
(applying for admission pro hac vice)
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court
and administrative proceedings before
federal agencies.

Dated: March 20, 2014

Verification

I am Michael Daugherty, owner and CEO of LabMD, Inc., which is the plaintiff in this action.

I have read the foregoing Complaint and verify and declare on behalf of LabMD, Inc., under penalty of perjury, that its factual allegations are true, except to those matters stated on information and belief, and as to those matters I believe them to be true to the best of my knowledge.

LabMD, Inc.

By: _____ Date: 3/19/14
Michael Daugherty

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14 point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: March 20, 2014.

/s/ Ronald L. Raider
Ronald L. Raider

EXHIBIT 1

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 13-15267-F

LABMD, INC.,

Petitioner,

versus

FEDERAL TRADE COMMISSION,

Respondent.

Petitions for Review of a Decision of the
Federal Trade Commission

Before: HULL, MARCUS, and WILSON, Circuit Judges.

BY THE PANEL:

This petition for review is DISMISSED, *sua sponte*, for lack of jurisdiction. All pending motions are DENIED as moot. Petitioner LabMD, Inc. claims that we can hear its petition either under 15 U.S.C. § 45(c), or as an independent Administrative Procedure Act ("APA"), *ultra vires*, or constitutional claim. 15 U.S.C. § 45(c) only gives courts of appeals authority to review "an order of the [Federal Trade] Commission to cease and desist from using any method of competition or act or practice." There is no such order here, and no authority suggests that our granted authority extends beyond review of such cease and desist orders. Because federal courts are courts of limited jurisdiction and possess only that power authorized by Constitution and statute, we lack jurisdiction to hear the petition for review under that section. *See Kokkonen v.*

Guardian Life Ins. Co. of Am., 511 U.S. 375, 377, 114 S. Ct. 1673, 1675, 128 L. Ed. 2d 391 (1994).

With respect to any APA, *ultra vires*, or constitutional claims that may be lurking in this petition for review, we do not have original jurisdiction to hear these claims, regardless of whether, as petitioner asserts, the actions the Federal Trade Commission has taken amount to reviewable agency action even if not reviewable under § 45(c). The APA itself does not confer subject matter jurisdiction upon any court. *See Califano v. Sanders*, 430 U.S. 99, 107, 97 S.Ct. 980, 985, 51 L.Ed.2d 192 (1977). Rather, jurisdiction to hear suits under the APA is conferred by 28 U.S.C. § 1331, which provides district courts original jurisdiction of all civil actions arising under the laws of the United States. *See id.* at 105, 97 S.Ct. at 984; *see also Sierra Club v. Martin*, 110 F.3d 1551, 1554 n.11 (11th Cir. 1997). Any APA, *ultra vires*, and constitutional claims, to the extent they can be asserted at this stage, first must be asserted and considered in a district court. We do not express or imply any opinion about whether a district court has jurisdiction to hear such claims or about the merits of those claims.

No motion for reconsideration may be filed unless it complies with the timing and other requirements of 11th Cir. R. 27-2 and all other applicable rules.

EXHIBIT 2

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

ORDER DENYING RESPONDENT LABMD'S MOTION TO DISMISS

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

This case presents fundamental questions about the authority of the Federal Trade Commission ("FTC" or "the Commission") to protect consumers from harmful business practices in the increasingly important field of data security. In our interconnected and data-driven economy, businesses are collecting more personal information about their customers and other individuals than ever before. Companies store this information in digital form on their computer systems and networks, and often transact business by transmitting and receiving such data over the Internet and other public networks. This creates a fertile environment for hackers and others to exploit computer system vulnerabilities, covertly obtain access to consumers' financial, medical, and other sensitive information, and potentially misuse it in ways that can inflict serious harms on consumers. Businesses that store, transmit, and use consumer information can, however, implement safeguards to reduce the likelihood of data breaches and help prevent sensitive consumer data from falling into the wrong hands.

Respondent LabMD, Inc. ("LabMD") has moved to dismiss the Complaint in this adjudicatory proceeding, arguing that the Commission has no authority to address private companies' data security practices as "unfair . . . acts or practices" under Section 5(a)(1) of the Federal Trade Commission Act ("FTC Act" or "the Act"), 15 U.S.C. § 45(a)(1). This view, if accepted, would greatly restrict the Commission's ability to protect consumers from unwanted privacy intrusions, fraudulent misuse of their personal information, or even identity theft that may result from businesses' failure to establish and maintain reasonable and appropriate data security measures. The Commission would be unable to hold a business accountable for its conduct, even if its data security program is so inadequate that it "causes or is likely to cause

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

substantial injury to consumers [that] is not reasonably avoidable by consumers themselves and [such injury is] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

LabMD's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings ("Motion to Dismiss" or "Motion"), filed November 12, 2013, calls on the Commission to decide whether the FTC Act's prohibition of "unfair . . . acts or practices" applies to a company's failure to implement reasonable and appropriate data security measures. We conclude that it does. We also reject LabMD's contention that, by enacting the Health Insurance Portability and Accountability Act ("HIPAA") and other statutes touching on data security, Congress has implicitly stripped the Commission of authority to enforce Section 5 of the FTC Act in the field of data security, despite the absence of any express statutory language to that effect. Nor can we accept the premise underlying LabMD's "due process" arguments – that, in effect, companies are free to violate the FTC Act's prohibition of "unfair . . . acts or practices" without fear of enforcement actions by the Commission, unless the Commission has first adopted regulations. Accordingly, we deny LabMD's Motion to Dismiss.

PROCEDURAL BACKGROUND

On August 28, 2013, the Commission issued an administrative complaint ("Complaint") against LabMD, a Georgia-based company in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers. The Complaint alleges that LabMD engaged in "practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks," *see* Complaint, ¶ 10; that these practices caused harm to consumers, including exposure to identity theft and disclosure of sensitive, private medical information, *id.*, ¶¶ 12, 17-21; and, consequently, that LabMD engaged in "unfair . . . acts or practices" in violation of the FTC Act. *Id.*, ¶¶ 22-23. LabMD submitted its Answer and Affirmative Defenses to the Administrative Complaint ("Answer") on September 17, 2013.

LabMD filed its Motion to Dismiss on November 12, 2013.[2] On November 22, 2013, Complaint Counsel filed its Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice ("CC Opp."). LabMD filed its Reply to Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss ("Reply") on December 2, 2013. Factual discovery is now underway and is scheduled to close on March 5, 2014. The evidentiary hearing before the Administrative Law Judge is scheduled to begin on May 20, 2014.

[2] The Commission issued an Order on December 13, 2013, denying both LabMD's request for a stay of the administrative proceedings pending resolution of its Motion to Dismiss (*see* Motion at 29-30) and a separate Motion for Stay Pending Judicial Review that LabMD filed on November 26, 2013.

STANDARD OF REVIEW

We review LabMD's Motion to Dismiss using the standards a reviewing court would apply in assessing a motion to dismiss for failure to state a claim.[3] *See* Fed. R. Civ. P. 12(b)(6); *see also* Motion at 8; CC Opp. at 3; *S.C. State Bd. of Dentistry*, 138 F.T.C. 230, 232-33 (2004); *Union Oil Co.*, 138 F.T.C. 1, 16 (2004). Under this framework, "[o]ur task is to determine whether the [Complaint] contains sufficient factual matter . . . to state a claim to relief that is plausible on its face." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2010) (citation omitted). For purposes of this analysis, we "accept[] the allegations in the complaint as true and constru[e] them in the light most favorable to [Complaint Counsel]." *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1288 (11th Cir. 2010).

ANALYSIS

I. THE COMMISSION HAS AUTHORITY TO ENFORCE THE FTC ACT BY ADJUDICATING WHETHER THE DATA SECURITY PRACTICES ALLEGED IN THE COMPLAINT ARE "UNFAIR."

LabMD contends that the Commission lacks statutory authority to regulate or bring enforcement action with respect to the data security practices alleged. Motion at 9-21. We disagree. As discussed below, the Commission's authority to protect consumers from unfair practices relating to deficient data security measures is well-supported by the FTC Act, is fully consistent with other statutes, and is confirmed by extensive case law.[4]

A. Congress Intended to Delegate Broad Authority to the Commission to Proscribe Activities that Qualify as "Unfair Acts or Practices."

LabMD's broadest argument is that Section 5 does not authorize the FTC to address *any* data security practices. *See, e.g.*, Motion at 10 ("even if Section 5 does authorize the FTC to

---

[3] The Commission's administrative adjudicatory proceedings are governed by the FTC Act and the Commission's Rules of Practice, rather than the rules and standards that govern federal courts. Nonetheless, "since many adjudicative rules are derived from the Federal Rules of Civil Procedure, the latter may be consulted for guidance and interpretation of Commission rules where no other authority exists." FTC Op. Manual § 10.7. Here, the most relevant provision in the Commission's Rules of Practice (16 C.F.R. § 3.11(b)(2)) is very similar to the analogous court rule (Fed. R. Civ. P. 8(a)(2)). Thus, in this instance, we exercise our discretion to apply the pleading standards summarized above.

[4] At some points in the Motion, LabMD frames its arguments as challenges to the scope of the Commission's "jurisdiction" (*e.g.*, at 1, 2, 8, 16, 18, 19), while elsewhere it acknowledges the Commission's "Section 5 'unfairness' authority" but asserts that we cannot apply such authority to LabMD's data security practices. *Id.* at 18. As the Supreme Court recently clarified, "there is *no difference*, insofar as the validity of agency action is concerned, between an agency's exceeding the scope of its authority (its 'jurisdiction') and its exceeding authorized application of authority that it unquestionably has." *City of Arlington v. FCC*, 133 S. Ct. 1863, 1870 (2013). This is because, "for agencies charged with administering congressional statutes[,] [b]oth their power to act and how they are to act is authoritatively prescribed by Congress." *Id.* at 1869; *see* Motion at 9.

regulate data-security, which it does not"); *id.* at 17 (asserting "the Commission's lack of power to regulate data security through its general Section 5 'unfairness' authority'"). Motion at 16. LabMD points out that "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate . . . data-security practices." *Id.* at 20. Ignoring the facially broad reach of Section 5's prohibition of "unfair . . . acts or practices in or affecting commerce," LabMD urges the Commission to conclude from the absence of explicit "data security" authority in the FTC Act that the Commission has no such authority. *See, e.g.*, Motion at 14 ("When Congress has wanted the FTC to have data security authority, it has said so"); *id.* ("However, Congress has never given the Commission such authority and has, in fact, repeatedly made it clear that the FTC's power is very limited in application and very narrow in scope."); *id.* at 16 ("Section 5 does not give the FTC the authority to regulate data-security practices as 'unfair' acts or practices"); *id.* at 21 ("Section 5 does not contain a clear and manifest statement from Congress to authorize the Commission's [authority over] data security"). The statutory text, legislative history, and nearly a century of case law refute LabMD's argument.

As the courts have long recognized, "[n]either the language nor the history of the [FTC] [A]ct suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories." *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 310 (1934). Rather, the legislative history of the FTC Act confirms that Congress decided to delegate broad authority "to the [C]ommission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply. . . . There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (quoting S. Rep. No. 597, 63d Cong., 2d Sess., 13 (1914), and H.R. Conf. Rep. No.1142, 63d Cong., 2d Sess., 19 (1914)). *See also Atl. Refining Co. v. FTC*, 381 U.S. 357, 367 (1965) (Congress "intentionally left development of the term 'unfair' to the Commission rather than attempting to define 'the many and variable unfair practices which prevail in commerce.'") (quoting S. Rep. No. 592, 63d Cong., 2d Sess., 13 (1914)).

This legislative history pertains to Congress' enactment of the prohibition of "unfair methods of competition" in 1914. Similar considerations motivated Congress's reuse of the same broad term ("unfair") when it amended the statute in 1938 to proscribe "unfair and deceptive acts and practices" as well as "unfair methods of competition." The 1938 amendment perpetuated and expanded the broad congressional delegation of authority to the Commission by "overturn[ing] . . . attempts [in some court decisions] to narrowly circumscribe the FTC's authority." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985). Congress thus clarified that "the Commission can prevent such acts or practices which injuriously affect the general public as well as those which are unfair to competitors." *Id.* (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess. 3 (1937)).

As LabMD points out (*see* Motion at 18), Congress enacted legislation in 1994 that provided a sharper focus for the application of the Commission's "unfairness" authority, by amending the FTC Act to incorporate three specific criteria governing the application of "unfair . . . acts or practices" in adjudicatory and rulemaking proceedings. Specifically, the new Section 5(n) of the Act provides that, in enforcement actions or rulemaking proceedings, the Commission has authority to determine that an act or practice is "unfair" if that act or practice

"[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. 45(n). These criteria, derived from the Commission's pre-existing *Policy Statement on Unfairness*, codified the analytical framework that the Commission already had been applying for the preceding decade in its efforts to combat "unfair . . . acts or practices." *See* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) ("*Policy Statement on Unfairness*"), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984). Section 5(n)'s specific criteria provide greater certainty for businesses by setting forth the factors to be used to evaluate whether their acts or practices are "unfair." That fact alone refutes LabMD's contention that the "general statutory terms" in Section 5 are too "vague" to be applied to the conduct alleged in the Complaint. *See* Motion at 19.

At the same time, Congress, in enacting Section 5(n), confirmed its intent to allow the Commission to continue to ascertain, on a case-by-case basis, which specific practices should be condemned as "unfair." Thus, to this day, "Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission in 1914 to define unfair practices on a flexible, incremental basis." *Am. Fin. Servs. Ass'n*, 767 F.2d at 966.

The Commission and the federal courts have been applying these three "unfairness" factors for decades and, on that basis, have found a wide range of acts or practices that satisfy the applicable criteria to be "unfair," even though – like the data security practices alleged in this case – "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate" such practices (*see* Motion at 20). *See, e.g., FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010) (creating and delivering unverified checks that enabled fraudsters to take unauthorized withdrawals from consumers' bank accounts); *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1193 (10th Cir. 2009) (covert retrieval and sale of consumers' telephone billing information); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1364 (11th Cir.1988) (unilateral breach of standardized service contracts); *Am. Fin. Servs. Ass'n*, 767 F.2d at 971 (oppressive litigation conduct to repossess household goods sold on credit).

LabMD cites *American Bar Association v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), for the proposition that the Commission is overstepping the bounds of its authority to interpret the FTC Act. *See* Motion at 20. But that case is inapposite. *ABA* concerned the agency's determination, in construing the Gramm-Leach-Bliley Act ("GLB Act"), that attorneys fell within that statute's definition of "financial institutions" – a defined term that, in turn, incorporated by reference a set of lengthy and detailed definitions imported from other statutes and other agencies' regulations. The court found it "difficult to believe" that, in enacting a statutory "scheme of the length, detail, and intricacy of the one" under review, Congress could have left sufficient remaining ambiguity, "hidden beneath an incredibly deep mound of specificity," to support imposing GLB Act requirements upon "a profession never before regulated by federal [financial service] regulators, and never mentioned in the statute." 430 F.3d at 469. By contrast, the statutory text at issue in this case – "unfair . . . acts or practices" – conveys a far broader scope of interpretive flexibility, particularly given that this term is at the core of the Commission's own organic statute, the FTC Act.

LabMD similarly invokes *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000), for the proposition that "simple 'common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude' . . . reinforces the conclusion that the FTC lacks the authority to regulate the acts or practices alleged in the Complaint." Motion at 19 (quoting *Brown & Williamson*, 529 U.S. at 133). But *Brown & Williamson* is inapposite as well. In that case, the Court found that the Food and Drug Administration's attempts to regulate tobacco products conflicted directly with concrete manifestations of congressional intent. In particular, the Court concluded that, if the FDA had the authority it claimed, its own findings would have compelled it to ban tobacco products outright, whereas various tobacco-related statutes made clear that Congress wished *not* to ban such products. *See* 529 U.S. at 137-39. Here, of course, LabMD can cite no similar congressional intent to preserve inadequate data security practices that unreasonably injure consumers.

Similarly, the Court found that "Congress' specific intent when it enacted the FDCA" (Food, Drug & Cosmetics Act) in 1938 was to deny the FDA authority to regulate tobacco products. 529 U.S. at 146. The Court reasoned that, "*given the economic and political significance of the tobacco industry at the time*, it is extremely unlikely that Congress could have intended to place tobacco within the ambit of the FDCA absent any discussion of the matter." *Id.* at 147 (emphasis added).[5] By contrast, when enacting the FTC Act in 1914 and amending it in 1938, Congress had no way of anticipating the "economic and political significance" of data security practices in today's online environment. Accordingly, the fact that "there is no evidence in the text of the [FTC Act] or its legislative history that Congress in 1938 even considered the applicability of the Act" to data security practices is completely irrelevant. Congress could not possibly have had any "specific intent" to deny the FTC authority over data security practices. It did, however, intend to delegate broad authority to the FTC to address emerging business practices – including those that were unforeseeable when the statute was enacted. That is the only congressional intent that matters here.

B. The Commission Has Consistently Affirmed Its Authority under the FTC Act to Take Enforcement Action against Unreasonable Data Security Activities that Qualify as Unfair Acts and Practices

LabMD similarly attempts to draw support from the *Brown & Williamson* Court's determination that the FDA's 1996 "assertion of authority to regulate tobacco products" contradicted the agency's previous "consistent and repeated statements [over the preceding 73 years] that it lacked authority . . . to regulate tobacco absent claims of therapeutic benefit by the manufacturer," and the Court's conclusion that congressional enactments "against the backdrop" of the FDA's historic disavowal of authority confirmed that Congress did not intend to authorize such regulation. 529 U.S. at 132, 144-46. LabMD argues, by analogy, that "the Commission

[5] As the D.C. Circuit has recently recognized, these considerations are essential to the holding of *Brown & Williamson*, and, in their absence, that case does not justify restricting agency action under a broad statutory mandate. *See Verizon v. FCC*, No. 11-1355, at 23-25 (D.C. Cir., Jan. 14, 2014) (slip op.).

[previously] did not claim Section 5 'unfairness' authority to regulate patient-information (or any other) data-security practices," but "recently reversed course without explanation," thus purportedly defying congressional intent. Motion at 16, 18.

That analogy, too, is without merit. Unlike the FDA, the Commission has never disavowed authority over online privacy or data security matters. To the contrary, "[t]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace," and has repeatedly and consistently affirmed its authority to challenge unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5. *See* FTC Report to Congress, *Privacy Online*, at 2 (June 1998) ("*1998 Online Privacy Report*").[6] LabMD cites out-of-context snippets from the Commission's 1998 and 2000 reports to Congress for the unfounded proposition that, at that time, the Commission believed its authority over data security matters was "limited to ensuring that Web sites follow their stated information practices."[7] LabMD's characterization does not withstand scrutiny. Neither the text it quotes nor the reports as a whole can plausibly be read as disavowing the Commission's authority to take enforcement action against data security practices that violate Section 5's prohibition of "unfair . . . acts or practices," as defined in Section 5(n). Indeed, the Commission clearly stated that certain conduct relating to online data security is "likely to be an unfair practice," and, in both reports, confirmed its view that the FTC Act "provides a basis for government enforcement" against information practices [that] may be inherently . . . unfair, regardless of whether the entity has publicly adopted any fair information practice policies."[8] In context, the sentences from the 1998 and 2000 reports relied upon by LabMD simply recognize that the Commission's existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern (such as aspects of children's online privacy) and that expanded rulemaking authority and enforcement remedies could enhance the Commission's ability to meaningfully address a broader range of such concerns.[9] The same

---

[6] *See* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[7] Motion at 16 n.12 (quoting *1998 Online Privacy Report* at 41) ("As a general matter, the Commission lacks authority to require firms to adopt information practice policies."); Reply at 7-8 (quoting FTC Report to Congress, *Privacy Online: Fair Information Practices in the Electronic Age* (May 2000) ("*2000 Online Privacy Report*") (http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf) ("As a general matter, . . . the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites").

[8] *1998 Online Privacy Report* at 12-13, 40-41. *See also 2000 Online Privacy Report* at 33-34 ("The Commission's authority over the collection and dissemination of personal data collected online stems from Section 5[,]" which "prohibits unfair and deceptive practices in and affecting commerce," and thus "authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain [norms concerning] fair information practices").

[9] *See 1998 Online Privacy Report* at 42 (recognizing that "Section 5 may only have application to some but not all practices that raise concern about the online collection and use of information from children," and recommending legislation authorizing the Commission to promulgate "standards of practice governing the online collection and use of information from children."); *2000 Online Privacy Report* at

error infects LabMD's mischaracterization of testimony that Commissioners and high-level Commission staff members delivered to various congressional committees and subcommittees.[10]

Since the late 1990s, the Commission has repeatedly affirmed its authority to take action against unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5, in reports, testimony to Congress, and other publicly-released documents.[11] The Commission has also confirmed this view by bringing administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and resulted in improper disclosures of personal information collected from consumers online. For example, on May 1, 2006, the Commission filed a complaint in the U.S. District Court for the District of Wyoming, charging that defendant Accusearch, Inc. and its principal obtained consumers' private information (specifically, data concerning their telecommunications usage) and caused such data to be disclosed to unauthorized third parties without consumers' knowledge or consent. *FTC v. Accusearch, Inc.*, Case No. 2:06-cv-0105, Complaint, at ¶¶ 9-13. The Commission alleged that this conduct was "an unfair practice in violation of Section 5(a) of the FTC Act," *id.*, ¶ 14, because it "caused or [was] likely to cause substantial injury to consumers that [was] not reasonably avoidable by consumers and [was] not outweighed by

---

36-37 (seeking legislation granting "authority to promulgate more detailed standards pursuant to the Administrative Procedure Act," including "rules or regulations [that] could provide further guidance to Web sites by defining fair information practices with greater specificity[,]"such as "what constitutes 'reasonable access' and 'adequate security'"). *See also* Motion at 17 n.13 (quoting same).

[10] *See* Motion at 16-17, nn.12, 13, 14 (citing testimony by Chairman Robert Pitofsky in 1998, then-Commissioner Edith Ramirez in 2011, Chairman Jonathan Leibowitz in 2012, and Bureau Directors Eileen Harrington and David Vladeck in 2009 and 2011, respectively). In such testimony, the FTC representatives conveyed the Commission's support for draft data security legislation that would expand the FTC's *existing* authority by providing it with rulemaking authority under the Administrative Procedure Act and civil penalty authority. *See, e.g.*, Prepared Statement of the FTC, *Data Security*, presented by Commissioner Edith Ramirez to House Comm. on Energy & Commerce, Subcomm. on Commerce, Mfg., and Trade, at 11-12 (June 5, 2011) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf).

[11] *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Innovative Solutions for an Evolving Problem*, presented by Bureau Dir. Lydia B. Parnes to Senate Comm. on the Judiciary, Subcomm. on Terrorism, Tech., and Homeland Security, at 5-6 (Mar. 21, 2007) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-identity-theft-innovative-solutions-evolving-problem/p065409identitytheftsenate03212007.pdf); FTC Staff Report, *Protecting Consumers in the Next Tech-ade*, at 29-30 (Spring 2008) (http://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-next-tech-ade-report-staff-federal-trade-commission/p064101tech.pdf); FTC Report, *Security in Numbers, SSNs and ID Theft*, at 7 (Dec. 2008) (http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf); Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft*, presented by Assoc. Bureau Dir. Maneesha Mithal to House Comm. on Ways and Means, Subcomm. on Soc. Security, at 8 (April 13, 2011) (http://ftc.gov/os/testimony/110411ssn-idtheft.pdf); FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, at 14, 73 (March 26, 2012) (http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers). *See also* note 13, *infra*.

countervailing benefits to consumers or competition." *Id.*, ¶ 13. The district court agreed, granting summary judgment to the Commission in 2007, and the Tenth Circuit affirmed in 2009. *See Accusearch*, *supra*, 570 F.3d 1187. Since then, the Commission has taken the same position in dozens of other enforcement proceedings, including administrative adjudications,[12] as well as complaints filed in federal courts, *see* CC Opp. at 12-13 n.9 (citing cases). In these cases, the Commission challenged allegedly unreasonable data security measures (or other practices that enabled unauthorized third parties to harm consumers by obtaining access to their confidential personal data) as "unfair acts or practices" in violation of Section 5. And in each case, it clearly reaffirmed its position that it possessed jurisdiction over the allegedly "unfair" data security practices under Section 5.

The fact that the Commission initially focused its enforcement efforts primarily on "deceptive" data security practices, and began pursuing "unfair" practices in 2005, does not mean that the Commission lacked jurisdiction over "unfair" practices before then. As then-Commissioner Orson Swindle testified to a House subcommittee in 2004, "To date, the Commission's security cases have been based on its authority to prevent deceptive practices," but it "also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing.'"[13] LabMD cites Commissioner Swindle's reference to the Commission's "deceptiveness" authority over data security practices, *see* Motion at 16 n.12, but neglects to mention his reference to the Commission's "unfairness" authority over such practices.

LabMD also misinterprets the Commission's expressions of support for legislation relating to data security as requests for authority to fill regulatory "gaps" that it could not fill without such legislation. *Id.* at 17 & nn.13, 14. LabMD refers to three data security-related laws that the Commission supported, and that Congress ultimately enacted – *i.e.*, the GLB Act,[14] the

---

[12] *See BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 470 (2005); *DSW, Inc.*, 141 F.T.C. 117, 122 (2006); *CardSystems Solutions, Inc.*, Docket No. C-4168, 2006 WL 2709787, *3 (Sept. 5, 2006); *Reed Elsevier, Inc.*, Docket No. C-4226, 2008 WL 3150420, *4 (July 29, 2008); *TJX Cos., Inc.*, Docket No. C-4227, 2008 WL 3150421, *3 (Sept. 29, 2008). In these and similar cases, the Commission issues its final Decisions & Orders only after placing the relevant proposed consent orders on the public record, issuing Notices in the Federal Register that summarize and explain the provisions of the proposed orders and invite public comment, and considering comments filed by interested members of the public. *See* 16 C.F.R. § 2.34(c) & (e).

[13] Prepared Statement of the FTC, *Protecting Information Security and Preventing Identity Theft*, presented by Commissioner Orson Swindle to House Comm. on Gov't Reform, Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, at 7, 14 n.24 (Sept. 22, 2004) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-information-security-and-preventing-identity/040922infosecidthefttest.pdf) ("*Comm'r Swindle's 2004 Information Security Testimony*").

[14] Pub. L. 106-102 (1999) (codified in pertinent part at 15 U.S.C. § 6804(a)(1)).

Children's Online Privacy Protection Act ("COPPA"),[15] and the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").[16] But these laws *recognized* the Commission's *existing* enforcement authority, *expanded* that authority in particular respects, and affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts. For example, in COPPA, Congress authorized the Commission to sue for civil penalties in addition to the equitable monetary relief available under existing law, and authorized and directed the Commission to promulgate rules to protect children's online privacy pursuant to the streamlined procedures of the Administrative Procedure Act ("APA"), rather than using the more time-consuming procedures mandated by Section 18 of the FTC Act, 15 U.S.C. § 57a. Similarly, in both FACTA and the GLB Act, Congress directed the Commission to adopt rules addressing specified topics using streamlined APA procedures; and in FACTA, Congress also expanded the range of remedies available in Commission enforcement actions.

Finally, even if they were otherwise plausible, LabMD's arguments about the intended meaning of the past statements of the Commission or its members or staff would still be immaterial to the ultimate question of the Commission's statutory authority. "An agency's initial interpretation of a statute that it is charged with administering is not 'carved in stone,'" and agencies "must be given ample latitude to 'adapt their rules and policies to the demands of changing circumstances." *Brown & Williamson*, 529 U.S. at 156-57 (quoting *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 863 (1984); *Smiley v. Citibank (S.D.)*, 517 U.S. 735, 742 (1996); *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983); and *Permian Basin Area Rate Cases*, 390 U.S. 747, 784 (1968)); *see also Verizon v. FCC*, *supra* note 5, at 19-20. Presented with the concrete circumstances of this case, the Commission concludes that it can and should address whether or not LabMD's data security procedures constitute "unfair . . . acts or practices" within the meaning of the FTC Act. To conclude otherwise would disregard Congress's instruction to the Commission to protect consumers from harmful practices in evolving technological and marketplace environments.

C. HIPAA and Other Statutes Do Not Shield LabMD from the Obligation to Refrain from Committing Unfair Data Security Practices that Violate the FTC Act.

Contrary to LabMD's contention, Congress has never enacted any legislation that, expressly or by implication, forecloses the Commission from challenging data security measures that it has reason to believe are "unfair . . . acts or practices." LabMD relies on numerous "targeted statutes" that Congress has enacted in recent years "specifically delegating" to the Commission or to other agencies "statutory authority over data-security" in certain narrower fields. Motion at 15. But LabMD has not identified a single provision in any of these statutes that expressly withdraws any authority from the Commission. Thus, its argument that these more specific statutes implicitly repeal the FTC's preexisting authority is unpersuasive. "The cardinal rule is that repeals by implication are not favored. Where there are two acts upon the same subject, effect should be given to both if possible." *Posadas v. Nat'l City Bank of N.Y.*,

[15] Pub. L. 105-277 (1998) (codified in pertinent part at 15 U.S.C. §§ 6502(b), 6505(d)).

[16] Pub. L. 108-159 (2003) (codified in pertinent part at 15 U.S.C. § 1681s(a)).

296 U.S. 497, 503 (1936). Thus, one cannot conclude that Congress implicitly repealed or narrowed the scope of an existing statute (*i.e.*, Section 5) by subsequently enacting a new law unless "the intention of the legislature to repeal [is] clear and manifest; otherwise, at least as a general thing, the later act is to be construed as a continuation of, and not a substitute for, the first act . . . ." *Id.*; *see also Branch v. Smith*, 538 U.S. 254, 273 (2003) ("An implied repeal will only be found where provisions in two statutes are in 'irreconcilable conflict,' or where the [later] Act covers the whole subject of the earlier one and 'is clearly intended as a substitute.'"); *Morton v. Moncari*, 417 U.S. 535, 551 (1974) ("when two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective").

Nothing in HIPAA, HITECH,[17] or any of the other statutes LabMD cites reflects a "clear and manifest" intent of Congress to restrict the Commission's authority over allegedly "unfair" data security practices such as those at issue in this case. LabMD identifies no provision that creates a "clear repugnancy" with the FTC Act, nor any requirement in HIPAA or HITECH that is "clearly incompatible" with LabMD's obligations under Section 5. *See* Motion at 13. To the contrary, the patient-information protection requirements of HIPAA are largely consistent with the data security duties that the Commission has enforced pursuant to the FTC Act. Indeed, the FTC and the Department of Health and Human Services ("HHS") have worked together "to coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act." HHS, *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules*, Final Rule, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013). And the two agencies have obtained favorable results by jointly investigating the data security practices of companies that may have violated each of these statutes.[18]

LabMD further argues that HIPAA's comprehensive framework governing "patient-information data-security practices" by HIPAA-regulated entities somehow trumps the

---

[17] *See* Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191 (1996) (codified in pertinent part at 42 U.S.C. §§ 1320d *et seq.*); American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, Div. A, Title XIII, and Div. B, Title IV ("Health Information Technology for Economic and Clinical Health Act") ("HITECH") (codified at 42 U.S.C. §§ 1320d-5 *et seq.*).

[18] For example, in 2009, CVS Caremark simultaneously settled HHS charges of HIPAA violations and FTC charges of FTC Act violations, stemming from the two agencies' coordinated investigations of the company's failure to securely dispose of documents containing consumers' sensitive financial and medical information. *See* FTC Press Release: *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations* (Feb. 18, 2009) (http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial); *CVS Caremark Corp.*, Consent Order, FTC Docket No. C-4259, 2009 WL 1892185 (June 18, 2009). *See also* HHS Press Release: *CVS Pays $2.25 Million and Toughens Practices to Settle HIPAA Privacy Case* (Feb. 18, 2009) (http://www.hhs.gov/news/press/2009pres/02/20090218a.html). Similarly, in 2010, Rite Aid entered consent decrees to settle both FTC charges of FTC Act violations and HHS charges of HIPAA violations, which the two agencies had jointly investigated. *See Rite Aid Corp.*, Consent Order, 150 F.T.C. 694 (2010); HHS Press Release: Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case (July 27, 2010) (http://www.hhs.gov/news/press/2010pres/07/20100727a.html).

application of the FTC Act to that category of practices. Motion at 11-12. But HIPAA evinces no congressional intent to preserve anyone's ability to engage in inadequate data security practices that unreasonably injure consumers in violation of the FTC Act, and enforcement of that Act thus fully comports with congressional intent under HIPAA. LabMD similarly contends that, by enacting HIPAA, Congress vested HHS with "exclusive administrative and enforcement authority with respect to HIPAA-covered entities under these laws." *Id.* at 11. That argument is also without merit. To be sure, the Commission cannot enforce HIPAA and does not seek to do so.[19] But nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act.[20]

Indeed, the FTC Act makes clear that, when Congress wants to exempt a particular category of entities or activities from the Commission's authority, it knows how to do so explicitly – further undermining LabMD's claim to an implicit "carve-out" from the Commission's jurisdiction over HIPAA-covered entities or their "patient-information data security practices." Section 5(a)(2) specifically lists categories of businesses whose acts and practices are not subject to the Commission's authority under the FTC Act. These include banks, savings and loans, credit unions, common carriers subject to the Acts to regulate commerce, air carriers, and entities subject to certain provisions in the Packers and Stockyards Act of 1921. 15 U.S.C. § 45(a)(2). Congress could have added "HIPAA-covered entities" to that list, but it did not. Similarly, the statute identifies certain types of practices that the Commission may not address, such as commerce with foreign nations in certain circumstances. *Id.* § 45(a)(3). But it provides no carve-out for data security practices relating to patient information, to which HIPAA may apply.

LabMD relies on *Credit Suisse Securities, LLC v. Billing*, 551 U.S. 264 (2007), for the proposition that industry-specific requirements in other statutes may trump more general laws such as the FTC Act. *See* Motion at 13. *Credit Suisse* is clearly distinguishable. As LabMD concedes, there was a "possible conflict between the [securities and antitrust] laws," creating a "risk that the specific securities and general antitrust laws, if both applicable, would produce conflicting guidance, requirements, . . . or standards of conduct." *Id.* By contrast, nothing in the

---

[19] LabMD repeatedly – but incorrectly – asserts that "the FTC agrees that LabMD has not violated HIPAA or HITECH." *See, e.g.*, Motion at 13; *see also* Reply at 4 ("a company FTC admits *complied* with HIPAA/HITECH in all respects") (emphasis in original); *id.* at 5 ("FTC admits LabMD has always complied with all applicable data-security regulations"); *id.* at 12 ("FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations") (emphasis in original). The Commission does not enforce HIPAA or HITECH, and has never expressed any view on whether LabMD has, or has not, violated those statutes.

[20] Both HHS (pursuant to HIPAA and HITECH) and the FTC (pursuant to the American Recovery and Reinvestment Act of 2009) have promulgated regulations establishing largely congruent requirements concerning notification of data breaches involving consumers' private health information, but they are applicable to two different categories of firms. *Compare* 16 C.F.R. Part 318 (FTC rule) *with* 45 C.F.R. Part 164, Subparts D & E (HHS rule). LabMD correctly notes that this FTC rule does not apply to HIPAA-covered entities, *see* Motion at 12 & n.9, but the conclusion it draws from this fact is unfounded. Significantly, the Complaint in the present proceeding alleges only statutory violations; it does not allege violations of the FTC's Health Breach Notification Rule.

FTC Act compels LabMD to engage in practices forbidden by HIPAA, or vice versa. It is not unusual for a party's conduct to be governed by more than one statute at the same time, as "we live in 'an age of overlapping and concurrent regulatory jurisdiction[.]'" *FTC v. Ken Roberts Co.*, 276 F.3d 583, 593 (D.C. Cir. 2001) (quoting *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1996)). LabMD and other companies may well be obligated to ensure their data security practices comply with both HIPAA and the FTC Act. But so long as the requirements of those statutes do not conflict with one another, a party cannot plausibly assert that, because it complies with one of these laws, it is free to violate the other. Indeed, courts have consistently ruled that "the FTC may proceed against unfair practices even if those practices [also] violate some other statute that the FTC lacks authority to administer." *Accusearch*, 570 F.3d at 1194-95 (concluding that conduct may be an unlawful "unfair . . . act or practice" under the FTC Act even if it also violates the Telecommunications Act of 1996). *See also Orkin Exterminating Co.*, 849 F.2d at 1353 (rejecting proposition that a "mere breach of contract . . . is outside the ambit of [the "unfairness" prohibition in] section 5"); *Am. Fin. Servs. Ass'n*, 767 F.2d at 982-83 (FTC may ban certain creditor remedies, such as wage assignments and repossession of consumers' household goods, as "unfair . . . acts or practices" under the FTC Act, even where such conduct also ran counter to state laws against enforcing unconscionable contracts of adhesion).

Finally, LabMD argues that Congress' enactment of three new statutes addressing the Commission's authority over certain data protection matters in discrete contexts implies that Congress must have believed that, in other respects, the Commission lacked statutory authority to address data protection matters under the FTC Act. That argument, too, is without merit. First, as discussed above, in each of these statutes Congress *expanded* the enforcement and rulemaking tools that the Commission *already* possessed for addressing data security problems in discrete areas. *See supra* at 8 n.10, 9-10. LabMD identifies nothing in any of those bills or their legislative histories indicating that the Commission's authority to enforce Section 5's prohibition of "unfair . . . acts or practices" was limited in any way. Moreover, these statutes affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts.[21] Of course, by *compelling* the Commission to take particular steps in those contexts, Congress did not somehow divest the Commission of its preexisting and much broader *authority* to protect consumers against "unfair" practices. Congress commonly authorizes agencies to oversee entire fields while specifying, in a few areas, what minimum steps those agencies must take in exercising that authority, and the enumeration of those minimum steps does not cast doubt on the agencies' broader authority. *See, e.g.*, *Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-06 (D.C. Cir. 2011). And LabMD's reliance on data security-related bills that ultimately were *not* enacted into law (*see* Motion at 17-18 & n.15; Reply at 9) contradicts basic principles of statutory interpretation.[22]

---

[21] For example, in COPPA, Congress directed the Commission to promulgate rules addressing the specific duties of child-directed website operators to provide specific notices and obtain parental consent before collecting or disclosing children's personal information. *See* 15 U.S.C. § 6502(b).

[22] The fact that a proposed bill was not enacted into law does not mean that Congress consciously "rejected" it. Enacting a bill into law is a notoriously difficult and time-consuming process, given the procedural and political hurdles to be overcome before obtaining majority votes of both Houses of Congress, reconciliation of any differences between the two Houses' versions, and signature by the President. Thus, "the fact that Congress has considered, but failed to enact, several bills" typically sheds

In sum, we reject LabMD's contention that the Commission lacks authority to apply the FTC Act's prohibition of "unfair . . . acts or practices" to data security practices, in the field of patient information or in other contexts; and we decline to dismiss the Complaint on that basis.

II. THE COMMISSION HAS AUTHORITY TO ENFORCE THE STATUTE BY ADJUDICATING ALLEGED VIOLATIONS, DESPITE THE ABSENCE OF REGULATIONS, WITHOUT INFRINGING LABMD'S DUE PROCESS RIGHTS.

A. Administrative Agencies May Interpret and Enforce Statutory Requirements in Case-by-Case Adjudications, as Well as By Rulemaking.

LabMD argues that the Commission may not adjudicate whether the alleged conduct violated Section 5 of the FTC Act because the Commission "has not prescribed regulations or legislative rules under Section 5 establishing patient-information (or any other) data-security standards that have the force of law." Motion at 23. LabMD asserts that "[t]he FTC's refusal to issue regulations is wrongful and makes no sense." *Id.* at 24. LabMD's position conflicts with longstanding case law confirming that administrative agencies may – indeed, must – enforce statutes that Congress has directed them to implement, regardless whether they have issued regulations addressing the specific conduct at issue. Thus, in the leading case of *SEC v. Chenery*, the Supreme Court recognized that the SEC had not exercised its statutory rulemaking authority with regard to the matter at issue, and squarely rejected the contention "that the failure of the Commission to anticipate this problem and to promulgate a general rule withdrew all power from that agency to perform its statutory duty in this case." 332 U.S. 194, 201-02 (1947). To the contrary: "the Commission had a statutory duty to decide the issue at hand in light of the proper standards[,] and . . . this duty remained 'regardless of whether those standards previously had been spelled out in a general rule or regulation.'" *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 292 (1974) (quoting *Chenery*, 332 U.S. at 201).

The Commission has long recognized that "information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve." *See Comm'r Swindle's 2004 Information Security Testimony* at 3. Such complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings, given the difficulty of drafting generally applicable regulations that fully anticipate the concerns that arise over emerging business arrangements in this rapidly changing area. As the Supreme Court has explained,

---

little, if any, light on what Congress believed or intended; and the adjudicator's "task . . . is not to construe bills that Congress has failed to enact, but to construe statutes that Congress has enacted." *Wright v. West*, 505 U.S. 277, 294 n.9 (1992) (Thomas, J.) (plurality op.); *see also Verizon v. FCC*, *supra* note 5, at 25 ("pieces of subsequent failed legislation tell us little if anything about the original meaning" of a statute, and thus such later, unenacted legislative proposals provide "an unreliable guide to legislative intent") (citations omitted).

> [P]roblems may arise . . . [that] must be solved despite the absence of a relevant general rule. Or the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule. Or the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule. In those situations, the agency must retain power to deal with the problems on a case-to-case basis if the administrative process is to be effective. There is thus a very definite place for the case-by-case evolution of statutory standards. And the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.

Chenery, 332 U.S. at 202-03. Accordingly, "agency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication[,] [and] [t]he Commission seems on especially solid ground in choosing an individualized process where important factors may vary radically from case to case." *American Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990). *See also FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965) ("the proscriptions [of unfair or deceptive acts and practices] in Section 5 are flexible, to be defined with particularity by the myriad of cases from the field of business," which "necessarily give[] the Commission an influential role in interpreting Section 5 and in *applying it to the facts of particular cases arising out of unprecedented situations*.") (emphasis added).

The Commission has enforced Section 5's prohibition of "unfair . . . acts or practices" primarily through case-by-case adjudication and litigation from the time the statute was enacted. Indeed, numerous recent cases have condemned conduct that facilitated identity theft or involved misuse of confidential consumer information as unlawful "unfair . . . acts or practices," although the practices were unprecedented and not covered by any preexisting rules. Thus, even though the Commission had never promulgated any regulations governing the creation of online checks or bank drafts without adequate verification procedures, the Ninth Circuit, in *Neovi*, easily affirmed both the district court's holding that the defendants had committed "unfair acts or practices," 604 F.3d at 1155-58, and its requirement that the defendants disgorge all revenue from the unlawful conduct. *Id.* at 1159-60. Similarly, despite the absence of any regulation prohibiting online data brokers from gathering and selling consumers' confidential information gleaned from telephone records, the Tenth Circuit affirmed a district court decision finding that the defendants' conduct constituted "unfair acts and practices" and imposing an equitable disgorgement remedy. *See generally Accusearch*, 570 F.3d 1187.

B. This Proceeding Respects LabMD's Due Process Rights

The Commission's decision to proceed through adjudication without first conducting a rulemaking also does not violate LabMD's constitutional due process rights. The courts have rejected such due process challenges to agency adjudications on numerous occasions. For example, in *Gonzalez v. Reno*, 212 F.3d 1338 (11th Cir. 2000), the court held that the agency did not violate due process in interpreting and implementing the immigration statute in an

enforcement proceeding, even though its "policy was developed in the course of an informal adjudication, rather than during formal rulemaking." 212 F.3d at 1350. *See also Taylor v. Huerta*, 723 F.3d 210, 215 (D.C. Cir. 2013) (statute enabling agency to revoke pilot's license following administrative adjudicatory proceeding "represented nothing more than an ordinary exercise of Congress' power to decide the proper division of regulatory, enforcement, and adjudicatory functions between agencies in a split-enforcement regime . . . . [Petitioner] cites no authority, and presents no persuasive rationale, to support his claim that due process requires more."); *RTC Transp., Inc. v. ICC*, 731 F.2d 1502, 1505 (11th Cir. 1984) (rejecting contention that agency's "application of its policy . . . denied them due process because the policy was announced in adjudicatory proceedings, . . . rather than being promulgated in rulemaking proceedings with notice and opportunity for comment"); *Shell Oil Co. v. FERC*, 707 F.2d 230, 235-36 (5th Cir. 1983) (noting that parties in administrative adjudicatory proceedings are not denied due process even when agencies establish new, binding standards of general application in such proceedings, so long as affected parties are given meaningful opportunities to address the factual predicates for imposing liability).

To be sure, constitutional due process concerns may arise if the government imposes criminal punishment or civil penalties for past conduct (or unduly restricts expression protected by the First Amendment) pursuant to a law that "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)). But, as the D.C. Circuit held in rejecting a constitutional due process challenge to the Commission's implementation of the Fair Credit Reporting Act,

> [E]conomic regulation is subject to a less strict vagueness test because its subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action. The regulated enterprise . . . may have the ability to clarify the meaning of the regulation by its own inquiry, or by resort to an administrative process. Finally, the consequences of imprecision are qualitatively less severe when laws have . . . civil rather than criminal penalties.

Trans Union Corp. v. FTC, 245 F.3d 809, 817 (D.C. Cir. 2001) (quoting *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982)).

Here, the three-part statutory standard governing whether an act or practice is "unfair," set forth in Section 5(n), should dispel LabMD's concern about whether the statutory prohibition of "unfair . . . acts or practices" is sufficient to give fair notice of what conduct is prohibited. In enacting Section 5(n), Congress endorsed the Commission's conclusion that "the unfairness standard is the result of an evolutionary process . . . . [that] must be arrived at by . . . a gradual process of judicial inclusion and exclusion." *Policy Statement on Unfairness*, 104 F.T.C. at 1072. This is analogous to the manner in which courts in our common-law system routinely develop or refine the rules of tort or contract law when applying established precedents to new

factual situations. As the Supreme Court has recognized, "[b]roadly worded constitutional and statutory provisions necessarily have been given concrete meaning and application by a process of case-by-case judicial decision in the common-law tradition." *Northwest Airlines, Inc. v. Transp. Workers Union of Am.*, 451 U.S. 77, 95 (1981).

LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself. The imposition of such tort liability under the common law of 50 states raises the same types of "predictability" issues that LabMD raises here in connection with the imposition of liability under the standards set forth in Section 5(n) of the FTC Act. In addition, when factfinders in the tort context find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages. Even so, it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified. There is similarly no basis to conclude that the FTC's application of the Section 5(n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties.

III. LABMD'S ALLEGED PRACTICES ARE "IN OR AFFECTING COMMERCE" UNDER THE FTC ACT

In Section III of the Motion to Dismiss, LabMD contends that the acts and practices alleged in the Complaint do not satisfy the statutory definition of "commerce" set forth in Section 4 of the FTC Act – *i.e.*, "commerce 'among' or 'between' states." *See* Motion at 28 (citing and paraphrasing 15 U.S.C. § 44, and asserting that LabMD's principal place of business is in Georgia; the alleged acts or practices were committed in Georgia; and its servers and computer network are located in Georgia). This argument is frivolous. The Complaint plainly alleges that LabMD "tests samples from consumers located throughout the United States." Complaint, ¶ 5; *see also* ¶ 2. Indeed, LabMD concedes in its Answer to the Complaint that it "tests samples . . . which may be sent from six states outside of Georgia: Alabama, Mississippi, Florida, Missouri, Louisiana, and Arizona." Answer, ¶ 5. Thus, the complaint unquestionably alleges that LabMD's acts and practices "have been in or affecting commerce, as 'commerce' is defined in Section 4[.]" Complaint, ¶ 2.

IV. THE ALLEGATIONS IN THE COMPLAINT STATE A PLAUSIBLE CLAIM THAT LABMD ENGAGED IN "UNFAIR . . . ACTS OR PRACTICES"

We turn next to LabMD's contention that "the Complaint does not state a plausible claim for relief" on the ground that the "Complaint's allegations are nothing more than inadequate 'legal conclusions couched as factual allegations.'" Motion at 28-29 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 554, 555 (2007)).

That is incorrect. The Complaint quite clearly sets forth specific allegations concerning LabMD's conduct and other elements of the charged violation. In particular, it includes plausible

allegations that satisfy each element of the statutory standard for unfairness: that (1) the alleged conduct caused, or was likely to cause, substantial injury to consumers; (2) such injury could not reasonably have been avoided by consumers themselves; and (3) such injury was not outweighed by benefits to consumers or competition. 15 U.S.C. § 45(n). We emphasize that, for purposes of addressing LabMD's Motion to Dismiss, we presume – without deciding – that these allegations are true. But the Commission's ultimate decision on LabMD's liability will depend on the factual evidence to be adduced in this administrative proceeding.

A. Causation or Likely Causation of Substantial Injury to Consumers

The Complaint contains sufficient allegations to satisfy the criterion that the respondent's acts or practices "cause[d], or [were] likely to cause, substantial injury to consumers." *Id.* First, the Complaint alleges that LabMD collected and stored on its computer system highly sensitive information on consumers' identities (*e.g.*, names linked with addresses, dates of birth, Social Security numbers, and other information), their medical diagnoses and health status, and their financial transactions with banks, insurance companies, and health care providers. *See* Complaint, ¶¶ 6-9, 19, 21.

Second, the Complaint contains allegations that LabMD implemented unreasonable data security measures. These measures allegedly included (*i*) "acts of commission," such as installing Limewire, a peer-to-peer file sharing application, on a billing manager's computer, *see id.*, ¶¶ 13-19, as well as (*ii*) "acts of omission," such as failing to institute any of a range of readily-available safeguards that could have helped prevent data breaches. *See id.*, ¶¶ 10(a)-(g)).

Third, the Complaint alleges that LabMD's actions and failures to act, collectively, directly caused "substantial injury" resulting from both (*i*) actual data breaches, enabling unauthorized persons to obtain sensitive consumer information, *id.*, ¶¶ 17-21, as well as (*ii*) increased risks of other potential breaches. *Id.*, ¶¶ 11-12, 22. Notably, the Complaint's allegations that LabMD's data security failures led to *actual* security breaches, if proven, would lend support to the claim that the firm's data security procedures caused, or were likely to cause, harms to consumers – but the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in "unfair . . . acts or practices." The Commission has long recognized that "the occurrence of a breach does not necessarily show that a company failed to have reasonable security measures. There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." *See Comm'r Swindle's 2004 Information Security Testimony* at 4.[23] Accordingly, we will need to determine whether the "substantial injury" element is satisfied by considering not only whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures

[23] *See also In re SettlementOne Credit Corp.*, File No. 082 3209, Letter to Stuart K. Pratt, Consumer Data Industry Association, from Donald S. Clark, Secretary, by Direction of the Commission, at 2 (Aug. 17, 2011) (http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819lettercdia_1.pdf) (affirming, in resolving three cases concerning data security practices alleged to violate the Fair Credit Reporting Act, that it had "applied the standard that is consistent with its other data security cases – that of reasonable security. This reasonableness standard is flexible and recognizes that there is no such thing as perfect security.")

were "unreasonable" in light of the circumstances. Whether LabMD's security practices were unreasonable is a factual question that can be addressed only on the basis of evidence to be adduced in this proceeding.

Fourth, the Complaint alleges that the actual and potential data breaches it attributes to LabMD's data security practices caused or were likely to cause cognizable, "substantial injury" to consumers, including increased risks of "identity theft, medical identity theft," and "disclosure of sensitive private medical information." *See* Complaint, ¶ 12; *see also id.*, ¶¶ 11, 21-22. These allegations clearly refute LabMD's contentions that the Complaint contains "no allegations of monetary loss or other actual harm" nor "any actual, completed economic harms or threats to health or safety." Motion at 28-29. Moreover, occurrences of actual data security breaches or "actual, completed economic harms" (*id.* at 29) are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted "unfair . . . acts or practices." *Accord Policy Statement on Unfairness*, 104 F.T.C. at 949 n.12 (act or practice may cause "substantial injury" if it causes a "small harm to a large number of people" or "raises a significant *risk* of concrete harm") (emphasis added); *accord Neovi*, 604 F.3d at 1157 (quoting *Am. Fin. Servs.*, 767 F.2d at 972).

B. Avoidability

The Complaint contains plausible allegations that these harms could not reasonably be avoided by consumers. Consumers allegedly did not have any "way of independently knowing about respondent's security failures," let alone taking any action to remedy them or avoid the resulting harm. Complaint, ¶ 12.

C. Countervailing Benefits to Consumers or Competition

Finally, the Complaint alleges that the alleged conduct did not even benefit LabMD, much less anyone else (*id.*, ¶ 20), and that LabMD could have remedied the risks of data breaches "at relatively low cost" (*id.*, ¶ 11). These allegations provide a plausible basis for finding that the harms to consumers were not outweighed by other benefits to consumers or competition. Again, Complaint Counsel will need to prove these allegations, and LabMD will have the opportunity to refute them, on the basis of factual evidence presented at the upcoming hearing.

* * * * *

For the reasons discussed above, we deny LabMD's Motion to Dismiss.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice **IS DENIED.**

By the Commission, Commissioner Brill recused.

Donald S. Clark
Secretary

SEAL:
ISSUED: January 16, 2014

EXHIBIT 3

January 21, 2014

Via CM/ECF

The Honorable Esther Salas
United States District Court
District of New Jersey
50 Walnut Street
Newark, NJ 07101

Re: *FTC v. Wyndham Worldwide Corp., et al.*, No. 2:13-cv-01887-ES-JAD

Dear Judge Salas:

Pursuant to the Court's order of December 27, 2013, the parties in the above-captioned matter respectfully submit the following supplemental letter brief.

I. Defendants' Position

A. The FTC Lacks Statutory Authority

The FTC, like any other federal agency, must show that Congress intended to delegate to it the specific authority it claims. *See La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374-75 (1986). The FTC has not done that. Nothing in Section 5 of the FTC Act gives the Commission all-encompassing authority to regulate the data-security practices of every company in America. And, by its own admission, the FTC cannot claim that authority by virtue of Congress's supposed acquiescence in the Commission's actions to date. *See* Mot. to Dismiss Oral Arg. Tr. ("Tr.") at 48:20-22 ("As [Defendants] pointed out in the reply brief, there is little point [in] trying to read tea leaves of Congressional inaction.").

Indeed, far from giving the FTC unfettered authority to regulate data-security in ***every*** sector of the economy, Congress has carefully circumscribed the FTC's data-security powers to certain narrow, well-defined subject matters. *See* Fair Credit Reporting Act ("FCRA"), Pub. L. 91-508, codified as amended at 15 U.S.C. § 1681 *et seq*. (consumer reporting agencies); Gramm-Leach-Bliley Act ("GLBA"), Pub. L. 106-102 (financial institutions); Children's Online Privacy Protection Act ("COPPA"), Pub. L. 105-277 (websites collecting information from children). Those targeted grants of authority would make no sense if Section 5 already gave the FTC authority to regulate data security in ***all*** circumstances. *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (explaining that statutes must be interpreted to avoid surplusage and "to give effect, if possible, to every clause and word"). Instead, the much more natural interpretation of Congressional intent is that Congress understood the FTC to possess no data-security powers at all, unless and until Congress enacted the FCRA, GLBA, and COPPA.

Faced with the plain conflict between its broad interpretation of Section 5 and the narrow grants of data-security authority that Congress has actually given the Commission, the FTC argues that Congress enacted the FCRA, GLBA, and COPPA merely to supplement the FTC's

existing general police power over data-security matters. That is revisionist history. Nothing in the text or legislative history of the FCRA, GLBA, or COPPA suggests that Congress has ever understood Section 5 of the FTC Act to give the FTC general police power to regulate data-security practices, and the FTC's attempts to argue otherwise are *post hoc* rationalizations intended to create out of whole cloth a statutory basis for the FTC's actions.

The FTC initially tried to square the FCRA, GLBA, and COPPA with the Commission's broad interpretation of Section 5 on the grounds that Congress enacted those statutes merely to grant the FTC "rulemaking and/or civil penalty authority" in certain specific contexts. *See* FTC Opp'n to WHR Mot. to Dismiss ("FTC Opp'n"), ECF No. 110, at 12. But far from being limited statutes that merely add civil-penalty and rulemaking authority to Section 5, the FCRA, GLBA, and COPPA each contain detailed provisions granting the FTC ***substantive*** authority over data-security practices, *see* 15 U.S.C. §§ 1681m(e)(1), 6804(a)(1)(C), 6502(b), and explicit authority to ***enforce*** those standards in limited contexts, *see id.* §§ 1681s(a), 6805(a)(7), 6505(d). The FCRA, for instance, directs the FTC to "prescribe regulations requiring [financial institutions] to establish reasonable policies and procedures . . . to identify possible risks to account holders." *Id.* § 1681m(e)(1)(B). And the GLBA instructs the FTC to "establish appropriate standards for the financial institutions subject to [its] jurisdiction relating to administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information." *Id.* § 6801(b). Those substantive grants of authority would have been entirely unnecessary if, as the FTC claims, the FCRA, GLBA, and COPPA did no more than merely add "rulemaking and/or civil penalty" powers to the FTC's existing Section 5 authority. FTC Opp'n at 12. The far more plausible interpretation is that Congress saw those substantive-authority provisions as necessary to give the FTC any authority at all over data-security matters, fundamentally undermining the FTC's belief that Section 5 already provided it that authority. *See, e.g.*, *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) ("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there."); *United States v. Ryan*, 350 U.S. 299, 305 (1956) ("If Congress intended to deal with that problem alone, it could have done so directly.").

For the first time at oral argument, the FTC advanced a second theory of how to reconcile the FCRA, GLBA, and COPPA with the Commission's novel interpretation of Section 5. According to the FTC, Congress always understood Section 5 to provide the FTC with general police power over data-security matters, but it enacted the FCRA, GLBA, and COPPA for the limited purpose of freeing the Commission from the need to prove substantial consumer injury in specific contexts. *See* Tr. at 45:8-12 ("[T]here is no injury requirement in those cases [under the FCRA, GLBA, and COPPA], so they are dramatically different than the FTC's authority under the FTC Act. Under the FTC Act we are limited to cases where we can prove substantial [in]jury.").

That is a far-fetched reconstruction of what Congress intended to accomplish in the FCRA, GLBA, and COPPA. The text of those statutes, to begin, does not support the FTC's understanding. If Congress really had intended to do no more than simply eliminate the substantial-consumer-injury requirement of Section 5, the data-security provisions of the FCRA, GLBA, and COPPA would have said little more than: "In enforcing Section 5 of the FTC Act in these circumstances, the FTC need not prove substantial injury to consumers." Needless to say, such language cannot be found in the text of these sector-specific statutes. To the contrary, the

FCRA, GLBA, and COPPA all contain detailed provisions granting the FTC ***substantive*** authority over data-security practices, something that would have been entirely unnecessary for Congress to do under the FTC's reconstruction of Congressional intent.

The context and legislative history of the FCRA, GLBA, and COPPA further undermine the FTC's argument that those sector-specific statutes were enacted merely to free the Commission from Section 5's consumer-injury requirement and not to provide the FTC with substantive authority it otherwise lacked. The legislative record shows that each statute was enacted in response to Congressional concerns over the collection and misuse of sensitive consumer data. *See, e.g.*, 149 Cong. Rec. H12198, H12214-15 (daily ed. Nov. 21, 2003) (conference report on the 2003 amendments to the FCRA, which granted the FTC data-security authority over the disposal of consumer credit information); H.R. Rep. 106-74(III) at 117-19 (1999) (committee report on the GLBA); 144 Cong. Rec. S8482, S8482-83 (daily ed. July 17, 1998) (statement of Sen. Bryan, drafter and co-sponsor of COPPA). Congress therefore enacted the FCRA, GLBA, and COPPA precisely because it believed that data security ***was not covered by existing statutory provisions***, including Section 5 of the FTC Act. Nothing in the legislative history supports the FTC's alternative theory that Congress already understood the FTC to have universal data-security authority under Section 5, but felt it necessary to enact three statutes to eliminate the consumer-injury requirement in certain circumstances.

Indeed, it is far from clear whether the FCRA, GLBA, and COPPA actually ***do*** eliminate the substantial-injury requirement in the first place. The FCRA and COPPA direct the FTC to enforce those statutes as though they included "***all applicable terms and provisions*** of the [FTC] Act." 15 U.S.C. § 6505(d) (emphasis added); *accord id.* § 1681s(a)(1) (directing the FTC to pursue violations of the FCRA and its underlying regulations "as though the applicable terms and conditions of the [FTC] Act were part of [the FCRA]"). That necessarily means the FTC must prove substantial, unavoidable consumer injury as a part of enforcing those statutes.* And although the statutes do alter ***some*** of the background requirements of the FTC Act, *see, e.g.*, § 1681s(a)(1), no provision of the FCRA, GLBA, or COPPA purports to relieve the FTC of its duty to prove substantial consumer injury. As a result, the FTC's asserted distinction between its sweeping understanding of Section 5 and the narrow delegations of the FCRA, GLBA, and COPPA is really not distinction at all—because both sets of statutes require substantial consumer injury, the FTC's understanding of Section 5 cannot be sustained without rendering the terms of the FCRA, GLBA, and COPPA entirely superfluous.

Finally, legislation recently proposed in Congress by Senator Patrick Leahy further confirms that the FTC lacks generalized data-security authority under Section 5. *See* Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. §§ 201-04. That legislation would require businesses with access to data on 10,000 or more individuals to establish "administrative, technical, or physical safeguards identified by the Federal Trade Commission." *Id.* § 202. The bill would also grant the FTC explicit enforcement authority over the data-security requirements

---

* The provisions in the FCRA, COPPA and GLBA providing that a violation of a regulation thereunder constitutes a violation of the FTC Act do nothing to alter this conclusion. See 15 U.S.C. § 1681s(a) (FCRA); *id.* §§ 6801(b), 6805(a)(7) (GLBA); *id.* § 6505(d) (COPPA). Rather than eliminating the substantial consumer injury requirement, those provisions implicitly acknowledge that these sector-specific statutes (and regulations validly enacted thereunder) already incorporate that requirement.

established thereunder. *See id.* § 203(b) ("Any business entity shall have the provisions of this subtitle enforced against it by the Federal Trade Commission."). Again, if the Commission already possessed plenary data security authority under Section 5, such comprehensive legislation would be unnecessary.

B. The FTC Has Not Provided Fair Notice

In any event, even if the FTC were correct in its understanding of the relevant statutes, its amended complaint should still be dismissed because the FTC has not provided regulated entities with the fair notice that the Due Process Clause requires. The FTC has not published any rules, regulations, or guidelines explaining to businesses what data-security protections they must employ to comply with the FTC's interpretation of Section 5 of the FTC Act. Such a failure to publish any interpretive guidance whatsoever violates the "fundamental principle in our legal system" that "laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012). It also violates bedrock principles of administrative law, which make clear that when a statute such as Section 5 is "so vague that [its] ambiguity can only be resolved by deferring to the agency's own interpretation," the agency must at the very least state with "ascertainable certainty" what conduct is prohibited. Sec. of Labor v. Beverly Healthcare-Hillview, 541 F.3d 193, 202 (3d Cir. 2008).

The FTC's lack of guidance has not gone unnoticed. Congress has expressed concern over "the regulatory uncertainty many businesses feel already" because the FTC has failed to provide "a coherent statement of policy on how the Commission plans to enforce Section 5." See Hearing on FTC Review and Outlook before the Subcomm. on Commerce, Manuf. and Trade of the House Comm. on Energy and Commerce, 113th Cong., 2013 WL 6237638 at 3 (Dec. 3, 2013). Without such a "coherent statement," one member noted, "many businesses, large and small, are left to examining past decisions to see how they may fit into a certain set of facts." Id. Similarly, leading business organizations participating in this case have explained that current FTC enforcement practices give "no advance notice to businesses on what they are required to do to comply with the law in a rapidly changing technological environment." Br. of Amici Curiae Chamber of Commerce of the United States, et al. at 11.

Nor would it be particularly difficult for the FTC to promulgate the rules and regulations that due process requires. Although the FTC has previously claimed that it would be "impossible" to craft generalized data-security rules, at least two other federal agencies have managed to do just that—and both of those agencies did so for computer networks much more sophisticated than those involved in this litigation. See Department of Homeland Security ("DHS") Office of Inspector General, Evaluation of DHS' Information Security Program for Fiscal Year 2013 (Nov. 21, 2013), available at http://goo.gl/OC4CNx [hereinafter, "DHS Evaluation"]; National Institute of Standards and Technology ("NIST") Preliminary Cybersecurity Framework: Improving Critical Infrastructure Cybersecurity (Oct. 22, 2013), available at http://goo.gl/ivPLnq [hereinafter, "NIST Framework"]. NIST recently released for public comment a 44-page document explaining precisely what data-security protocols should be employed to protect computer networks at "critical infrastructure" locations, including facilities such as nuclear power plants. See NIST Framework at 13-27. And DHS has, since at least 2008,

assessed the state of its own internal data security using an "Information Security Scorecard" with a 0-100 rating on various, specific data-security metrics. See, e.g., DHS Evaluation at 42.

If NIST and DHS are readily able to compile a set of objective data-security standards for critical infrastructure and homeland security applications, the FTC can certainly do the same for consumer payment applications in order to satisfy constitutional fair notice requirements. Although the FTC claims it has not engaged in rulemaking because of the difficulty in crafting standards that would apply to businesses of all types and sizes, see Tr. at 77:6-9, 18-23, that variation among regulated entities is precisely why Congress and the courts require rulemaking in these types of situations—to ensure that the agency considers the views of all stakeholders and then fashions a policy or rule that remedies the problem at issue in a sensible manner, see, e.g., Hall v. EPA, 273 F.3d 1146, 1163 (9th Cir. 2001) ("[T]he point of notice-and-comment rulemaking is that public comment will be considered by an agency and the agency may alter its action in light of those comments."). The FTC's concession that different standards should apply to different businesses confirms the arbitrary nature of its current approach, which leaves businesses guessing as to what they must do to avoid running afoul of the Commission's ad hoc data security policy.

Although it concedes that it has published no rules or regulations on data-security requirements, Tr. at 69:24-70:2, the FTC argues that its prior consent decrees and an informal brochure provide all the notice that due process mandates. FTC Opp'n at 18-20. But it is well-established that third-party agency consent decrees do not constrain FTC discretion and thus cannot provide any meaningful notice to third parties. See, e.g., United States v. E.I. du Pont de Nemours & Co., 366 U.S. 316, 330 n.12 (1961); Integraph Corp. v. Intel Corp., 253 F.3d 695, 698 (Fed. Cir. 2001) ("[A] consent order does not establish illegal conduct."). And the informal brochure on which the FTC so heavily relies, see FTC Opp'n at 18-19 (citing Protecting Personal Information: A Guide for Business (2007)), is far too vague to provide meaningful guidance, particularly in the complex world of data security. For proof of that, one need look no further than the 44 pages of guidance that NIST has propounded on the same subject, much of which contains references to other, even more detailed protocols. See NIST Framework at 13-27.

For these reasons, Defendants' motions to dismiss should granted. Defendants also request leave from this Court to file a two-page reply letter after the FTC has set out its arguments below. Because the FTC raised its substantial-injury argument for the first time at oral argument, the response below is the first time Defendants will have been provided with a written articulation of the FTC's position on these issues. Defendants therefore request that the Court grant Defendants leave to file a short reply brief, so that Defendants can respond properly to the FTC's arguments.

II. Plaintiff's Position

Section 5 of the FTC Act applies by its terms to *all* unfair commercial practices that violate the three-part statutory test of 15 U.S.C. § 45(n). The plain language of Section 5 is not susceptible to a "data security" exception. Wyndham thus resorts to an argument that Section 5 must not mean what it says because, if that plain-language interpretation were correct, Congress would not have needed to enact various subsequent statutes. *See supra* p. 2. That argument is wrong because, in at least three different respects, these statutes supplement the Commission's preexisting Section 5 authority. First, as discussed below, these statutes dispense with the "consumer injury" requirement that the FTC would otherwise face in any case it brings under Section 5. Second, these newer statutes grant the FTC additional powers, such as streamlined Administrative Procedure Act rulemaking authority and civil-penalty authority, each of which the FTC would otherwise lack. *See* Pl.'s Resp. in Opp'n to Mot. to Dismiss 12, ECF No. 110 ("Pl.'s Opp'n). Third, unlike the FTC Act itself, these newer statutes affirmatively compel (rather than merely authorize) the FTC to use its consumer-protection authority in specified ways. Those many differences alone undermine Wyndham's argument that, by enacting these statutes, Congress meant to carve out an atextual "data security" exception to the Commission's Section 5 authority.

We discuss the merits of these issues below, but we first note that any doubt about the FTC's statutory authority would be dispelled by two recent developments: (1) the FTC's recent decision in *LabMD*, which is entitled to full *Chevron* deference under *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863, 1871 (2013); and (2) the D.C. Circuit's decision in *Verizon v. FCC*, No. 11-1355, 2014 WL 113946, at *11-12 (D.C. Cir. Jan. 14, 2014), which rejects a very similar argument based on *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000).

The FTC's *LabMD* order. On January 16, 2014, the Federal Trade Commission entered an order in an administratively-pending Section 5 data security case against LabMD, in which the Commission addressed many of the arguments Wyndham makes in its Motions to Dismiss. *See LabMD, Inc.*, Order Den. Resp't Mot. to Dismiss 3-14, Docket No. 9357 (F.T.C. Jan. 16, 2014), ECF No. 151-1 ("LabMD Order"). In particular, in *LabMD*, the Commission explicitly, and thoroughly, rejected an identical statutory-authority argument, removing any doubt that Section 5 authorizes the FTC to enforce unfairness in the data security context. As the Supreme Court recently confirmed, under *Chevron*, courts "must defer to an agency's interpretation of statutory ambiguity that concerns the scope of the agency's statutory authority (that is, its jurisdiction)." *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863, 1868 (2013) (citing *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837 (1984)). *See also Nat'l Cable & Telecomms Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 985 (2005) ("Before a judicial construction of a statute . . . may trump an agency's, the court must hold that the statute unambiguously requires the court's construction.").

The D.C. Circuit's Verizon decision. Wyndham's reliance on *Brown & Williamson* is untenable. *See* Pl.'s Opp'n 10-15; Mot. to Dismiss Hr'g Tr. 15-16, 45-46, ECF No. 139. The D.C. Circuit recently confirmed that point by rejecting a similar argument based on that decision for reasons that are instructive here. As the circuit court explained, the Supreme Court's

decision in *Brown & Williamson* turned on the fact "that the FDA had not only completely disclaimed any authority to regulate tobacco products, but had done so *for more than eighty years*." *Verizon*, 2014 WL 113946, at *11. Here, as previously explained, the FTC has never disclaimed its authority to enforce Section 5 unfairness in the data security context. *See* Pl.'s Opp'n 13-15, Mot. to Dismiss Hr'g Tr. 27-29; *accord* LabMD Order 7-10. Moreover, as the D.C. Circuit noted, the *Brown & Williamson* court deemed it significant "that the FDA's newly adopted conclusion that it did in fact have authority to regulate this industry would, given its findings regarding the effects of tobacco products and its authorizing statute, *logically require the agency to ban such products altogether, a result clearly contrary to congressional policy*." *Verizon*, 2014 WL 113946, at *11 (emphasis added). Like LabMD, Wyndham "can cite no similar congressional intent to preserve inadequate data security practices that unreasonably injure consumers." LabMD Order 6. Finally, none of the complementary statutes cited by Defendants conflict with the FTC's background Section 5 unfairness authority, let alone "logically require . . . a result clearly contrary to congressional policy." *Verizon*, 2014 WL 113946, at *11.

A. The FTC Act and Complementary Statutes

The Court specifically asked for supplemental briefing concerning the relationship between the FTC Act's injury requirement set forth in 15 U.S.C. § 45(n), and three other statutes the FTC enforces, all of which have data security components: the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, *et seq*. (1970, amended 2003, 2010), the Gramm-Leach-Bliley Financial Modernization Act ("GLBA"), 15 U.S.C. § 6801, *et seq*. (1999), and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501, *et seq*. (1998).

Section 45(n) limits the definition of "unfair acts or practices" under the FTC Act to those which "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). For the FCRA, GLBA, and COPPA, Congress has in essence said that a violation of the terms of these statutes is itself a sufficient injury to permit the FTC to enforce the statute in federal court. "The passage of [a] statute is, in a sense, an implied finding that violations will harm the public and ought, if necessary, be restrained." *United States v. Diapulse Corp. of Am*., 457 F.2d 25, 28 (2d Cir. 1972). *See also United States v. Cappetto*, 502 F.2d 1351, 1358-59 (7th Cir. 1974). For example, Congress has determined that when a credit reporting agency violates the FCRA by furnishing a consumer's financial data without a permissible purpose, that violation causes consumer injury. *See Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142 (D.C. Cir. 2001) ("*Trans Union I*") ("[T]he government cannot promote its interest (protection of personal financial data) except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent."). *See also Trans Union LLC v. FTC*, 295 F.3d 42, 53 (D.C. Cir. 2002) ("*Trans Union II*") (as in *Trans Union I*, in the GLBA context, the dissemination of financial data causes the very harm the government seeks to prevent).[1]

[1] Defendants suggest the language in the FCRA and COPPA stating the terms and provisions of the FTC Act are incorporated into those statutes requires the FTC to meet the Section 45(n) substantial injury requirement before it can enforce those statutes. *Supra* pp. 3-4. Section 45(n) places limitations on the Commission's authority to declare

These newer statutes also grant the FTC additional enforcement tools, further differentiating them from the FTC Act. Pl.'s Opp'n 10-12. As the Commission held in *LabMD*, Congress enacted the FCRA, GLBA, and COPPA to address specific concerns in particular sectors of the economy. LabMD Order 10. *See* FCRA, 15 U.S.C. § 1681a (consumer reporting agencies); GLBA, 15 U.S.C. § 6801(a) (financial institutions); COPPA, 15 U.S.C. §§ 6501-6508; 144 Cong. Rec. S12787 (daily ed. Oct. 21, 1998) (statement of Sen. Bryan, drafter and co-sponsor of COPPA) ("The goals of this legislation are: . . . to maintain the security of personally identifiable information of children collected online; and [] to protect children's privacy."). *See also* Mot. to Dismiss Hr'g Tr. 44:17-25; 45:1-22. As the Commission noted, these statutes not only impose specific regulatory requirements on companies in particular areas, but they provide the FTC with additional tools to protect consumers. *See* LabMD Order 10. One of those tools is Administrative Procedure Act rulemaking authority. *See* GLBA, 15 U.S.C. §§ 6801(b), 6805(b)(2); COPPA, 15 U.S.C. § 6502(b)(1)(D); FCRA, 15 U.S.C. § 1681w. Another tool is civil penalty authority, which is not available under Section 5. *See* FCRA, 15 U.S.C. § 1681s; COPPA, 15 U.S.C. § 6505(d). *See also* LabMD Order 10.

Moreover, as opposed to the FTC Act which merely authorizes, the FCRA, GLBA, and COPPA affirmatively compel the FTC to use its authority in particular ways. For example, COPPA instructs the FTC to promulgate rules addressing the specific duties of child-directed website operators to provide notices and obtain parental consent before collecting or disclosing children's personal information. 15 U.S.C. § 6502(b). *See also* FCRA, 15 U.S.C. § 1681w (requiring the FTC to issue regulations requiring proper disposal of consumer information); LabMD Order 10. "Of course, by *compelling* the Commission to take particular steps in those contexts, Congress did not somehow divest the Commission of its preexisting and much broader *authority* to protect consumers against 'unfair' practices." LabMD Order 13. *See also Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-06 (D.C. Cir. 2011).

Again, any question about the FTC's authority in the data security area is put to rest by the *LabMD* decision. In *LabMD*, the unanimous Commission specifically addressed the FCRA, GLBA, and COPPA, holding that "these laws *recognized* the Commission's *existing* enforcement authority, *expanded* that authority in particular respects, and affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts." LabMD Order 10. "To conclude otherwise," the Commission held, "would disregard Congress's instruction to the Commission to protect consumers from harmful practices in evolving technological and marketplace environments." *Id.* As the Commission noted, Section 5 of the FTC Act is an intentionally broad grant of power to the FTC to protect consumers from "unfair or deceptive acts or practices in or affecting commerce." *Id.* at 3-6. This grant of authority applies to *all* acts or practices in or affecting commerce. It is not limited to specific acts or practices, nor was it intended to be. *See* Pl.'s Opp'n 11. There is nothing unique about data security that exempts it from this broad authority. In fact, the Commission held, Congress intended the FTC to "ascertain, on a case-by-case basis, which specific practices should be condemned as 'unfair.'" LabMD Order 5. These findings all warrant substantial deference.

---

particular actions unfair under Section 5, either in litigation or rulemaking. It has no application where Congress itself has statutorily defined categories of actions to be unlawful and authorized the FTC to enforce those statues.

"Statutory ambiguities will be resolved, within the bounds of reasonable interpretation, not by the court but by the administering agency." *City of Arlington*, 133 S. Ct. at 1868, 1871.

B. Fair Notice

Although the Court did not request briefing on the topic, Defendants return to the untenable claim that the FTC has not satisfied due process fair notice requirements because it has not issued a comprehensive rule on data security. *Supra* pp. 4-5. This argument has no basis in the law. *See* Pl.'s Opp'n 17-25. Were Defendants correct, the FTC could never protect consumers from unfair practices without first issuing a regulation governing the specific practice at issue. Such a requirement would undermine 100 years of FTC precedent, and it would crash headlong into the Supreme Court's recognition that "the proscriptions in [Section] 5 are flexible, to be defined with particularity by the myriad of cases from the field of business," a fact that inherently requires the FTC to apply Section 5 "to the facts of particular cases arising out of unprecedented situations." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965). *See also FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (Congress delegated broad authority "to the Commission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply."). Indeed, such a requirement would be an exercise in futility because "[t]here is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *Sperry & Hutchinson Co.*, 405 U.S. at 241.

Section 45(n)'s three part test addressing when an act or practice is "unfair" adequately provides "a person of ordinary intelligence fair notice of what is prohibited" and constrains the FTC's authority to bring unfairness actions sufficiently so that the FTC may not enforce the FTC Act in a "seriously discriminatory" way. *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). *See also* LabMD Order 15-17. Agencies routinely bring enforcement actions where the governing statute or rules lack particularized prohibitions, and instead require compliance with a general reasonableness standard like that set forth in Section 45(n). *See* Pl.'s Opp'n 23-24 (discussing the National Labor Relations Board's "good faith" requirement, and the Occupational Safety and Health Act's "general duty clause."). In fact, this Circuit has rejected fair notice challenges to similar reasonableness standards. *See Voegele Co., Inc. v. Occupational Safety & Health Review Comm'n*, 625 F.2d 1075, 1078 (3d Cir. 1980).[2]

[2] Without acknowledging the discussion of the case at the Motion to Dismiss Hearing, Defendants cite to *Secretary of Labor v. Beverly Healthcare-Hillview* ("*Beverly*"), 541 F.3d 193 (3d Cir. 2008), in baldly asserting that to satisfy fair notice requirements the FTC must provide "ascertainable certainty" of how it will enforce Section 5 unfairness. *See supra* p. 4. As the FTC explained at the hearing, however, the ascertainable certainty test set forth in *Beverly* does not apply here. *Beverly*, 541 F.3d at 202. The FTC has not given "conflicting public interpretations" of how it will apply "unfairness." Rather, the FTC has repeatedly, and publicly, explained that it will enforce unfairness consistent with the unambiguous plain terms of the statute, which defines unfair acts or practices through the Section 45(n) balancing test. *See United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004); Mot. to Dismiss Hr'g Tr. 72-74; Pl.'s Opp'n 13-14, 17-20. In fact, the FTC's many public complaints and consent agreements, as well as public statements and business guidance, have provided further contour to the Section 45(n) test as it is applied in the data security context. Pl.'s Opp'n 18-20. Any doubt as to whether the FTC meets fair notice here is settled in this Circuit by *Voegele*, which noted that similar "reasonable person" standards survive fair notice challenges even though they provide no guidance other than to act as a reasonable person would. 625 F.2d at 1078 (citing *B&B Insulation, Inc. v. Occupational Safety & Health Review Comm'n*, 583 F.2d 1364 (5th Cir. 1978)). *See also* LabMD Order 18-19.

Moreover, the FTC's decision to enforce the FTC Act's prohibition of unfair practices through individual enforcement actions rather than rulemaking is well within the FTC's "informed discretion." *PBW Stock Exch., Inc. v. SEC*, 485 F.2d 718, 732 (3d Cir. 1973). *See also SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947); Pl.'s Opp'n 20-22; LabMD Order 14-15. "[A]gency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication[,] [and] [t]he Commission seems on especially solid ground in choosing an individualized process where important factors may vary radically from case to case." *Am. Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990).[3]

Accordingly, courts routinely uphold FTC unfairness actions despite the fact that there are no preexisting rules specifically governing the specific conduct at issue. In *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010), the Ninth Circuit affirmed the district court's holding that the defendants' acts or practices related to online check drafting and delivery were unfair even though there is no specific regulation addressing the practice. The Tenth Circuit reached the same conclusion in *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009), even though no regulation explicitly prohibited the conduct in question. *See also* Pl.'s Opp'n 11. In short, Defendants' claim that the FTC must issue regulations governing data security before it may enforce its unfairness authority is inconsistent with the FTC's long enforcement history.

Moreover, as the Commission held in *LabMD*, the claim that agencies can only satisfy due process through issuing specific regulations is "particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care," and when they "find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages." LabMD Order at 17. "There is simply no basis to conclude that the FTC's application of the Section [45](n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties." *Id.*[4]

For the reasons set forth above, and in prior briefing and argument, the Court should deny Defendants' Motions to Dismiss.

---

[3] Nor is that doctrine altered by the National Institute of Standards and Technology's ("NIST") critical infrastructure cyber security framework or the Department of Homeland Security's ("DHS") internal network assessment. *See supra* p. 5. The NIST framework is not an enforceable regulation requiring specific security measures. *See* Pl.'s Opp'n 16. Rather, it sets forth a voluntary *process* by which critical infrastructures can assess the threats they face and the protections they should reasonably take in response. *See, e.g.*, Exec. Order 13636, 78 FR 11737 (2013). The DHS Report is DHS's own internal assessment of its network security, and has no bearing on this case.

[4] In support of their claim that the FTC must make rules in the data security area, Defendants offer a single comment of a Congressman at a Subcommittee hearing (which in context appears actually to be about the FTC's competition-side efforts and not consumer protection unfairness actions), and an amicus brief from the U.S. Chamber of Commerce. *See supra* p. 5. Whatever weight should be accorded a single comment in a Subcommittee hearing, and an amicus brief, these statements cannot overcome the well-settled precedent holding that the FTC comports with due process even when proceeding through adjudication, rather than rulemaking. Pl.'s Opp'n 20-22.

Dated: January 21, 2014

/s/Jonathan E. Zimmerman
Lisa Weintraub Schifferle
Kristin Krause Cohen
Kevin H. Moriarty
John A. Krebs
Jonathan E. Zimmerman
Andrea V. Arias
Federal Trade Commission
600 Pennsylvania Ave., NW
Mail Stop NJ-8100
Washington, D.C. 20580

Attorneys for Plaintiff
Federal Trade Commission

/s/ Jennifer A. Hradil
Jennifer A. Hradil, Esq.
Justin T. Quinn, Esq.
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102-5310
(973) 596-4500

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice
K. Winn Allen, DC Bar 1000590
Pro Hac Vice
KIRKLAND & ELLIS, LLP
655 Fifteenth St. N.W.
Washington, D.C. 20005
(202) 879-5078
eugene.assaf@kirkland.com
winn.allen@kirkland.com

Douglas H. Meal, MA Bar 340971
Pro Hac Vice
David T. Cohen, MA Bar 670153
Pro Hac Vice
ROPES & GRAY, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517
douglas.meal@ropesgray.com
david.cohen@ropesgray.com

Attorneys for Defendants

cc: Counsel via ECF

KE 29388388.1

EXHIBIT 4

1023099

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that LabMD, Inc. ("LabMD" or "respondent"), a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

RESPONDENT'S BUSINESS

1. Respondent LabMD is a Georgia corporation with its principal office or place of business at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339.

2. The acts and practices of respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

3. Since at least 2001, respondent has been in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers.

4. Respondent files insurance claims for charges related to the clinical laboratory tests with health insurance companies. Insured consumers typically pay the part of respondent's charges not covered by insurance; uninsured consumers are responsible for the full amount of the charges. Consumers in many instances pay respondent's charges with credit cards or personal checks.

5. Respondent tests samples from consumers located throughout the United States.

6. In performing tests, respondent routinely obtains information about consumers, including, but not limited to: names; addresses; dates of birth; gender; telephone numbers; Social Security numbers ("SSN"); medical record numbers; bank account or credit card information; health care provider names, addresses, and telephone numbers; laboratory tests, test codes and results, and diagnoses; clinical histories; and health insurance company names and policy numbers (collectively, "personal information").

7. Respondent has accumulated and maintains personal information for nearly one million consumers.

8. Respondent operates computer networks in conducting its business. The computer networks include computers, servers, and other devices in respondent's corporate offices and laboratory, computers used by its personnel in different parts of the country, and computers that respondent provides to some health care providers.

9. Among other things, respondent uses the computer networks to: receive orders for tests from health care providers; report test results to health care providers; file insurance claims with health insurance companies; prepare bills and other correspondence to consumers; obtain approvals for payments made by consumers with credit cards; and prepare medical records. For example, respondent's billing department uses the computer networks to generate or access documents related to processing claims and payments, such as:

   (a) monthly spreadsheets of insurance claims and payments ("insurance aging reports"), which may include personal information such as consumer names, dates of birth, SSNs, the American Medical Association current procedural terminology ("CPT") codes for the laboratory test conducted, and health insurance company names, addresses, and policy numbers;

   (b) spreadsheets of payments received from consumers ("Day Sheets"), which may include personal information such as consumer names, SSNs, and methods, amounts, and dates of payments; and

   (c) copies of consumer checks, which may include personal information such as names, addresses, telephone numbers, payment amounts, bank names and routing numbers, and bank account numbers ("copied checks").

RESPONDENT'S SECURITY PRACTICES

10. At all relevant times, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, respondent:

    (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Thus, for example, employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure;

    (b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of its networks;

    (c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;

    (d) did not adequately train employees to safeguard personal information;

    (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;

    (f) did not maintain and update operating systems of computers and other devices on its networks. For example, on some computers respondent used operating systems that were unsupported by the vendor, making it unlikely that the systems would be updated to address newly discovered vulnerabilities; and

    (g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its networks. As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks.

11. Respondent could have corrected its security failures at relatively low cost using readily available security measures.

12. Consumers have no way of independently knowing about respondent's security failures and could not reasonably avoid possible harms from such failures, including identity theft, medical identity theft, and other harms, such as disclosure of sensitive, private medical information.

PEER-TO-PEER FILE SHARING APPLICATIONS

13. Peer-to-peer ("P2P") file sharing applications are often used to share music, videos, pictures, and other materials between persons and entities using computers with the same or a compatible P2P application ("P2P network").

14. P2P applications allow a user to both designate files on the user's computer that are available to others on a P2P network and search for and access designated files on other computers on the P2P network.

15. After a designated file is shared with another computer, it can be passed along among other P2P network users without being downloaded again from the original source. Generally, once shared, a file cannot with certainty be removed permanently from a P2P network.

16. Since at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks.

SECURITY INCIDENTS

17. In May 2008, a third party informed respondent that its June 2007 insurance aging report (the "P2P insurance aging file") was available on a P2P network through Limewire, a P2P file sharing application.

18. After receiving the May 2008 notice that the P2P insurance aging file was available through Limewire, respondent determined that:

    (a) Limewire had been downloaded and installed on a computer used by respondent's billing department manager (the "billing computer");

    (b) at that point in time, the P2P insurance aging file was one of hundreds of files that were designated for sharing from the billing computer using Limewire; and

    (c) Limewire had been installed on the billing computer no later than 2006.

19. The P2P insurance aging file contains personal information about approximately 9,300 consumers, including names, dates of birth, SSNs, CPT codes, and, in many instances, health insurance company names, addresses, and policy numbers.

20. Respondent had no business need for Limewire and removed it from the billing computer in May 2008, after receiving notice.

21. In October 2012, the Sacramento, California Police Department found more than 35 Day Sheets and a small number of copied checks in the possession of individuals who pleaded no contest to state charges of identity theft. These Day Sheets include personal information, such as names and SSNs, of several hundred consumers in different states. Many of these consumers were not included in the P2P insurance aging file, and some of the information post-dates the P2P insurance aging file. A number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves.

VIOLATION OF THE FTC ACT

22. As set forth in Paragraphs 6 through 21, respondent's failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, SSNs, medical test codes, and health information, caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

23. The acts and practices of respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a).

NOTICE

Notice is hereby given to the respondent that the twenty-eighth day of April, 2014, at 10:00 a.m., is hereby fixed as the time, and the Federal Trade Commission offices at 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580, as the place when and where a hearing will be had before an Administrative Law Judge of the Federal Trade Commission, on the charges set forth in this complaint, at which time and place you will have the right under the Federal Trade Commission Act to appear and show cause why an order should not be entered requiring you to cease and desist from the violations of law charged in this complaint.

You are notified that the opportunity is afforded you to file with the Federal Trade Commission an answer to this complaint on or before the fourteenth (14th) day after service of it upon you. An answer in which the allegations of the complaint are contested shall contain a concise statement of the facts constituting each ground of defense; and specific admission, denial, or explanation of each fact alleged in the complaint or, if you are without knowledge thereof, a statement to that effect. Allegations of the complaint not thus answered shall be deemed to have been admitted.

If you elect not to contest the allegations of fact set forth in the complaint, the answer shall consist of a statement that you admit all of the material facts to be true. Such an answer shall constitute a waiver of hearings as to the facts alleged in the complaint and, together with the complaint, will provide a record basis on which the Commission shall issue a final decision containing appropriate findings and conclusions, and a final order disposing of the proceeding. In such answer, you may, however, reserve the right to submit proposed findings of fact and conclusions of law under Rule 3.46 of the Commission's Rules of Practice for Adjudicative Proceedings.

Failure to answer within the time above provided shall be deemed to constitute a waiver of your right to appear and to contest the allegations of the complaint, and shall authorize the Commission, without further notice to you, to find the facts to be as alleged in the complaint and to enter a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding.

The Administrative Law Judge shall hold a prehearing scheduling conference not later than ten (10) days after the answer is filed by the respondent. Unless otherwise directed by the Administrative Law Judge, the scheduling conference and further proceedings will take place at the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580. Rule 3.21(a) requires a meeting of the parties' counsel as early as practicable before the prehearing scheduling conference, but in any event no later than five (5) days after the answer is filed by the respondent. Rule 3.31(b) obligates counsel for each party, within five (5) days of receiving respondent's answer, to make certain disclosures without awaiting a formal discovery request.

The following is the form of order which the Commission has reason to believe should issue if the facts are found to be as alleged in the complaint. If, however, the Commission should conclude from record facts developed in any adjudicative proceedings in this matter that the proposed order provisions might be inadequate to fully protect the consuming public, the Commission may order such other relief as it finds necessary or appropriate.

Moreover, the Commission has reason to believe that, if the facts are found as alleged in the complaint, it may be necessary and appropriate for the Commission to seek relief to redress injury to consumers, or other persons, partnerships or corporations, in the form of restitution for past, present, and future consumers and such other types of relief as are set forth in Section 19(b) of the Federal Trade Commission Act. The Commission will determine whether to apply to a court for such relief on the basis of the adjudicative proceedings in this matter and such other factors as are relevant to consider the necessity and appropriateness of such action.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

2. Unless otherwise specified, "respondent" shall mean LabMD, Inc., and its successors and assigns.

3. "Affected Individual" shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before the date of service of this order, including, but not limited to, consumers listed in the Insurance File and the Sacramento Documents.

4. "Insurance File" shall mean the file containing personal information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, health insurance company names and policy numbers, and medical test codes, that was available to a peer-to-peer file sharing network through a peer-to-peer file sharing application installed on a computer on respondent's computer network.

5. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.

6. "Sacramento Documents" shall mean the documents identified in Appendix A.

I.

IT IS ORDERED that the respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and

D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No.1023099. Provided, however, that in lieu of overnight courier, assessments may be sent by first-class mail, but only if an electronic version of any such assessment is contemporaneously sent to the Commission at Debrief@ftc.gov.

III.

IT IS FURTHER ORDERED that respondent shall provide notice to Affected Individuals and their health insurance companies within 60 days of service of this order unless an appropriate notice has already been provided, as follows:

A. Respondent shall send the notice to each Affected Individual by first class mail, only after obtaining acknowledgment from the Commission or its staff that the form and substance of the notice satisfies the provisions of the order. The notice must be easy to understand and must include:

1. a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.),

and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

2. advice on how Affected Individuals can protect themselves from identity theft or related harms. Respondent may refer Affected Individuals to the Commission's identity theft website (www.ftc.gov/idtheft), advise them to contact their health care providers or insurance companies if bills don't arrive on time or contain irregularities, or to obtain a free copy of their credit report from www.annualcreditreport.com and monitor it and their accounts for suspicious activity, or take such other steps as respondent deems appropriate; and

3. methods by which Affected Individuals can contact respondent for more information, including a toll-free number for 90 days after notice to Affected Individuals, an email address, a website, and mailing address.

B. Respondent shall send a copy of the notice to each Affected Individual's health insurance company by first class mail.

C. If respondent does not have an Affected Individual's mailing address in its possession, it shall make reasonable efforts to find such mailing address, such as by reviewing online directories, and once found, shall provide the notice described in Subpart A, above.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, notice letters required by Part III of this order and documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to: (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order; and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099.

VIII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that each respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

IN WITNESS WHEREOF, the Federal Trade Commission has caused this complaint to be signed by its Secretary and its official seal to be hereto affixed, at Washington, D.C. this twenty-eighth day of August, 2013.

By the Commission.

Donald S. Clark
Secretary

EXHIBIT 5

Dissenting Statement of Commissioner J. Thomas Rosch
Petitions of LabMD, Inc. and Michael J. Daugherty
to Limit or Quash the Civil Investigative Demands

FTC File No. 1023099
June 21, 2012

I dissent from the Commission's vote affirming Commissioner Brill's letter decision, dated April 20, 2012, that denied the petitions of LabMD, Inc. and Michael J. Daugherty to limit or quash the civil investigative demands.

I generally agree with Commissioner Brill's decision to enforce the document requests and interrogatories, and to allow investigational hearings to proceed. As she has concluded, further discovery may establish that there is indeed reason to believe there is Section 5 liability regarding petitioners' security failings *independent* of the "1,718 File" (the 1,718 page spreadsheet containing sensitive personally identifiable information regarding approximately 9,000 patients) that was originally discovered through the efforts of Dartmouth Professor M. Eric Johnson and Tiversa, Inc. In my view, however, as a matter of prosecutorial discretion under the unique circumstances posed by this investigation, the CIDs should be limited. Accordingly, without reaching the merits of petitioners' legal claims, I do not agree that staff should further inquire – either by document request, interrogatory, or investigational hearing – about the 1,718 File.

Specifically, I am concerned that Tiversa is more than an ordinary witness, informant, or "whistle-blower." It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations. Indeed, in the instant matter, an argument has been raised that Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve the 1,718 File, and then repeatedly solicited LabMD, offering

investigative and remediation services regarding the breach, long before Commission staff contacted LabMD. In my view, while there appears to be nothing *per se* unlawful about this evidence, the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

EXHIBIT 6

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC

Office of the Secretary

April 20, 2012

VIA E-MAIL AND COURIER DELIVERY

Claudia Callaway, Esq.
Christina Grigorian, Esq.
Julian Dayal, Esq.
Katten Muchin Rosenman LLP
2900 K Street, N.W.
North Tower - Suite 200
Washington, D.C. 20007
E-mail: claudia.callaway@kattenlaw.com

RE: *LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand*; and *Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand*

Dear Ms. Callaway, Ms. Grigorian, and Mr. Dayal:

On January 10, 2012, the Federal Trade Commission ("FTC" or "Commission") received the above Petitions filed by LabMD, Inc. ("LabMD") and its President, Michael J. Daugherty (collectively, "Petitioners"). This letter advises you of the Commission's disposition of the Petitions, effected through this ruling by Commissioner Julie Brill, acting as the Commission's delegate.[1]

For the reasons explained below, the Petitions are denied. You may request review of this ruling by the full Commission.[2] Any such request must be filed with the Secretary of the Commission within three days after service of this letter ruling.[3] The timely filing

[1] *See* 16 C.F.R. § 2.7(d)(4).

[2] 16 C.F.R. § 2.7(f).

[3] *Id.* This ruling is being delivered by e-mail and courier delivery. The e-mail copy is provided as a courtesy, and the deadline by which an appeal to the full Commission

of a request for review by the full Commission shall not stay the return dates established by this ruling.[4]

I. INTRODUCTION

The FTC commenced its investigation into the adequacy of LabMD's information security practices in January 2010, after a LabMD file had been discovered on a peer-to-peer ("P2P") file sharing network.[5] The file, which Petitioners call the "1,718 File" because it is 1,718 pages long, is a spreadsheet of health insurance billing information for uropathology and microbiology medical tests of around 9,000 patients. It contains highly sensitive information about these consumers, including:

- Name;
- Social Security Number;
- Date of birth;
- Health insurance provider and policy number; and
- Standardized medical treatment codes.[6]

Such information can be misused to harm consumers.

The purpose of the investigation is to determine whether Petitioners violated the FTC Act by engaging in deceptive or unfair acts or practices relating to privacy or information security. The inquiry is authorized by Resolution File No. P954807, which provides for the use of compulsory process in investigations of potential Section 5 violations involving "consumer privacy and/or data security."

---

would have to be filed should be calculated from the date on which you receive the original letter by courier delivery.

[4] *Id.*

[5] P2P programs allow users to form networks with others using the same or a compatible P2P program. Such programs allow users to locate and retrieve files of interest to them that are stored on computers of other users on the networks.

[6] LabMD Pet., Ex. C, at Fig. 4. Because the LabMD and Daugherty Petitions make the same arguments (the Petitions differ only in details about the submitter), we generally cite only to LabMD's Petition.

The investigation began with voluntary information requests for documents and information about LabMD's information security policies, procedures, practices, and training generally, as well as information about security incidents, including, but not limited to, the discovery of the 1,718 File on P2P networks. In response, LabMD produced hundreds of pages of documents, including supplements and responses to follow-up questions. To complete the investigation, staff requested issuance of CIDs to LabMD and Michael J. Daugherty, LabMD's President.

The Commission issued the CIDs on December 21, 2011. Both require testimony relating to information security policies, practices, training, and procedures. They also include a limited number of interrogatories that require Petitioners to identify documents used by the witnesses to prepare for their testimony.[7] The LabMD CID also includes a single document request asking for only those documents that were both identified in response to the CID's interrogatories and had not been previously produced to staff.[8]

Petitioners seek to quash or limit the CIDs because, they claim, the CIDs "appear to be premised on" the download of the 1,718 File (hereinafter, the "File disclosure").[9] Their principal objection relates to the merits of the investigation. In particular, they contend (without citing any authority) that the Commission must have a "justifiable" belief that a law violation has occurred before it can issue CIDs, and that the File disclosure cannot support such a belief. They claim that the File disclosure occurred not because LabMD failed to implement reasonable and appropriate security measures, but because the company was the victim of an illegal intrusion conducted by Tiversa (a P2P information technology and investigation services company) and Dartmouth College faculty using Tiversa's powerful P2P searching technology.[10] Further, Petitioners argue that no actual harm to consumers resulted from the File disclosure.[11] Accordingly, they

---

[7] LabMD Pet., Ex. A.

[8] LabMD Pet., Ex. A.

[9] LabMD Pet., at 1.

[10] Petitioners claim that in the course of a Department of Homeland Security-funded research project, Professor M. Eric Johnson of Dartmouth College's Tuck School of Business and Tiversa used Tiversa's P2P searching technology to search for and then download the file. LabMD Pet., at 3-4, 7, & Ex. F, at 10-12.

[11] The Petitions claim that there is no allegation of actual consumer injury from the File disclosure. LabMD Pet., at 7.

contend that investigating either the File disclosure or the adequacy of LabMD's security practices is improper because no law violation can have occurred, and that the CIDs therefore should be quashed.[12]

As discussed below, these arguments are undermined by: (1) the obvious point that an investigation necessarily must precede assessment of whether there is reason to believe a law violation may have occurred (in any matter); (2) the scope of the authorizing resolution; and (3) the language of the FTC Act. The resolution authorizes use of compulsory process in an investigation to determine whether Petitioners engaged in deceptive or unfair practices related to privacy or security. Petitioners' focus on the File disclosure is misplaced – it may bear on the adequacy of LabMD's security practices under the FTC Act but does not establish the investigation's scope under the resolution.[13] Further, in such an investigation Section 5 directs the Commission to consider whether security practices are unfair because they create a sufficient risk of harm, even if no harm has been reported.

Petitioners make two additional arguments in support of their Petitions. First, they argue that the resolution authorizing the CIDs did not provide them with sufficient notice of the purpose and scope of the investigation. Second, they argue that the FTC is without jurisdiction to pursue this investigation. Both of these additional arguments are equally without merit.

II. ANALYSIS

A. The applicable legal standards.

Compulsory process such as a CID is proper if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant to the inquiry, as that inquiry is defined by the investigatory resolution.[14]

---

[12] LabMD Pet., at 7-8.

[13] *See, e.g.*, *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008) (confirming that the scope of an investigation authorized by Resolution P954807 properly included all of CVS' "consumer privacy and data security practices" (including its computer security practices) and could not be limited (as the company argued) to just known incidents of unauthorized disposal of paper documents in dumpsters).

[14] *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

Agencies have wide latitude to determine what information is relevant to their law enforcement investigations and are not required to have "a justifiable belief that wrongdoing has actually occurred," as Petitioners claim.[15] As the D.C. Circuit has stated, "The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one . . . . The requested material, therefore, need only be relevant to the *investigation* – the boundary of which may be defined quite generally, as it was in the Commission's resolution here."[16] Agencies thus have "extreme breadth" in conducting their investigations,[17] and "in light of [this] broad deference . . ., it is essentially the respondent's burden to show that the information is irrelevant."[18]

B. The CIDs satisfy the foregoing standards.

Petitioners argue that the CIDs are improper for several reasons. In particular, they claim no law violation could have occurred, by arguing that: (1) not even "perfect" security measures (let alone the reasonable security measure standard the Commission uses to determine whether a law violation may have occurred) could have prevented the File disclosure because Tiversa's technology "can penetrate even the most robust network security,"[19] and (2) no actual injury resulted from the File disclosure.

---

[15] LabMD Pet., at 6. *See, e.g.*, *Morton Salt*, 338 U.S. at 642-43 ("[Administrative agencies have] a power of inquisition, if one chooses to call it that, which is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence but can investigate merely on suspicion that the law is being violated, or even just because it wants an assurance that it is not.").

[16] *Invention Submission*, 965 F.2d at 1090 (emphasis in original, internal citations omitted) (citing *FTC v. Carter*, 636 F.2d 781, 787-88 (D.C. Cir. 1980), and *Texaco*, 555 F.2d at 874 & n.26).

[17] *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1517 (D.C. Cir. 1993) (citing *Texaco*, 555 F.2d at 882).

[18] *Invention Submission*, 965 F.2d at 1090 (citing *Texaco*, 555 F.2d at 882) ("burden of showing that the request is unreasonable is on the subpoenaed party"). *Accord FTC v. Church & Dwight Co.*, 756 F. Supp. 2d 81, 85 (D.D.C. 2010).

[19] LabMD Pet., at 7.

The Commission is not required, as a precondition to conducting a law enforcement investigation, to make a showing that it is likely that a law violation has occurred. The D.C. Circuit confirmed this point in *FTC v. Texaco, Inc.*, when it stated, "[I]n the pre-complaint stage, an investigating agency is under no obligation to propound a narrowly focused theory of a possible future case . . . . The court must not lose sight of the fact that the agency is merely exercising its legitimate right to determine the facts, and that a complaint may not, and need not, ever issue."[20] Here, Petitioners seek to quash the CIDs by asserting that LabMD's practices must have been reasonable under the FTC Act because the 1,718 File was retrieved using Tiversa's powerful searching technology. Accepting this argument would prevent the Commission from exploring relevant issues bearing on reasonableness, such as, for example, whether the company's security practices could have prevented the 1,718 File from being retrieved using the common P2P programs that are used by millions of computer users each day or whether there were readily available security measures LabMD did not implement that would have prevented even Tiversa's technology from successfully retrieving the file. Although such evidence (if it exists at all) could undermine their reasonableness claim, Petitioners nonetheless argue that the Commission cannot use CIDs to investigate whether the evidence exists unless it already has reason to believe it does exist. For this reason, Petitioners' argument that the strength of Tiversa's P2P searching technology precludes the possibility that a law violation occurred, regardless of the state of LabMD's security, must fail.

Similarly, Petitioners' assertion that no law violation can have occurred because no actual harm has been shown also fails because, under Section 5, a failure to implement reasonable security measures may be an unfair act or practice if the failure is *likely* to cause harm. No showing of actual harm is needed.[21]

Both arguments conflate the purpose of a CID with the purpose of a future potential complaint. A CID can only compel information necessary for an investigation, and the investigation may or may not result in allegations of a law violation.[22]

---

[20] 555 F.2d 862, 874 (D.C. Cir. 1977). This holding from *Texaco* has been repeatedly reaffirmed, most recently in *FTC v. Church & Dwight*, 747 F. Supp. 2d 3, 6, *aff'd*, 2011 U.S. App. LEXIS 24587 (D.C. Cir. Dec. 13, 2011).

[21] 15 U.S.C. § 45(n) (an unfair practice is one that "causes or *is likely to cause* substantial injury to consumers"); *see also* FTC Policy Statement on Unfairness, 104 F.T.C. 949, 1073 & n.15 (1984).

[22] Petitioners also argue that the CIDs are improper for other reasons. They claim that because security issues posed by P2P programs were common (according to Tiversa), such issues could not constitute an unfair or deceptive practice in violation of the FTC

Additionally, Petitioners have claimed that the CIDs are burdensome, but they have not come forward with any support for these assertions. Instead, they make only bald statements that the CIDs are "highly burdensome," "unduly burdensome," "costly and burdensome," and "deeply burdensome."[23] Having offered no factual information about the alleged burdens of complying with the CIDs, Petitioners have not sustained their burden to demonstrate that the CIDs are unduly burdensome.[24]

Such a showing would be difficult here in any event. Notwithstanding Petitioners' description, the CIDs call primarily for testimony, not documents. Thus, it seems unlikely that compliance would require large-scale or time-consuming document production.

Act. LabMD Pet., at 7-8 & n.34. This argument is unavailing. The fact that a particular practice may be pervasive or widespread has no bearing on whether the FTC may investigate it as also deceptive or unfair. Indeed, accepting Petitioners' argument would confine the FTC to investigating only those activities that were rare or uncommon, thus crippling the agency's law enforcement mission. Along the same lines, Petitioners contend that the risks of P2P technology, and the resulting potential liabilities to businesses, were not known in 2008, when the File disclosure occurred. In support of this claim, they assert that the FTC did not notify businesses or publish guidance about P2P until 2010. LabMD Pet., at 8. In fact, many, including the FTC, warned about the risks presented by P2P programs years before the File disclosure occurred. *See, e.g.*, FTC Staff Report, "Peer-to-Peer File Sharing Technology: Consumer Protection and Competition Issues" (June 2005), available at http://www.ftc.gov/reports/ p2p05/050623p2prpt.pdf; Prepared Statement of the Federal Trade Commission Before The Committee on Oversight and Government Reform, United States House of Representatives (July 24, 2007) (discussing P2P programs and risks), available at http://www.ftc.gov/os/testimony/P034517p2pshare.pdf.

[23] LabMD Pet., at 7, 9, & 10.

[24] *See, e.g.*, *Texaco*, 555 F.2d at 882 ("The burden of showing that the request is unreasonable is on the subpoenaed party.") (citing *United States v. Powell*, 379 U.S. 48, 58 (1964)); *accord EEOC v. Maryland Cup Corp.*, 785 F.2d 471, 476 (4th Cir. 1986) (subpoena is enforceable absent a showing by recipient that the requests are unduly burdensome); *FTC v. Standard American, Inc.*, 306 F.2d 231, 235 (3d Cir. 1962) (recipient has responsibility to show burden and must make "a record . . . of the measure of their grievance rather than ask [the court] to assume it"); *In re Nat'l Claims Serv., Inc.*, 125 F.T.C. 1325, 1328-29 (1998) (FTC ruling that petition to quash must substantiate burden with specific factual detail).

Furthermore, to the extent that the CIDs call for narrative responses, they merely require Petitioners to identify documents related to the requested testimony. In fact, there is only one specification that requires the production of documents, and even that specification is limited to documents identified in response to the interrogatories to the extent they were "not already been produced to the FTC."[25]

Finally, Petitioners, without explaining its relevance, contend that the timing of the CIDs is "troubling," coming after LabMD's conduct had been reviewed by two congressional committees, and after LabMD filed suit against Tiversa and others alleging conversion and trespass, among other violations, based on the File disclosure in 2008.[26] Though Petitioners seem to believe that there is some connection between their rejection of Tiversa's offer to provide LabMD with information security services, their subsequent lawsuit, and the FTC's investigation, the chronology of the investigation does not support such a conclusion. The FTC first contacted LabMD for information in January 2010, well before LabMD filed its lawsuit against Tiversa in October 2011.[27] Moreover, the claim that LabMD's conduct was reviewed by congressional committees does not appear to be based on evidence presented in the Petitions. Although Petitioners have attached as exhibits three instances of congressional testimony by Tiversa, none identifies LabMD by name or discusses the specifics of the File disclosure.

C. The resolution provides sufficient notice of the purpose and scope of the FTC's investigation.

Under the FTC Act, a CID is proper when it "state[s] the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation."[28] It is well-established that the resolution authorizing the process provides the requisite statement of the purpose and scope of the investigation,[29]

---

[25] LabMD Pet., Ex. A.

[26] LabMD Pet., at 9 & Ex. F.

[27] We note further that this suit came more than three years after the solicitations Petitioners complain of in their Petitions. LabMD Pet., Ex. F, at 1, 17-23.

[28] 15 U.S.C. § 57b-1(c)(2).

[29] *Invention Submission.*, 965 F.2d at 1088; *accord Texaco*, 555 F.2d at 874; *FTC v. Carter*, 636 F.2d 781, 789 (D.C. Cir. 1980); *FTC v. Anderson*, 631 F.2d 741, 746 (D.C. Cir. 1979).

and also that the resolution may define the investigation generally, need not state the purpose with specificity, and need not tie it to any particular theory of violation.[30]

Despite this, Petitioners object that Resolution File No. P954807 did not provide sufficient notice of the purpose and scope of the investigation, and they further claim that this resolution is inadequate under the standard developed by the D.C. Circuit in *FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980).[31]

Petitioners' first argument reads the governing standard too narrowly. Resolution File No. P954807 authorizes the use of compulsory process:

> to determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.[32]

This general statement of the purpose and scope of the investigation is more than sufficient under the standard for such resolutions, and courts have enforced compulsory process issued under similarly broad resolutions.[33]

Petitioners' reliance on *Carter* is also misplaced. While *Carter* held that a bare reference to Section 5, without more, "would not serve very specific notice of purpose," the Court approved the resolution at issue in that case, noting that it also referred to specific statutory provisions of the Cigarette Labeling and Advertising Act, and further

---

[30] *Invention Submission*, 965 F.2d at 1090; *Texaco*, 555 F.2d at 874 & n.26; *FTC v. Nat'l Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (citing *EPA v. Alyeska Pipeline Serv. Co.*, 836 F.2d 443, 477 (9th Cir. 1988)).

[31] LabMD Pet., at 10-12.

[32] LabMD Pet., Ex. A.

[33] *See FTC v. Nat'l Claims Serv.*, 1999 WL 819640, at *2 (finding omnibus resolution referring to FTC Act and Fair Credit Reporting Act sufficient); *FTC v. O'Connell Assoc., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (enforcing CIDs issued pursuant to omnibus resolution). The Commission has repeatedly rejected similar arguments about such omnibus resolutions. *See, e.g.*, *Firefighters Charitable Found.*, No. 102-3023, at 4 (Sept. 23, 2010); *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010); *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008).

related it to the subject matter of the investigation.[34] With this additional information, the Court felt "comfortably apprised of the purposes of the investigation and the subpoenas issued in its pursuit . . . ."[35]

The resolution here, like the one in *Carter*, does not cite solely to Section 5, but also recites the subject matter of the investigation: "deceptive or unfair acts or practices related to consumer privacy and/or data security." Since the resolution here discloses the subject matter of the investigation in addition to invoking Section 5, the resolution provides notice sufficient under *Carter* of the purpose and scope of the investigation.

As a final note, the history of the investigation itself undermines Petitioners' argument that the present CIDs do not sufficiently advise them of the nature and scope of the investigation. Petitioners have been under investigation since January 2010 and have engaged in repeated discussions with staff. At no point have Petitioners indicated they did not understand the purpose or scope; in fact, Petitioners have already produced hundreds of pages of documents in response to staff requests. Moreover, the Petitions under consideration here present highly detailed and factual arguments going to the very merits of the investigation. The Commission has previously found that such interactions may be considered along with the resolution in evaluating the notice provided to Petitioners.[36]

D. Petitioners' challenge to the FTC's regulatory authority is premature and without basis.

Petitioners' final argument is that the FTC lacks jurisdiction to conduct the instant investigation.[37] Petitioners assert that LabMD is a health care company and that the

---

[34] *Carter*, 636 F.2d at 788.

[35] *Id.*

[36] *Assoc. First Capital Corp.*, 127 F.T.C. 910, 915 (1999) ("[T]he notice provided in the compulsory process resolutions, CIDs and other communications with Petitioner more than meets the Commission's obligation of providing notice of the conduct and the potential statutory violations under investigation.").

[37] Petitioners also claim that the resolution does not meet the requirements established by the FTC's Operating Manual. LabMD Pet., at 10. As discussed above, by disclosing the statutory basis and subject matter of the investigation, the resolution does provide notice as required by the Operating Manual. That said, the Operating Manual, by its own terms, is advisory. It is not a "basis for nullifying any action of the Commission or the staff."

information disclosed in the 1,718 File is protected health information ("PHI") under the Health Insurance Portability and Accountability Act ("HIPAA"). Accordingly, they contend, the adequacy of their security practices with respect to this information is subject to the exclusive jurisdiction of HHS.[38]

As an initial matter, it is well-established that challenges to the FTC's jurisdiction are not properly raised through challenges to investigatory process. As the D.C. Circuit stated: "Following *Endicott* [*Johnson Corp. v. Perkins*, 317 U.S. 501, 509 (1943)], courts of appeals have consistently deferred to agency determinations of their own investigative authority, and have generally refused to entertain challenges to agency authority in proceedings to enforce compulsory process."[39] The reasons for such a rule are obvious. If a party under investigation could raise substantive challenges in an enforcement proceeding, before the agency has obtained the information necessary for its case – essentially requiring the FTC to litigate an issue before it can learn about it – then the FTC's investigations would be foreclosed or substantially delayed.[40] Thus, Petitioners' basic challenge to the FTC's jurisdiction is premature and will not support quashing the instant CIDs.

In any event, the claim that HHS has exclusive jurisdiction to investigate privacy and data security issues involving PHI is without basis. Petitioners essentially invoke the doctrine of implied repeal to assert that HIPAA and its Privacy and Security Rules displace FTC jurisdiction. But implied repeal is "strongly disfavored," for two reasons.[41] First, courts have recognized that agencies may have overlapping or concurrent jurisdiction, and thus that the same issues may be addressed and the same parties

---

Operating Manual, § 1.1.1.1. *See also FTC v. Nat'l Bus. Consultants, Inc.* 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) ¶68,984, at *29 (E.D. La. March 19, 1990).

[38] LabMD Pet., at 12-13.

[39] *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) (citing *United States v. Sturm, Ruger & Co.*, 84 F.3d 1, 5 (1st Cir. 1996)); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 468-73 (2d Cir. 1996); *EEOC v. Peat, Marwick, Mitchell & Co.*, 775 F.2d 928, 930 (8th Cir. 1985); *Donovan v. Shaw*, 668 F.2d 985, 989 (8th Cir. 1982); *FTC v. Ernstthal*, 607 F.2d 488, 490 (D.C. Cir. 1979); *accord Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 213-14 (1946).

[40] *Texaco*, 555 F.2d at 879.

[41] *Galliano v. United States Postal Serv.*, 836 F.2d 1362, 1369 (D.C. Cir. 1988).

proceeded against simultaneously by more than one agency.[42] Second, courts rarely hold that one federal statute impliedly repeals another because "'when two statutes are capable of co-existence, it is the duty of the courts . . . to regard each as effective.'"[43] Thus, repeals by implication will only be found where the Congressional intent to effect such a repeal is "clear and manifest."[44]

Petitioners can point to no such "clear or manifest" evidence that Congress intended HIPAA or its rules to displace the FTC Act. The authority Petitioners cite for the proposition that HHS has exclusive jurisdiction does not address such repeal.[45] To the contrary, there is ample evidence against such implied repeal. For one, the same authority cited by Petitioners – the preamble to the Privacy Rule – expressly provides that entities covered by that Rule are "also subject to other federal statutes and regulations."[46] Also, this preamble includes an "Implied Repeal Analysis," which is silent as to any implied repeal of the FTC Act.[47] Recent legislation shows that, if anything, Congress intended the FTC and HHS to work collaboratively to address potential privacy and data security risks related to health information. The American Recovery and Reinvestment Act of 2009, for instance, required HHS and the FTC to develop harmonized rules for data breach notifications by HIPAA-covered and non-HIPAA-covered entities, respectively. *See* 74

---

[42] *FTC v. Cement Inst.*, 333 U.S. 683, 694 (1948); *see also Texaco*, 555 F.2d at 881 ("[T]his is an era of overlapping agency jurisdiction under different statutory mandates."); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1986). Because agencies have overlapping jurisdiction, they often work together. For instance, the FTC and HHS collaborated on the investigation of CVS Caremark Corporation. *See CVS Caremark Corp.*, No. 072-3119, at 7 (Aug. 6, 2008).

[43] *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 155 (1976) (quoting *Morton v. Mancari*, 417 U.S. 535, 551 (1974)).

[44] *Id.* at 154.

[45] LabMD Pet., at 12 (citing 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000)). This Federal Register notice is the Notice of Public Rulemaking for the Privacy and Security Rules under HIPAA. The excerpt cited by Petitioners does not address the scope of HHS' enforcement jurisdiction, but rather discusses the delegation of enforcement authority from the Secretary of HHS to HHS' Office for Civil Rights. 65 Fed. Reg. 82,472 (Dec. 28, 2000).

[46] 65 Fed. Reg. 82,462, 82,481 (Dec. 28, 2000).

[47] *Id.* at 82,481-487.

Fed. Reg. 42,962, 42,962-63 (Aug. 25, 2009). Thus, HIPAA and its Rules do not serve to repeal FTC jurisdiction, which is overlapping and concurrent to HHS'.

This is particularly appropriate where, as here, the consumer information at issue included more than just health information. The consumer information exposed in the 1,718 File also included names, Social Security numbers, and dates of birth. While this information can be considered PHI under HIPAA when combined with health information, the information clearly exposes consumers to the risk of identity theft and is exactly the kind of sensitive personal information that the Commission is charged with protecting under Section 5 of the FTC Act and other statutes. Petitioners have provided no proper basis to challenge the investigation as an exercise of the Commission's jurisdiction under these authorities.

III. CONCLUSION AND ORDER

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

IT IS FURTHER ORDERED THAT Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

IT IS FURTHER ORDERED THAT Commission staff may reschedule the investigational hearings of LabMD and Michael J. Daugherty at such dates and times as they may direct in writing, in accordance with the powers delegated to them by 16 C.F.R. § 2.9(b)(6); and

IT IS FURTHER ORDERED THAT all other responses to the specifications in the Civil Investigative Demands to LabMD, Inc. and Michael J. Daugherty must now be produced on or before May 11, 2012.

By direction of the Commission.

Donald S. Clark
Secretary

EXHIBIT 7

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC

Office of the Secretary

June 21, 2012

BY E-MAIL AND COURIER DELIVERY

Stephen F. Fusco, Esq.
LabMD
2030 Powers Ferry Drive
Building 500, Suite 520
Atlanta, GA 30339
sfusco@labmd.org

RE: *Request for Full Commission Review of Denial of Petitions to Limit or Quash the Civil Investigative Demand by LabMD, Inc. and Michael J. Daugherty (FTC File No. 1023099)*

Dear Mr. Fusco:

This letter advises you of the Commission's disposition of LabMD, Inc.'s and Michael J. Daugherty's request dated April 25, 2012, that the full Commission review the denial of their petition to limit or quash civil investigative demands.

The Commission issued the CIDs to LabMD and Mr. Daugherty on December 21, 2011. LabMD and Mr. Daugherty filed petitions to limit or quash the CIDs, which were received by the Commission on January 10, 2012. On April 20, 2012, Commissioner Brill directed the issuance of a letter denying both petitions and directing both petitioners to comply by May 11, 2012. That deadline was extended to June 8, 2012 due to emergency circumstances that you brought to the Commission's attention.[21]

The Commission affirms the ruling denying the petitions to limit or quash the civil investigative demands. The Commission has independently reviewed LabMD and Mr. Daugherty's petitions to limit or quash the CIDs, and their requests for full Commission review. The Commission has also reviewed the letter ruling issued by the Commission at the direction of Commissioner Brill, and hereby affirms that ruling, finding its conclusions to be valid and correct.

[21] On April 30, 2012, you contacted the Commission's Office of the Secretary to request additional time to comply with the CID due to emergency circumstances. By letter dated May 7, 2012, the Commission modified the date to June 8, 2012.

Commissioner Rosch generally agrees with the Commission's decision to enforce the CIDs, but dissents from this ruling to the extent it permits staff to rely on a LabMD document found on a peer-to-peer file sharing network, out of concern about petitioners' allegations that a third party located this document through wrongdoing and for financially-motivated reasons. In this ruling, we make no findings of fact regarding that third party's conduct or the admissibility of this document, nor do we need to do so. In upholding the CIDs, the Commission allows staff to continue to use pertinent information—including information from or concerning any LabMD documents made available to users of peer-to-peer file-sharing networks and accessed by any third party—to conduct its data security investigation. Indeed, in our data security investigations, the Commission often uses information obtained by third parties concerning security vulnerabilities of entities that maintain substantial amounts of personal information. Although we understand petitioners have alleged that the third party in question has a financial incentive to use its patented monitoring tool to find information that has been improperly disclosed on peer-to-peer file sharing networks, that does not overcome the Commission's compelling public interest in seeking to protect consumers' sensitive health data by pursuing this investigation through all lawful means, including the use of this document.

The April 25, 2012 request for full Commission review also requested a hearing on the denial of the petitions. The FTC Rule governing petitions to quash or limit, 16 C.F.R. § 2.7, does not provide for such a hearing, however, and accordingly, this request will be denied.

For the forgoing reasons,

IT IS ORDERED THAT the April 20, 2012 letter ruling is **AFFIRMED**;

IT IS FURTHER ORDERED THAT LabMD's and Mr. Daugherty's request for a hearing is **DENIED**;

IT IS FURTHER ORDERED THAT Commission staff may reschedule the investigational hearings of LabMD and Michael J. Daugherty at such dates and times as they may direct in writing, in accordance with the powers delegated to them by 16 C.F.R. § 2.9(b)(6)(2012); and

IT IS FURTHER ORDERED THAT all other responses to the specifications in the Civil Investigative Demands to LabMD, Inc. and Michael J. Daugherty must be produced on or before June 8, 2012.

By direction of the Commission, Commissioner Rosch dissenting, and Commissioner Ohlhausen not participating.

Donald S. Clark
Secretary

EXHIBIT 8

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEDERAL TRADE COMMISSION, **Petitioner,** **v.** **LABMD, INC., and MICHAEL J. DAUGHERTY,** **Respondents.**	**1:12-cv-3005-WSD**

OPINION AND ORDER

This matter is before the Court on the Federal Trade Commission's ("FTC," "Commission," or "Petitioner") "Petition of the Federal Trade Commission for an Order to Enforce Civil Investigative Demands" ("Petition") [1].

I. BACKGROUND

On January 3, 2008, the FTC issued a "Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security" (the "2008 Resolution"). (Ex. 2 to Pet. at 3).

The 2008 Resolution authorizes the use of the FTC's compulsory process powers, for a period of five (5) years from its issuance, "[t]o determine whether

unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act [("FTCA")], 15 U.S.C. § 45, as amended." (Id.).

In 2009, the FTC learned that personally-identifiable and sensitive health information belonging to consumers was publically available on peer-to-peer ("P2P") file sharing networks. (Pet. ¶ 6). The FTC undertook a further "inquiry to determine whether disclosures of consumers' sensitive personal information were attributable to failures to employ reasonable data security measures in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), or whether they violated any other statutes or regulations enforced by the Commission." (Id. ¶ 7). The FTC issued Civil Investigative Demands ("CIDs"), pursuant to the 2008 Resolution, to various entities to "obtain copies of electronic files that were located on P2P networks and that contain sensitive information." (Id. ¶ 8). In response to its CIDs, the FTC obtained a spreadsheet (the "1,718 File") that contained information about 9,000 LabMD, Inc. ("LabMD") customers, to include names, Social Security numbers, dates of birth, and personal health insurance information. (Id.).

In 2010, after reviewing the 1,718 File and consulting with law enforcement agencies, the FTC issued a request for information to LabMD in the form of a

"voluntary access request." (Id. ¶ 9). The voluntary access request sought information that would help the FTC determine if LabMD "had violated laws enforced by the Commission by failing to use reasonable and appropriate security measures to safeguard sensitive information." (Id.). LabMD responded to the voluntary access request, but the FTC was dissatisfied with the scope of materials and information that were provided. (Id. ¶ 10).

On December 21, 2011, the FTC issued CIDs to LabMD and its owner and president, Michael J. Daugherty ("Daugherty," collectively "Respondents"), to obtain information it believed it needed to complete its investigation into Respondents' data security policies and practices. (Id. ¶¶ 10-11). The CIDs demanded that: (1) "Daugherty and one or more representatives of LabMD . . . appear and testify at investigational hearings with FTC staff;" (2) "LabMD and Mr. Daugherty . . . respond to a limited set of interrogatories;" (3) "LabMD . . . respond to a single request for documents related to its data security practices that had not already been produced to the Commission in response to the voluntary access requests;" (4) "LabMD and Mr. Daugherty . . . provide interrogatory responses and documents by January 13, 2012, and schedule the investigational hearings for January 23, 2012;" and, (5) LabMD and Daugherty "certify that they had complied with the CID requirements." (Pet. ¶ 11; Ex. 2 to Pet.; Ex. 3 to Pet.).

Between January and June 2012, Respondents sought to limit or quash the CIDs through the administrative appeal process established by the Code of Federal Regulations and Federal Trade Commission Rules. (Pet. ¶¶ 12-15).

On June 21, 2012, Respondents' administrative remedies in challenging the CIDs were exhausted when the FTC denied Respondents' administrative petition to limit or quash the CIDs. (Id. ¶¶ 14-15).

On June 25, 2012, the FTC staff contacted Respondents to discuss their compliance with the CIDs. (Id. ¶ 16). On June 29, 2012, Respondents replied and restated their objections to the CIDs. (Id.).

On August 29, 2012, after Respondents failed to comply with the CIDs, the FTC filed its Petition in this Court seeking an order requiring Respondents to comply with CIDs issued to them on December 21, 2011, pursuant to the FTC's authority under 15 U.S.C. §§ 46, 57b-1 of the FTCA and the 2008 Resolution. (Id. at 1-4). In its Petition, the FTC alleges that the "[R]espondents' failure to comply with the CIDs greatly impedes the Commission's ongoing investigation [into breaches of consumers' sensitive personal information], and prevents the Commission from completing its investigation in a timely manner." (Id. at 9).

On September 5, 2012, the Court ordered: (i) Petitioner to serve Respondents with its Petition; (ii) required Respondents to show cause at a hearing

on September 19, 2012, regarding why the CIDs should not be enforced; and, (iii) directed Respondents to file a pleading "stating their legal and factual support for failing to comply with the FTC's CIDs and explaining why an order should not issue from this Court requiring compliance with the CIDs." (Order of Sept. 5, 2012, [3] at 2-3).

On September 19, 2012, after receiving briefing by the parties, the Court held the show cause hearing and heard argument from the parties. Following the hearing, the Court ordered the FTC to file a supplemental pleading addressing the following questions:

> 1. In a proceeding to enforce an investigative subpoena, what is the FTC required to show to meet the requirement that the subpoena is issued in an inquiry that is within the authority of the agency?
>
> 2. Does the 'plausible' argument standard set out in E.E.O.C. v. Kloster Cruise, Ltd., 939 F.2d 920, 922 (11th Cir. 1991) apply to FTC enforcement actions?
>
> 3. How does the FTC meet the "within the authority of the agency" standard in this case?
>
> 4. What impact, if any, does the Federal Trade Commission's June 21, 2012, decision have on this Court's consideration of the "within the authority of the agency" showing required in this case?
>
> 5. Did LabMD have a means of challenging the Commission's June 21, 2012 decision that the information security investigative inquiry here is within its authority under Section

> 45 and, if so, does that impact the ability of LabMD to raise the issue in this enforcement proceeding?

On September 24, 2012, the FTC filed its supplemental pleading [20]. On September 28, and October 2, 2012, Respondents and the FTC filed a response and reply, respectively [21, 22].

II. DISCUSSION

A. Standard for enforcement of an administrative subpoena

"It is well-settled that the role of a district court in a proceeding to enforce an administrative subpoena is sharply limited; inquiry is appropriate only into whether the evidence sought is material and relevant to a lawful purpose of the agency." Kloster Cruise, 939 F.2d 920, 922 (11th Cir. 1991); see also United States v. Feaster, 376 F.2d 147, 149 (5th Cir. 1967) ("In subpoena cases the Supreme Court has rejected claims that the court must satisfy itself that probable cause exists for the agency's contention that the subject of the subpoena is covered by the statute; the only judicial inquiry to be made in enforcing an agency subpoena is whether the evidence sought is 'plainly incompetent or irrelevant to any lawful purpose' of the agency."); Tobin v. Banks & Rumbaugh, 201 F.2d 223, 224 (5th Cir. 1953) ("[I]n the absence of a clear showing of unreasonableness or gross abuse of the administrative investigative function, the Courts will not interfere with an investigation 'merely in order to render an anticipatory judgment

on the merits.'"). In other words, "a subpoena enforcement proceeding is not the proper forum in which to litigate the question of coverage under a particular statute" and "[t]he agency need not make a conclusive showing of jurisdiction to justify enforcement of the subpoena." Kloster Cruise, 939 F.2d at 922 (citations omitted).[1]

Two inquiries related to the validity of a subpoena issued by a governmental agency are appropriate to be addressed in a subpoena enforcement proceeding: (1) Whether the agency makes a "plausible argument in support of its assertion of jurisdiction"; and (2) Whether the information sought by the subpoena is "plainly incompetent or irrelevant to any lawful purpose [of the FTC]." Id.; see also Ken Roberts Co., 276 F.3d at 587 ("enforcement of an agency's investigatory subpoena will be denied only when there is 'a patent lack of jurisdiction' in an agency to regulate or to investigate"); United States v. Sturm, Ruger & Co., 84 F.3d 1, 5-6 (1st Cir. 1996) (citing Kloster Cruise, 939 F.2d at 923) ("As long as the agency's assertion of authority is not obviously apocryphal, a procedurally sound subpoena

[1] "[C]ourts of appeals have consistently deferred to agency determinations of their own investigative authority, and have generally refused to entertain challenges to agency authority in proceedings to enforce compulsory process." FTC v. Ken Roberts Co., 276 F.3d 583, 586 (D.C. Cir. 2001) (citing cases). Consistent with other courts of appeal, the Eleventh Circuit has held that "[t]he initial determination of the coverage question is left to the administrative agency seeking enforcement of the subpoena." Kloster Cruise, 939 F.2d at 922.

must be enforced."); EEOC v. Tire Kingdom, Inc., 80 F.3d 449, 450-51 (11th Cir. 1996); United States v. Fla. Azalea Specialists, 19 F.3d 620, 622-23 (11th Cir. 1994); Casey v. FTC, 578 F.2d 793, 799 (9th Cir. 1978) ("The district court's role in a subpoena enforcement proceeding is strictly limited where the subpoena is attacked for lack of agency jurisdiction. The subpoena must be enforced if the information sought is 'not plainly incompetent or irrelevant to any lawful purpose' of the FTC."). Thus, the Court's inquiry at the enforcement stage is limited. The Court addresses these questions in assessing whether to grant the FTC's request to enforce the CIDs.

1. Plausible argument that the FTC has jurisdiction to regulate data security and consumer privacy under Section 5

Section 5 does not specifically identify data security and consumer privacy as areas in which the FTC has jurisdiction to regulate. 15 U.S.C. § 45(n). Rather, courts interpret Section 5 as a statute that broadly confers authority on the FTC to investigate and regulate unfair practices that cause or are "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." See 15 U.S.C. § 45(n); Genuine Parts Co. v. FTC, 445 F.2d 1382, 1391 (5th Cir. 1971) (FTC accorded "extreme breadth" in conducting investigations). The authority of the FTC under Section 5 to regulate unfair

practices is broadly construed by courts because it is impossible to define what constitutes unfair practices in a constantly changing and evolving economic climate. See FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 240, 244 (1972); Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1368 (11th Cir. 1988).

In determining the limits of the FTC's authority to investigate and address unfair practices regarding failures to employ reasonable data security measures, this Court is mindful that "[c]ourts have long held that consumers are injured for purposes of [Section 5 of the FTCA] not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable consequence of those actions." FTC v. Neovi, 604 F.3d 1150, 1156-57 (9th Cir. 2010) (citing FTC v. Winsted Hosiery Co., 258 U.S. 483, 494 (1922) (holding that "[t]he honest manufacturer's business may suffer, not merely through a competitor's deceiving his direct customer, the retailer, but also through the competitor's putting into the hands of the retailer an unlawful instrument . . ."); FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 314 (1934) (holding candy retailer liable for unfair practices although manufacturer was responsible for the element of chance that made the practices unfair); Regina Corp. v. FTC, 322 F.2d 765, 768 (3d Cir. 1963) (explaining that "[w]ith respect to those instances where petitioner did not

contribute to the [misleading act], it is settled that [o]ne who places in the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act") (quotation marks and citations omitted)).

"The statutory scheme at issue here 'necessarily gives the Commission an influential role in interpreting section 5 and in applying it to facts of particular cases arising out of unprecedented situations.'" Orkin Exterminating Co., 849 F.2d at 1367-68 (quoting FTC v. Colgate-Palmolive, Co., 380 U.S. 374, 385 (1965)). "Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission in 1914 to define unfair practices on a flexible, incremental basis." Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 967 (D.C. Cir. 1985); see also Orkin, 849 F.2d at 1368 (FTC's Section 5 authority is a "broad mandate conferred upon the Commission by Congress."); FTC v. Windward Mktg., Inc., No. Civ.A. 1:96-CV-615F, 1997 WL 33642380, at *11 (N.D. Ga. Sept. 30, 1997) ("Congress has not enacted any more particularized definition of unfairness to limit the Commission's discretion.").

Although it is given broad discretion to determine what constitutes an unfair practice, the FTC's authority to investigate unfair practices using its subpoena enforcement power is not unlimited. Courts measure the validity of an FTC

subpoena against the purposes stated in the FTC resolution authorizing an investigation into specific practices. See 15 U.S.C. § 57b-1(i);[2] FTC v. Invention Submission Corp., 965 F.2d 1086, 1092 (D.C. Cir. 1992).

Respondents argue that the CIDs here are invalid because the 2008 Resolution was issued before the FTC learned of the existence of the 1,718 File and, in any event, is too vague to support the issuance of an administrative subpoena seeking information from LabMD. (See Ex. 2 to Pet. at 3). Respondents also assert that the FTC's claim of authority to regulate data security is not based on any threat of substantial injury to consumers, but only gross generalities.

As to Respondents' argument that the 2008 Resolution is vague and invalid, the Court disagrees. There is no dispute that the 2008 Resolution was validly issued by the Commission and the Court finds it sufficiently specifies the nature, scope, and subject matter upon which subpoenas and demands for information may

[2] The FTCA provides:

> Notwithstanding any other provision of law, the Commission shall have no authority to issue a subpoena or make a demand for information, under authority of this subchapter or any other provision of law, unless such subpoena or demand for information is signed by a Commissioner acting pursuant to a Commission resolution. The Commission shall not delegate the power conferred by this section to sign subpoenas or demands for information to any other person.

15 U.S.C. § 57b-1(i).

be made.[3] Respondent has not cited any legal authority, and the Court has found none, that invalidates an administrative agency's subpoena because it is issued based on authority in a resolution that pre-dates the identification of a specific issue of concern within the scope of that resolution. See Invention Submission Corp., 965 F.2d at 1092 (quoting FTC v. Carter, 636 F.2d 781, 789 (D.C. Cir. 1980)) ("clear that 'the validity of Commission subpoenas is to be measured against the purposes stated in the resolution, and not by reference to extraneous evidence'").

The Court also disagrees with Respondents' contention that there is no basis for the FTC to investigate and regulate data security and consumer privacy because there is no threat of substantial injury to consumers. The FTC presents sufficient information in its pleadings to support its claim that there is a significant and

---

[3] The 2008 Resolution states, under a heading entitled "Nature and Scope of Investigation," that it was adopted to permit the FTC:

> To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act [("FTCA")], 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

(Ex. 2 to Pet. at 3).

widespread impact and threat to consumers, including identity theft, that results from breaches of data security and consumer privacy. (See Pet'r's Supplemental Mem. in Supp. of Pet. to Enforce Civil Investigative Demand [20] at 9-10; Pet'r's Reply Mem. in Supp. of Pet. [15] at 8, 12-13). The Court finds that the FTC presents a plausible argument for the exercise of its jurisdiction to investigate and enforce in the realm of data security and consumer privacy—which it has done so in at least forty-four instances since 2000—in light of the threat of substantial consumer harm that occurs when consumers are victims of identity theft—a routine occurrence in the United States. See Pl.'s Rep. in Opp'n to Wyndham Hotels and Resorts' Mot. to Dismiss at 5, FTC v. Wyndham Worldwide Corp., Case No. 2:12-cv-01365-PHX-PGR (D. Ariz. filed June 26, 2012); Legal Resources, BCP Business Center, http://business.ftc.gov/legal-resources/29/35 (last visited Nov. 16, 2012) (citing enforcement actions); (Pet'r's Supplemental Mem. in Supp. of Pet. to Enforce Civil Investigative Demand at 9-10; Pet'r's Reply Mem. in Supp. of Pet. at 8, 12-13).

The Court also finds support for the conclusion that the FTC's argument is plausible regarding its jurisdiction because federal courts have recognized the FTC's authority under Section 5 to investigate and use its authority to address unfair practices regarding related data security and consumer privacy issues. See

FTC v. Pricewert, LLC, No. C-09-2407 RMW, 2010 WL 329913, at *2-*3 (N.D. Cal. 2010) (Section 5 used to address "distribution of illegal, malicious and harmful electronic content"); FTC v. CyberSpy Software, LLC, No. 6:08-cv-1872-Orl-31GJK, 2009 WL 455417, at *1 (M.D. Fla. Feb. 23, 2009) (Section 5 used to address marketing of a software program that could be used illegitimately to commit identity theft); FTC v. Accusearch, Inc., No. 06-CV-105-D, 2007 WL 4356786, at *1, *7-*8 (D. Wyo. Sept. 28, 2007), aff'd 570 F.3d 1187 (10th Cir. 2009) (Section 5 used to address the unauthorized disclosure of confidential customer phone records); FTC v. Seismic Entm't Prods., Inc., No. Civ. 04-377-JD, 2004 WL 2403124, at *2-*4 (D.N.H. 2004) (Section 5 used to address internet advertising methods that cause unauthorized changes to computers and that affect data security).

Although the Court finds there is significant merit to Respondents' argument that Section 5 does not justify an investigation into data security practices and consumer privacy issues, it is a plausible argument to assert that poor data security and consumer privacy practices facilitate and contribute to predictable and substantial harm to consumers in violation of Section 5 because it is disturbingly commonplace for people to wrongfully exploit poor data security and consumer privacy practices to wrongfully acquire and exploit personal consumer

information. Because the FTC's assertion of jurisdiction to issue its CIDs is premised on a plausible argument, the Court finds that Respondents' argument that the CIDs should not be enforced for a lack of jurisdiction is not a sufficient reason to deny the FTC's request for enforcement. See Kloster Cruise, 939 F.2d at 922.

2. Whether the information sought by the subpoena is unreasonable or "plainly incompetent or irrelevant to any lawful purpose [of the FTC]"

With regard to administrative subpoenas issued by the FTC, the Supreme Court has stated:

> Even if one were to regard [a] request for information . . . as caused by nothing more than official curiosity, nevertheless lawenforcing [sic] agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest.
>
> Of course a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power. Federal Trade Comm. v. American Tobacco Co., supra. But it is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant. 'The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.' Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 208, 66 S.Ct. 494, 505, 90 L.Ed. 614, 166 A.L.R. 531.

See United States v. Morton Salt Co., 338 U.S. 632, 652-53 (1950).

Thus, "[t]he chief limitation on an investigation by an administrative agency is that it must meet the test of reasonableness." Genuine Parts Co., 445 F.2d at 1391 (citing Oklahoma Press Publishing Co. v. Walling, 327 U.S. at 208). The information sought by the FTC also must "not [be] plainly incompetent or irrelevant to any lawful purpose." See Kloster Cruise, 939 F.2d at 922 (quotations omitted). In seeking information in an investigation, the FTC is accorded "extreme breadth" by courts when evaluating its demands for testimony and documents. See Genuine Parts Co., 445 F.2d at 1391.

Furthermore, the burden of showing that an administrative subpoena is unreasonable is a heavy one because

> [s]ome burden on subpoenaed parties is to be expected and is necessary in furtherance of the agency's legitimate inquiry and the public interest. The burden of showing that the request is unreasonable is on the subpoenaed party. Further, that burden is not easily met where . . . the agency inquiry is pursuant to a lawful purpose and the requested documents are relevant to that purpose. Broadness alone is not sufficient justification to refuse enforcement of a subpoena. Thus courts have refused to modify investigative subpoenas unless compliance threatens to unduly disrupt or seriously hinder normal operations of a business.

See FTC v. Texaco, Inc., 555 F.2d 862, 882 (D.C. Cir. 1977).

The FTC here demands documents and testimony related to the public disclosure on P2P networks of Respondents' 1,718 File containing the names and

sensitive information of 9,000 consumers and LabMD's data security practices. The Court has reviewed the FTC's CIDs in this action and finds they are specific in scope, reasonably relevant to its investigation into LabMD's data security practices, and, even though LabMD has already produced a significant amount of material, are not duplicative or unreasonable. (See Ex. 2 to Pet. at 11-12; Ex. 3 to Pet. at 8). The Court finds that the demands in the CIDs—beyond being based on a plausible argument regarding the FTC's statutory authority and jurisdiction—are not too indefinite and the information sought is reasonably relevant to its investigation into Respondents' data security and customer privacy practices.

In light of the "sharply limited" "role of a district court in a proceeding to enforce an administrative subpoena," the Court finds the CIDs are required to be enforced because there is a plausible argument for the exercise of jurisdiction by the FTC and "the evidence sought is material and relevant to a lawful purpose of the agency." See Kloster Cruise, 939 F.2d at 922.

III. CONCLUSION

For the foregoing reasons,

IT IS HEREBY ORDERED that Petitioner's Petition [1] is **GRANTED**.

IT IS FURTHER ORDERED that, no later than December 15, 2012, Respondents shall comply with Petitioner's Civil Investigative Demands.

SO ORDERED this 26th day of November, 2012.

WILLIAM S. DUFFEY, JR.
UNITED STATES DISTRICT JUDGE

EXHIBIT 9

In the Matter of:

LabMD, Inc.

September 25, 2013
Initial Pretrial Conference

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

I N D E X

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of:)
LABMD, INC.,) Docket No. 9357
a corporation.)
----------)

INITIAL PRETRIAL CONFERENCE
SEPTEMBER 25, 2013
2:00 P.M.
PUBLIC SESSION

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Administrative Law Judge

Reported by: Susanne Bergling, RMR-CRR-CLR

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
ALAIN SHEER, ESQ.
LAURA RIPOSO VANDRUFF, ESQ.
MEGAN COX, ESQ.
MARGARET LASSACK, ESQ.
RYAN MEHM, ESQ.
Federal Trade Commission
Division of Privacy and Identity Protection
601 New Jersey Avenue, N.W.
Washington, D.C. 20001
(202) 326-2999
asheer@ftc.gov

ON BEHALF OF RESPONDENT:
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W., Suite 610
Washington, D.C. 20004
(202) 372-9100
reed.rubinstein@dinsmore.com

ALSO PRESENT:
Victoria Arthaud and Hillary Sloane Gebler

P R O C E E D I N G S
- - - - -

JUDGE CHAPPELL: Okay. Call to order Docket 9357, In Re: LabMD. Is there a space after the B or is that one word, "LabMD"?

MR. RUBINSTEIN: It is one word, Your Honor.

JUDGE CHAPPELL: Okay. Thank you.

I will start with appearances of the parties, and I will start with the Government. Go ahead.

MR. SHEER: Good afternoon, Your Honor. I'm Alain Sheer representing the Commission.

MS. VANDRUFF: Good afternoon, Your Honor. Laura VanDruff, Complaint Counsel.

JUDGE CHAPPELL: Okay.

And for Respondent?

MR. RUBINSTEIN: Your Honor, Reed Rubinstein representing Respondent. If I could, I would like to take this opportunity to thank you and to thank government counsel for their accommodation of my schedule. It is very much appreciated.

JUDGE CHAPPELL: You're welcome. I would expect that request to come a little sooner next time.

MR. RUBINSTEIN: Yes, Your Honor.

JUDGE CHAPPELL: And also, just so everyone knows, we do follow motions practice, and I will need a

5

motion from here out to deal with something.
MR. RUBINSTEIN: Thank you.
JUDGE CHAPPELL: I notice that we have got more than two people listed at on least one side. Our office will email courtesy copies of orders to the parties. That's courtesy copies. Official service is made by the Office of the Secretary. I will need each party to designate no more than two individuals to receive communications from my office. You can send an email to my assistant, Dana Gross, or just to the OALJ Web site, and give us the two people you want to receive courtesy copies from my office.
I think for the first time in history we have no modifications to the draft scheduling order. So, thanks to both of you. I will issue that order by tomorrow or Friday. I think I'm obligated to get it out by Friday under the latest rules.
There's a limit to the amount of time we're in trial. I don't anticipate us getting anywhere near the limit. Does -- while we're here, how many witnesses do you anticipate for the Government? I just need a ballpark. I'm not holding you to anything.
MR. SHEER: Judge, I'm watching the monitor. We expect that we will be putting on seven or eight witnesses.

6

JUDGE CHAPPELL: Okay.
And for the Respondent?
MR. RUBINSTEIN: Approximately the same number.
JUDGE CHAPPELL: I'm thinking this is going to move along fairly quickly. Any experts?
MR. SHEER: Yes, Your Honor. We are going to be using experts on technical issues and also on consumer injury.
JUDGE CHAPPELL: You need to stand up when you speak. She needs to hear you. Use that microphone.
MR. SHEER: Sorry. We are expecting to use technical experts and also experts for consumer injury.
JUDGE CHAPPELL: Okay.
MR. RUBINSTEIN: Your Honor, we also will be using --
JUDGE CHAPPELL: If you -- if you use that microphone -- just stand and use one of the microphones, either one. You have got one over in the middle.
MR. RUBINSTEIN: This one works, if it works for you.
We will also be presenting expert testimony, rebuttal testimony to the Government's witnesses. We anticipate there will be two, perhaps three, that will go to harm and will also go to the technical issues associated with the file theft.

7

JUDGE CHAPPELL: Okay. Under the current rules, the hearing is limited to no more than 210 hours. So, I need the parties to develop a system or mechanism to keep track of that, although I don't see us stretching those boundaries in this hearing.
Regarding -- one thing regarding the scheduling order, let me talk about dispositive motions. I didn't put a deadline on the scheduling order for summary judgment motions. There is a rule that covers that, if you intend to file a summary judgment, and if you don't know, I'll tell you.
Summary judgments will be ruled on by the Commission, the same body that voted to issue the complaint in this case. With respect to motion to dismiss or other substantive motion, the rules provide that if they are filed before the start of the evidentiary hearing, they will be ruled on by that same Commission; however, motions to dismiss or substantive motions filed after the start of the evidentiary hearing will be decided by me, not the Commission.
Have there been any settlement discussions?
MR. SHEER: There were very, very preliminary settlement discussions; that is to say that Respondent LabMD had indicated they had interest in settlement at one point long ago, but the parties did not pursue it,

8

and at this moment, there are no settlement discussions on the table or ongoing.
JUDGE CHAPPELL: Any comment on that?
MR. RUBINSTEIN: That is correct, Your Honor.
JUDGE CHAPPELL: At this time, I allow each side to present an overview of their case, and I limit it to 15 minutes, and I'll let the Government go first; however, I'll let you know, if I ask questions, I will add to your time, or take up any of your 15 minutes.
Go ahead.
MR. SHEER: Thank you, Your Honor. LabMD is a medical laboratory that tests blood and tissue samples that doctors take from consumers. In doing so, it's collected very sensitive information about hundreds of thousands of consumers, including names, Social Security numbers, checking account information, and medical test results.
JUDGE CHAPPELL: Hundreds of thousands. So, you're saying they do a national business?
MR. SHEER: They do a national business.
LabMD exposes this treasure trove of information to people who never should have had access to it by failing to take reasonable and appropriate security measures. Identity thieves use consumers' personal information to impersonate them in a variety of ways,

9

1 depending on the information. For example, financial
2 information has been misused to open new -- to conduct
3 credit card fraud and to go into bank accounts; and
4 medical information has been misused to steal insurance
5 benefits. In each of the last ten years, identity theft
6 has been the number one complaint that the FTC has
7 received. There were 369,000 complaints in 2012.
8 The personal information that LabMD maintains is
9 information that identity thieves want. This was action
10 was brought under Section 5 of the FTC Act. Section 5
11 provides the Commission with broad authority to address
12 new areas and practices as they develop.
13 JUDGE CHAPPELL: Have you -- in that regard, has
14 the Commission issued guidelines for companies to
15 utilize to protect this information or is there
16 something out there for a company to look to?
17 MR. SHEER: There is nothing out there for a
18 company to look to. The Commission has entered into
19 almost 57 negotiations and consent agreements that set
20 out a series of vulnerabilities that firms should be
21 aware of, as well as the method by which the Commission
22 assesses reasonableness.
23 In addition, there have been public statements
24 made by the Commission, as well as educational materials
25 that have been provided. And in addition, the industry,

10

1 the IT industry itself, has issued a tremendous number
2 of guidance pieces and other pieces that basically set
3 out the same methodology that the Commission is
4 following in deciding reasonableness, with one
5 exception, and the exception is that the Commission's
6 process as to the calculation of the potential consumer
7 harm from unauthorized disclosure of information.
8 JUDGE CHAPPELL: Is there a rulemaking going on
9 at this time or are there rules that have been issued in
10 this area?
11 MR. SHEER: There are no -- there is no
12 rulemaking, and no rules have been issued, other than
13 the rule issued with regard to the Gramm-Leach-Bliley
14 Act. There is a safeguards rule there which is issued
15 for financial institutions. The way that rule reads and
16 the way it works, it basically --
17 JUDGE CHAPPELL: The FTC has jurisdiction in
18 that area?
19 MR. SHEER: It has jurisdiction over certain
20 types of financial institutions, such as --
21 JUDGE CHAPPELL: Is that expressed in that Act?
22 MR. SHEER: It is.
23 JUDGE CHAPPELL: Okay.
24 MR. SHEER: As I was saying, Your Honor,
25 information security, which is an essential part of our

11

1 economy now given the increasing reliance on and use of
2 computer networks, is one of the new areas that the
3 Commission is able to look into. The complaint alleges
4 that the company, LabMD, engaged in an unfair act or
5 practice in violation of Section 5 by collecting and
6 storing large amounts of very sensitive consumer
7 information and failing to use reasonable and
8 appropriate security measures to prevent the information
9 from being disclosed without authorization.
10 As set out in 15 USC 45(n), an act or practice
11 is unfair when it causes or is likely to cause
12 substantial consumer injury that is not -- and the
13 injury is not reasonably avoidable by consumers and not
14 offset by countervailing benefits to consumers or
15 competition. The complaint alleges that LabMD
16 systematically failed to practice what IT professionals
17 generally call -- quote unquote -- defense in depth.
18 Defense in depth is a general approach for
19 identifying the kinds of security measures that will be
20 reasonable under particular circumstances. It sets out
21 guiding principles that IT professionals and industry
22 have known and used for years. There are lots of
23 sources for the principles, such as materials published
24 by the National Institute of Standards and Technology,
25 continuing education for IT professionals, practical IT

12

1 experience, and lessons learned from publicized
2 breaches.
3 Some of these guiding principles are, first, do
4 not put all your eggs in one basket, because a single
5 security measure may fail or be vulnerable. For
6 example, if the only security measure for a company's
7 network were a firewall and the firewall were not set up
8 correctly, an outsider could exploit the mistake and
9 gain entry to the network, because there are no other
10 security measures in place. The outsider would have
11 free reign within the network and could find -- easily
12 find and export sensitive information.
13 Second, limit a computer user's control over the
14 computers and data to the lowest level the user needs to
15 perform their job. For example, users do not need to be
16 able to change security settings on their computers or
17 install programs on their computers without getting
18 prior approval.
19 Third, also use nontechnical measures, such as
20 providing security training for employees, a plan for
21 responding to security incidents, and maintaining
22 written security policies and procedures for IT
23 employees to follow.
24 The final step in identifying measures that will
25 provide reasonable defense in depth is a common sense

13

1 balancing of the costs and benefits of available
2 security measures. The balancing process is very
3 similar to how businesses decide sometimes whether to
4 purchase new equipment, except that it includes the
5 potential loss from disclosing the company's business
6 plans, for example. This is called risk management,
7 management by IT professionals and industry.
8 The Commission's cases set out this same
9 approach for analyzing the reasonableness of security
10 measures with one possible difference. The possible
11 difference is that the Commission's approach takes into
12 account potential consumer harm from unauthorized
13 disclosure of the information.
14 So, you might ask, how hard is it to do this?
15 In many instances, it will be relatively easy to
16 qualitatively balance cost and benefit using risk
17 management concepts. Consider the following
18 hypothetical. A company uses a program to store
19 thousands of consumer names and Social Security numbers.
20 A vulnerability in the program was discovered and made
21 public a year ago. At the time, IT professionals
22 classified the vulnerability as a 10 risk on a scale of
23 1 to 10, with 10 being the most critical risk.
24 In less than an hour, an IT employee could fix
25 the vulnerability by installing a free update that was

14

1 made available when the vulnerability was first
2 discovered, and the company didn't do so. The potential
3 loss is very high for this hypothetical. The
4 vulnerability is critical, and disclosing names and
5 Social Security numbers could cause considerable
6 consumer harm. On the other hand, the cost to having an
7 IT professional install the free update is very low.
8 Because the potential consumer loss obviously far
9 exceeds the cost of installing the update, it's
10 unreasonable not to do so.
11 Applying these concepts, LabMD did not pass
12 Defense in Depth 101, not just in one way, but in a
13 number of ways. As set out in paragraph 10 of the
14 complaint, the company failed to identify commonly known
15 or reasonably foreseeable risks to personal information.
16 It did not adequately train employees about security
17 risks and practices. It did not appropriately limit
18 employee access to just the information they needed to
19 do their jobs.
20 It did not correctly or appropriately
21 authenticate users to verify that they are who they say
22 they are. It did not adequately update computer
23 operating systems and equipment. And it did not take
24 reasonable measures to prevent and detect unauthorized
25 access to personal information. And finally, it did not

15

1 implement a comprehensive information security program.
2 LabMD systematically failed to use reasonable
3 security measures to protect very sensitive information.
4 I'd like to talk about two of them in a little more
5 depth. The first is the company's failure to use
6 appropriate measures to prevent and detect unauthorized
7 access to consumer information, as happened here when a
8 LabMD file was shared through a peer-to-peer
9 file-sharing network without alarm bells going at off
10 the company. The network is called peer-to-peer, or
11 P2P, because users can share files directly from their
12 own computers to the computers of other people on the
13 network.
14 The complaint alleges in paragraph 18 that a P2P
15 program called Limewire was installed on a LabMD
16 computer used by the company's billing manager.
17 Limewire allows users, like the billing manager, to
18 select files on their computers to make available to
19 other Limewire users. Hundreds of files on the billing
20 manager's computer were available through Limewire,
21 including some business files.
22 One business file that was available and shared
23 contained highly sensitive information about
24 approximately 9300 consumers, including their names,
25 Social Security numbers, dates of birth, health

16

1 insurance provider names and policy numbers, and
2 standardized medical treatment codes. This is the kind
3 of information that can easily be misused to conduct new
4 account fraud and medical identity theft and disclosing
5 treatment codes that may cause privacy harms.
6 Limewire does present a risk that files that
7 should not be shared will be shared inadvertently with
8 other Limewire users, as likely happened here. The
9 irony is that LabMD had no need to accept this risk,
10 because it admittedly had no need for Limewire. The
11 company could have addressed the risk very easily, but
12 it didn't. If it had, it could have stopped Limewire
13 from being downloaded; it could have prevented or
14 detected its installation on the LabMD computer; and it
15 would have been alerted when files were shared so that
16 it could stop the sharing.
17 It's no excuse here that the billing manager
18 should not have been using Limewire in the first place.
19 People are known to make mistakes and to use programs
20 that they shouldn't, which is why technical security
21 measures or controls are needed to achieve defense in
22 depth.
23 JUDGE CHAPPELL: Limewire, is this something
24 that is free or was it purchased?
25 MR. SHEER: Our understanding is that it was

17

1 free.
2 I'd like to turn to the second failure, and that
3 is the failure to use appropriate measures to identify
4 commonly known or reasonably foreseeable risks to
5 personal information as set out in paragraph 10 of the
6 complaint. Because no single tool can identify all the
7 different security threats a company may face, IT
8 professionals tell us that identifying risks usually
9 requires a variety of measures or tools.
10 One such tool that's familiar to almost all of
11 us is an antivirus program. Another tool is called a
12 penetration test, which usually includes an automated
13 vulnerability scan and related activities. Pen tests,
14 as they're called, probe a company's defenses from the
15 outside looking for cracks, just like an intruder would.
16 A pen test might, again, by looking for a
17 vulnerability in a firewall, looking to test the
18 firewall for a vulnerability, looking for an opening,
19 basically, to get into the network. Once inside the
20 network, the test might test computers and applications
21 or programs, looking for vulnerabilities that could be
22 leveraged to get access to sensitive information.
23 We are told that antivirus programs can't
24 identify holes in firewalls and that pen tests can't
25 identify viruses. Both of them are needed to

18

1 effectively identify risks in networks that connect
2 online like LabMD's. Both are basic, foundational tools
3 that have been used by companies for years.
4 JUDGE CHAPPELL: You're talking about antivirus,
5 but if you have a P2P program, you've created the hole.
6 So, how is your antivirus going to stop something that
7 you've created? What's the point of that?
8 MR. SHEER: That's exactly the point. The point
9 is that the antivirus program is not going to identify
10 the P2P application or program that's on your network.
11 JUDGE CHAPPELL: It's like clicking on the link
12 on the email you shouldn't open. Your Norton Antivirus
13 isn't going to stop that because you clicked.
14 MR. SHEER: You're preaching to the choir, yes.
15 JUDGE CHAPPELL: Well, not necessarily. I'm
16 objective here. My point is, why would I pay for extra
17 antivirus software if I've decided to use P2P software
18 and I know the hole is there? What's the point in
19 telling me I needed to put antivirus on my computer?
20 MR. SHEER: Well, we're not making the argument
21 that they should have been putting an antivirus on their
22 computers, and I will say -- and I thought this was what
23 you said earlier -- that an antivirus program is not
24 going to identify a P2P program, because it's looking
25 for viruses, which are small, malicious programs that

19

1 operate in the background that you don't know about,
2 that you may get on your computer by what you just
3 described, media that comes in with a link that says
4 "Click on this link," you click on the link, and a
5 program -- a virus program is downloaded onto your
6 computer and operates in the background. But that's not
7 what we're alleging here was the problem in this
8 explanation.
9 What we're alleging here was the failure to have
10 a penetration test would not identify to the company
11 other risks that could not be identified by an antivirus
12 program. That's why the IT professionals tell us that
13 you really need to have a variety of tools to identify
14 risks, because there's no one tool that will identify
15 all the threats that a company faces.
16 JUDGE CHAPPELL: Okay. Now I follow why you're
17 talking about antivirus. Go ahead.
18 MR. SHEER: The complaint alleges that LabMD did
19 not use adequate measures, such as pen tests, to
20 identify commonly known or reasonably foreseeable risks.
21 As a result, it was blind to some risks and, therefore,
22 unlikely to effectively guard against them.
23 To sum up, the complaint alleges that LabMD's
24 security failures went beyond sharing a file with
25 sensitive information about 9300 people to a P2P

20

1 network. The company's security practices created
2 vulnerabilities an outsider could stitch together to
3 find a way into the network, to move around the network
4 and explore it, to find sensitive information, and then
5 to package up the information and export it from the
6 network without the company's noticing.
7 LabMD failed to implement reasonable security
8 measures, and that is an unfair act or practice because
9 it caused or is likely to cause substantial consumer
10 injury that's not offset by countervailing benefits to
11 consumers or competition and also not reasonably
12 avoidable by consumers. After all, how can a consumer
13 even know what LabMD's security practices were, let
14 alone assess how adequate or inadequate they might be?
15 One final point. Neither the complaint nor the
16 notice order prescribes specific security practices that
17 LabMD should implement going forward. They do not, for
18 example, require that a certain vulnerability scanning
19 product be used. Because security threats and responses
20 change so rapidly, the order leaves it to the company to
21 determine the particular security measures that, taken
22 together, will provide reasonable security at lowest
23 cost in its circumstances.
24 Although the Commission retains the right to do
25 so, under the notice order and all of the other

21

1 Commission information security consent orders, a strong
2 indication that security is reasonable is a security
3 certification from an independent IT professional who's
4 capable of balancing the costs and benefits and follows
5 protocols commonly used in the profession. These are
6 the same sorts of things that internal IT employees
7 commonly do for companies across the country. Frankly,
8 the order only asks LabMD to do what it should have been
9 doing anyway but didn't.
10 Thank you.
11 JUDGE CHAPPELL: I have one question. I heard
12 you refer to Section 5, but I also heard you refer to
13 various other rules, regulations, et cetera. Is it the
14 Government's position that whatever rule or regulation
15 or statute that you're alleging was violated is
16 contained within the four corners of this complaint?
17 MR. SHEER: What we're saying is that the
18 allegation is that the company failed to comply with
19 Section 5 in engaging an unfair act or practice by
20 failing to provide reasonable security for sensitive
21 information. We are saying that reasonableness is a
22 common sense balancing of cost and benefit and that
23 common sense is available from many, many sources,
24 including organizations -- government organizations,
25 such as the National Institute of Standards and

22

1 Technology, private entities, such as the SANS
2 Institute, and many others as well. So that we are
3 assessing reasonable -- reasonableness in much the same
4 way, following the same process that is commonly used
5 throughout the IT industry now. We add only one
6 additional factor, and that is take into account the
7 potential consumer harm from failing to have reasonable
8 security to protect that information.
9 JUDGE CHAPPELL: I'm not sure you answered my
10 question, Counselor. Are there any rules or regulations
11 that you're going to allege were violated here that are
12 not within the four corners of the complaint?
13 MR. SHEER: I misunderstood. I'm sorry. No.
14 JUDGE CHAPPELL: All right. Thank you.
15 MR. RUBINSTEIN: The facts in this case are
16 pretty simple and pretty clear. The billing manager,
17 the person responsible for handling LabMD's invoicing --
18 a small company, a very limited staff --
19 JUDGE CHAPPELL: Tell me more about what LabMD
20 does. Do you take blood samples?
21 MR. RUBINSTEIN: It's a pathology lab. The
22 customers -- LabMD's customers are doctors. You go in
23 to see a doctor -- and it's a very small specialty
24 business for particular kinds of cancer detection. You
25 go in to see a doctor. He will take a tissue sample for

23

1 biopsy or what have you. They don't do the work in the
2 lab, they send it out, and LabMD's market, which is
3 primarily Georgia and the states surrounding it, it
4 would do biopsies and give diagnoses to help with cancer
5 treatment.
6 JUDGE CHAPPELL: So, that work is actually done
7 in your company offices.
8 MR. RUBINSTEIN: That's correct.
9 JUDGE CHAPPELL: You have got the guys in the
10 white lab coats.
11 MR. RUBINSTEIN: That's correct.
12 JUDGE CHAPPELL: Are you doing blood tests, like
13 cholesterol?
14 MR. RUBINSTEIN: No. No, it's only -- and I
15 don't want to speculate, and we will put this in
16 obviously in the facts, but it's related to cancer
17 diagnoses, but only certain kinds of cancers, prostate
18 cancers, other sort of related maladies.
19 JUDGE CHAPPELL: So, generally a doctor takes a
20 biopsy; they send it to you.
21 MR. RUBINSTEIN: That's correct.
22 JUDGE CHAPPELL: Okay.
23 MR. RUBINSTEIN: So, the doctors are our
24 customers, technically.
25 JUDGE CHAPPELL: And the doctor sends the

24

1 patient data to you? Where does the data come from
2 that's alleged to have been released in this case?
3 MR. RUBINSTEIN: The data came from an internal
4 spreadsheet that was used by the billing manager, as I
5 understand it -- as we understand it, to keep track of
6 the accounts. She was in charge of making sure that the
7 insurance companies got billed for the work that LabMD
8 was doing. It was an internal spreadsheet. It was
9 never meant to be shared with anybody.
10 And actually, I would like to, if I could, just
11 take issue with the file that triggered this
12 investigation was not shared; it was stolen. A company
13 called Tiversa, under a government contract --
14 JUDGE CHAPPELL: Wait. I'd like to make sure I
15 understand the particulars, to get a grasp of the big
16 picture.
17 MR. RUBINSTEIN: Yes, sir.
18 JUDGE CHAPPELL: Somebody like INOVA Fairfax
19 sends their tissue samples to your lab, and they
20 probably have patient identifiable information on them,
21 but then someone in your office developed a spreadsheet
22 on their own, nothing to do with INOVA or Johns Hopkins
23 or any other hospital. That was done internally, this
24 spreadsheet.
25 MR. RUBINSTEIN: The spreadsheets were done

25

1 internally using information that came from the doctors.
2 JUDGE CHAPPELL: Right. But the doctors and the
3 hospitals knew nothing about it.
4 MR. RUBINSTEIN: Well, I mean, I assume that
5 they -- I don't know what they knew to begin with, but
6 I'm going to assume they knew for billing purposes and
7 invoicing we had to have some sort of billing procedures
8 that --
9 JUDGE CHAPPELL: That's what I was going to ask
10 you. Why was the spreadsheet created?
11 MR. RUBINSTEIN: To manage accounts, basically,
12 accounts receivable.
13 JUDGE CHAPPELL: And that spreadsheet had
14 personally identifiable information?
15 MR. RUBINSTEIN: Sure. It would identify the
16 individual, their identifying number, and their
17 insurance information, so that appropriate bills could
18 be sent out.
19 JUDGE CHAPPELL: And did your client bill, for
20 example, Blue Cross or did they bill the hospital or
21 doctor who sent the sample?
22 MR. RUBINSTEIN: I think it differed from
23 patient to patient depending on the particular
24 circumstances, but I'm not 100 percent sure exactly, you
25 know, what happened for each patient.

26

1 JUDGE CHAPPELL: It just -- you know, I find it
2 helps to have a thorough understanding of the business
3 to then go to an interpretation of what's going on and
4 what -- and what has happened and what's not.
5 MR. RUBINSTEIN: Absolutely, Your Honor. It was
6 standard kind of accounts receivable, is the best way to
7 conceptualize what this spreadsheet was, and it was a
8 way internally of tracking who it was and what was being
9 paid and so forth.
10 And as I said, there are a couple of things here
11 from a factual standpoint they are real simple and
12 clear. The billing manager, she was in charge of -- as,
13 you know, the proofs will show, she was in charge of
14 managing money coming in, going out, and so forth,
15 downloaded Limewire. Limewire is a P2P program that was
16 primarily, I think, designed to share music and other
17 files.
18 A government contractor by the time of Tiversa
19 was paid, in conjunction with Professor Eric Johnson to
20 surveil other companies --
21 JUDGE CHAPPELL: How do you spell that?
22 MR. RUBINSTEIN: Tiversa?
23 JUDGE CHAPPELL: Yes.
24 MR. RUBINSTEIN: T-I-V, Victor, E-R-S, as in
25 Sam, -A.

27

1 JUDGE CHAPPELL: Is that like an incorporated
2 company or --
3 MR. RUBINSTEIN: It's a security -- an internet
4 security company based in Pittsburgh, a pretty large
5 company. And apparently they had contracts with several
6 government agencies to go out and see -- knock on doors,
7 as if it were, and see if they could log in and steal
8 files, and they did. And they put out a press release,
9 Tiversa, that is --
10 JUDGE CHAPPELL: And just so you know, this is
11 not argument. You are telling me what you're going to
12 prove at trial.
13 MR. RUBINSTEIN: This is what's going to be
14 proven, talking about right now the facts. They put out
15 a press release claiming that they had found all sorts
16 of breaches with spreadsheets that contained client
17 names, Social Security numbers, birth dates, detailed
18 hospital databases, over 20,000 patients, and the press
19 release mentions the file that was taken from LabMD in
20 this case.
21 The proofs will show that Tiversa notified the
22 Respondent that it obtained one or stole one of LabMD's
23 files --
24 JUDGE CHAPPELL: Let me make sure I understand
25 this. You're saying Tiversa had a contract, they were

28

1 paid by our Government, to try to break in or hack
2 files?
3 MR. RUBINSTEIN: Yes, sir. There was a study
4 done by this Professor Eric Johnson in conjunction with
5 Tiversa. I believe that the study was funded, according
6 to Tiversa, by the Department of Homeland Security,
7 among others. Yeah, it was designed to test the
8 security of networks for confidential health and other
9 information. And we will put into evidence --
10 JUDGE CHAPPELL: Are you aware of the details of
11 that contract?
12 MR. RUBINSTEIN: We don't have a copy of the
13 contract yet. We are going to get it in discovery we
14 hope.
15 JUDGE CHAPPELL: For example, if you're a victim
16 of the hacking, do they inform you and do they tell you
17 what's been done?
18 MR. RUBINSTEIN: Well, that's what they did in
19 this case, and then the testimony, certainly from
20 LabMD's principals, is going to be that they then
21 pitched their business. LabMD turned them down and
22 said, "No, thank you," at which point in time the -- the
23 stolen file made its way to the Government, and this
24 proceeding followed.
25 So, we don't know at what point in time Tiversa

29

1 and the Government began communicating about LabMD. We
2 anticipate that that relationship will be clarified in
3 discovery, and it's obviously something we're very
4 interested in.
5 JUDGE CHAPPELL: All right. You're saying you
6 have proof, they told you you were hacked, they wanted
7 to charge you to prevent attacks, but you're assuming
8 they then spread the infor -- spread the data out.
9 MR. RUBINSTEIN: Well, as far as we know --
10 JUDGE CHAPPELL: Are you making a jump there or
11 do you have proof of that?
12 MR. RUBINSTEIN: No, we believe -- we have proof
13 of that. That's how the file came to the FTC, was from
14 Tiversa. And, in fact, there will be testimony that a
15 lawyer for Tiversa called a lawyer for LabMD, I think
16 about a 12-, 13-month time frame, and said, "Well, we're
17 giving this document now to the Government."
18 JUDGE CHAPPELL: Did you get any complaints from
19 customers, your clients?
20 MR. RUBINSTEIN: No, sir. To the best of our
21 knowledge, this file -- the only entities that have seen
22 this, other than LabMD and its employees, are Tiversa
23 and the Government.
24 JUDGE CHAPPELL: So, it's your position this
25 information hasn't been released.

30

1 MR. RUBINSTEIN: That's correct. What we're
2 also not clear, though, I should say, because this is --
3 as I mentioned, Tiversa puts out a press release
4 identifying a number of other companies for which it
5 attained data. It's not clear to us what happened to
6 that data, where it went, whether it came to the
7 Government, how the decision was made or why the
8 decision was made to disclose LabMD's data. And,
9 obviously, that -- all of those issues, we believe, are
10 very significant and have very immediate, clear legal
11 consequences. And so they are going to be addressed in
12 discovery.
13 We also are, frankly, going to investigate why
14 the Government knowingly commenced an investigation
15 using a stolen file obtained from a government
16 contractor being paid with taxpayer money to steal from
17 LabMD. It doesn't make sense to us.
18 There are a number of very significant legal
19 issues --
20 JUDGE CHAPPELL: Hold on a second.
21 Mr. Sheer, what's the Government's position on
22 the disclosure of the data?
23 MR. SHEER: This comes down to a fundamental
24 disagreement about how Limewire and other P2P
25 applications work.

31

1 JUDGE CHAPPELL: Well, that's my job. I am
2 going to deal with the fundamental disagreement.
3 MR. SHEER: Our view -- and we will put on
4 evidence that shows this -- is that Limewire -- is that
5 the LabMD file was not taken by being stolen; instead,
6 Limewire does two things, basically two things. Someone
7 installs it on their computer. It allows them to
8 designate files on their computer that they will make
9 freely available to anybody else on the Limewire
10 network.
11 JUDGE CHAPPELL: I understand how P2P works. I
12 may not look like it, but I understand technology.
13 MR. SHEER: Okay.
14 JUDGE CHAPPELL: What I want to know is what's
15 your position of what happened to this actual data
16 that's in dispute here or the subject of this dispute?
17 MR. SHEER: Our position is that the information
18 was actually shared voluntarily from LabMD by virtue of
19 its being in the "my shared files" folder in Limewire on
20 the computer.
21 JUDGE CHAPPELL: And you have a witness who's
22 going to say, "I saw it, they shared it with me"?
23 MR. SHEER: We have evidence that will show that
24 the file that is in issue was, in fact, in the "my
25 shared files" folder.

32

1 JUDGE CHAPPELL: That it was available to be
2 viewed.
3 MR. SHEER: Correct. It was available to anyone
4 who might look for it using Limewire.
5 JUDGE CHAPPELL: Kind of like when the
6 Commission posted proprietary data a few years in a case
7 that fortunately was not mine; there was this assumption
8 that nobody had seen it, but now the assumption is
9 somebody did see it?
10 MR. SHEER: Well, we know it was downloaded by
11 one entity, they're saying Tiversa, and we also -- we
12 also know that, because it was available, it could have
13 been downloaded by any number of other people. And one
14 would also want to say, even if you accept all of
15 that -- which we don't -- it would have been very easy
16 for the company to prevent this from having happened in
17 the first place.
18 JUDGE CHAPPELL: And, again, I'm not -- clearly
19 not making any substantive decisions today, but I'm just
20 trying to figure out what the positions are, when I hear
21 something this 180 degrees different. So, what you're
22 telling me, though, is you're not going to have a
23 witness say they saw it, but you intend to prove that it
24 was available publicly.
25 MR. SHEER: We will be able to show that it was

33

1 available publicly and we may be able to have a witness
2 who says they saw it.
3 JUDGE CHAPPELL: Do you have any complaining
4 witnesses who say their data was released or disclosed?
5 MR. SHEER: Not at this time.
6 JUDGE CHAPPELL: Okay.
7 MR. SHEER: We will develop that.
8 JUDGE CHAPPELL: All right. Thank you.
9 MR. RUBINSTEIN: There are some very significant
10 legal issues that are created by these facts. The first
11 is the ambit of the Commission's authority under Section
12 5, which we intend to test. The second is the extent to
13 which the file in question is within the Commission's
14 ambit under Article 1, Section 8. There are due process
15 issues, because notwithstanding counsel's discussions,
16 there are no fixed or ascertainable standards by which
17 LabMD, a small company, could judge the propriety of
18 what it was doing.
19 Proofs will show that the billing manager
20 downloaded Limewire and did it without the knowledge of
21 the company's upper management and contrary to the
22 company policy. This was not a shared file. This was
23 not a shared file at all. It was never meant for public
24 consumption. In fact, there's yet another issue here.
25 LabMD is subject to HIPAA, and the Department of Health

34

1 and Human Services determined that no action was
2 appropriate.
3 So, in effect, you have the Commission
4 overfiling the agency of the Government that Congress
5 designated with primary responsibility for management
6 and regulation of HIPAA.
7 JUDGE CHAPPELL: So, you're saying -- your
8 position is the data was not in a shared folder.
9 MR. RUBINSTEIN: It may have been in a -- it was
10 in a folder and obviously it was accessible to Tiversa.
11 The mechanics of how Tiversa accessed it and what kind
12 of folder it was in are things that we are not clear
13 about and we are going to, through discovery, better
14 ascertain.
15 Certainly, it was not supposed to be made
16 available to the public. That was not LabMD's policy,
17 certainly, and to the extent that the Limewire was
18 downloaded, it was done, as I said, without
19 authorization and contrary to LabMD's standard policies.
20 JUDGE CHAPPELL: I've heard you say a couple
21 times you're a small company. I mean, is that
22 confidential? I mean, are you 5 million, 10 million?
23 What kind of revenues? If it's not -- just ballpark.
24 How small or how large are you.
25 MR. RUBINSTEIN: I would rather not -- I will

35

1 make that information available to you in camera.
2 JUDGE CHAPPELL: That's okay. I'll see it in
3 the documents. I just thought, when you say small, you
4 know --
5 MR. RUBINSTEIN: I would rather not -- we will
6 say it is a small company with less than 50 employees,
7 is my understanding. We will make that available to
8 you, Your Honor.
9 JUDGE CHAPPELL: Less than 50, 5-0, or 15?
10 MR. RUBINSTEIN: I'm sorry, less than 50. But
11 for various reasons, it's a closely held corporation,
12 and I don't want to put the numbers out. But we are not
13 INOVA or Johns Hopkins.
14 JUDGE CHAPPELL: Labcorp?
15 MR. RUBINSTEIN: Not them either.
16 So, what we anticipate with this case, as I
17 said, we are going to have to find out Tiversa's role.
18 We are going to have to find out the extent to which it
19 was involved with and its relationship with the
20 Commission in the decision to move forward with this
21 investigation. And we're going to be filing a series of
22 dispositive motions very early on, because quite
23 frankly, we don't believe the Commission has the
24 authority to be doing what it's doing to LabMD. We
25 don't think that the information --

36

1 JUDGE CHAPPELL: Very early on?
2 MR. RUBINSTEIN: Very early on, within the -- I
3 mentioned this to counsel. We anticipate filing a
4 series of motions within the next two to three weeks.
5 JUDGE CHAPPELL: And you understand who will be
6 deciding those motions?
7 MR. RUBINSTEIN: We are well aware, Your Honor,
8 but we have an obligation to exhaust our remedies. So,
9 we're going to be raising a series of legal issues.
10 We're going to be raising a series of evidentiary
11 objections based on the circumstances, as we understand
12 them today, about how the Government came into
13 possession of the information in the first instance.
14 And then all of the other things that are laid
15 out in the complaint were the result of the knowing
16 acceptance from a government contractor of a stolen
17 file, files stolen, by the way, in contravention of
18 Georgia's law. There was a case in the Eleventh Circuit
19 which was dismissed for want of jurisdiction under the
20 Georgia long arm statute, but there is, you know, a
21 clear suggestion that what Tiversa did violate Georgia's
22 law.
23 JUDGE CHAPPELL: Who brought that case?
24 MR. RUBINSTEIN: LabMD against Tiversa.
25 JUDGE CHAPPELL: And, of course, LabMD didn't

37

1 decide that motion, did they?
2 MR. RUBINSTEIN: Well, it was dismissed based
3 on, like I said, lack of long arm jurisdiction. I have
4 a copy of the Eleventh Circuit decision if you would
5 like it. I can provide that to you right now, if you
6 care to see it.
7 JUDGE CHAPPELL: It won't do me any good until
8 after the hearing starts.
9 MR. RUBINSTEIN: But that's where we're at.
10 We're going to be filing dispositive motions. We fully
11 anticipate that the scope of discovery will be
12 clarified. We look forward to working with the
13 Government to ensure that this matter moves as quickly
14 and as painlessly forward as possible. And we look
15 forward to trying this issue before Your Honor.
16 JUDGE CHAPPELL: Anything else?
17 MR. RUBINSTEIN: I believe, for today, that's --
18 that's enough.
19 JUDGE CHAPPELL: I notice there's another
20 attorney who's appeared in the case for your client.
21 Are you -- can you let us know, is he going to be 50/50?
22 Is he going to be involved in taking witnesses?
23 MR. RUBINSTEIN: Yes, Your Honor. And forgive
24 me, I should have explained this up front. LabMD is
25 represented by Cause of Action, a 501(C)(3) charity that

38

1 does government accountability, government watchdog, and
2 government transparency work. In the interest of their
3 educational mission, they from time to time take on
4 lawsuits that implicate important issues. In this case,
5 there's an organizational issue in the fact that you
6 have a government commission acting and putting in
7 jeopardy a small business without having any clear
8 standards or ascertainable standards for doing so.
9 So, I'm a partner at Dinsmore & Shohl. I have a
10 practice. Cause of Action is a client of mine from time
11 to time. They asked me to serve as lead counsel. There
12 will be a staff counsel from Cause of Action by the name
13 of Michael Pepson who will be involved in this case. A
14 lot of the document production and so forth that we will
15 be doing will be coming from Cause of Action, but I will
16 be serving as lead counsel and he will be assisting me.
17 JUDGE CHAPPELL: All right, thank you.
18 MR. RUBINSTEIN: Thank you.
19 JUDGE CHAPPELL: Mr. Sheer, anything further?
20 MR. SHEER: No, Your Honor.
21 JUDGE CHAPPELL: Okay. Hearing nothing further,
22 we are, until we meet again, adjourned.
23 (Whereupon, at 2:46 p.m., the initial pretrial
24 conference was adjourned.)
25

39

1 CERTIFICATION OF REPORTER
2 DOCKET/FILE NUMBER: DOCKET 9357
3 CASE TITLE: IN RE: LABMD, INC.
4 DATE: SEPTEMBER 25, 2013
5
6 I HEREBY CERTIFY that the transcript contained
7 herein is a full and accurate transcript of the notes
8 taken by me at the hearing on the above cause before the
9 FEDERAL TRADE COMMISSION to the best of my knowledge and
10 belief.
11
12 DATED: 9/25/2013
13
14
15
16 SUSANNE BERGLING, RMR-CRR-CLR
17
18 CERTIFICATION OF PROOFREADER
19
20 I HEREBY CERTIFY that I proofread the transcript
21 for accuracy in spelling, hyphenation, punctuation and
22 format.
23
24
25 SARA J. VANCE, CMRS

EXHIBIT 10

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEDERAL TRADE COMMISSION	)	
	)	
Plaintiff,	)	CIVIL ACTION FILE
	)	NO. 1:12-CV-3005-WSD
v.	)	
	)	ATLANTA, GEORGIA
LabMD, INC., et al.	)	
	)	
Defendants.	)	
	)	

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE WILLIAM S. DUFFEY, JR.,
UNITED STATES DISTRICT JUDGE

Wednesday, September 19, 2012

APPEARANCES OF COUNSEL:

For the Plaintiff: FEDERAL TRADE COMMISSION
(By: Burke W. Kappler
Ryan Thomas Holte
Bradley D. Grossman)

For the Defendants: BALCH & BINGHAM
(By: Christopher S. Anulewicz)

LabMD, INC.
(By: Stephen Frank Fusco)

Proceedings recorded by mechanical stenography
and computer-aided transcript produced by
NICHOLAS A. MARRONE, RMR, CRR
1714 U. S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
(404) 215-1486

Wednesday Morning Session

September 19, 2012

10:01 a.m.

-- -- --

P R O C E E D I N G S

-- -- --

(In open court:)

THE COURT: Good morning, everybody. This is a show cause hearing in FTC v. LabMD, Inc., which is Civil Action No. 12-3005.

Would counsel please announce their appearances?

MR. KAPPLER: Good morning, Your Honor. For the FTC, Burke Kappler, to my right is Ryan Holte and Bradley Grossman.

THE COURT: Good morning.

MR. FUSCO: For the respondents, Stephen Fusco with LabMD, and to my left, Chris Anulewicz with Balch & Bingham, and that's Michael Daugherty.

THE COURT: Good morning.

I haven't had a lot of time to look at the briefs, but I have looked at the briefs, and I just want to frame the issue as it strikes me.

It looks to me -- and I have done this enough to know the deferential responsibility I have to administrative agencies conducting investigations. It's

about the same in this kind of action by the FTC as it would be in others.

So my understanding and my belief is that regulatory agencies have broad authority to do certain things, and when they are within that broad authority, they can do a lot of things, one of which is to conduct these sorts of investigations. And the general rule in my mind is that when that happens, if you are asked to produce information, you have to.

I don't think that's the issue in this case. I think the issue in this case, now having read Section 45 and having read the 2008 resolution, is a question of whether or not this is within the authority of the FTC.

I haven't done any independent research as I would normally do if I had more time for that, so I'm just looking at broad 25,000-foot issues.

It's not entirely clear to me, but it does look like this fundamental is the FTC acting within the scope of its authority under Section 45 was the subject of the initial objections through the Commissioner/Commission process.

In fact, I think even in the submission by the FTC that started this action, they said in their petitions LabMD, Mr. Daugherty, raised a number of claims challenging the FTC's authority to investigate their data security

practices. And so the FTC has made that representation to me.

So we go through the regular administrative practices route or administrative challenge route and you get a decision out of the Commission. So the first question I have is if in fact the general question of whether or not the information being requested of LabMD was within the authority of the Commission, at the Commission level, after that decision, does a party have a right to go somewhere at that point to challenge the Commission's decision.

Because it seems to me that what the Commission is saying is we passed this 2008 resolution. You are saying that we couldn't do that. We wouldn't have passed the resolution unless we thought we could do that. So, therefore, that's why -- the reason why we think that by acting pursuant to the resolution, that we were acting within our authority.

I'm just -- it just seems to me at that point, because of the nature of that process, that a party ought to have a right to say, well, I don't agree with that, and I would like somebody who is fair and objective -- i.e., a district court or whatever federal court has authority when -- and I don't know who does.

So the first question I have is did LabMD at that point have a further review or recourse to challenge their --

to assert their claim that what was being asked was not within the agency's authority.

That's important to me, because then it raises the question of, them not doing that, was that challenge not waived.

Now -- but then I said to myself, well, then there are all these cases where they challenged investigative CIDs, and all those cases say, well, the fundamental question, the first question that a court has to evaluate is that you have to enforce it, but it has to be within the authority of the agency.

So I thought, well, maybe this is the right process, maybe this is where those issues are supposed to be raised. But I will say I don't know the answer to that.

So where I want to focus this morning and before I even get to -- I think before I can get to the enforcement issues is that I have to make sure I understand and correctly decide the within the jurisdiction of the agency issue.

And I don't know, and I apologize for not sending you something beforehand to tell you that we could have put this off and we could have taken another week and I could have focused on that, we could have come back and I could have been more informed and better prepared, but I didn't do that.

So thank you for coming. I assume you traveled from Washington. I got you out of town, and it's always a good town to get out of.

So maybe we can have that discussion now, which is in your view -- I know that you are going to disagree with what LabMD is saying. What I need to know is I need to just have that disagreement presented to me with the right authority so that I can study it.

And I thought the best discussion to have would be how can I have you help me do that. Does that make sense?

MR. KAPPLER: It does, Your Honor.

THE COURT: So how can I have you help me do that?

MR. KAPPLER: Well, Your Honor, would you like me to address the questions that you have raised and perhaps begin the discussion?

THE COURT: That would be great. That would be fine.

MR. KAPPLER: Your Honor, would you prefer if I address you from here or should I come to the podium?

THE COURT: You know, it's probably -- you have got your stuff all laid out there, and these are great microphones. So I don't -- you don't speak with any more authority by walking three feet and standing at the podium.

MR. KAPPLER: Thank you, Your Honor. I appreciate

that.

Well, Your Honor, thank you. May it please the Court, we actually appreciate the Court's speedy time frame for this proceeding, and I understand you would like to have more time to review --

THE COURT: You mean I could have taken longer?

MR. KAPPLER: Well, we do. These are meant to be summary proceedings, and we really appreciate the Court's attention to that fact.

Responding to the question -- you posed a couple of questions. One deals with the FTC's authority over this area, but more importantly you asked the question does the party have the right to raise these claims of authority after the FTC has completed its review of the petitions to limit or quash.

And the answer is not really, Your Honor. Because as the case law explains, this proceeding before you today is really a question of whether the CIDs should be enforced.

The question of whether the FTC has the regulatory coverage or the jurisdiction to actually engage in this or actually to conduct a law enforcement action comes later if we were to in fact then bring a complaint or bring an action or bring an enforcement action against LabMD, which is a decision that has not been made yet.

At that point, LabMD would have recourse to argue

it went outside of the FTC's jurisdiction.

THE COURT: I understand. I'm not sure I totally agree with your -- as a practical matter, as a legal matter, I agree with that general statement, although I understand why you are making the statement.

Because even if you go to our circuit, in '91 when they are looking -- and that was an EEOC case in *Kloster Cruise* -- and it's probably -- maybe the language would be a little different if I had run across an FTC case, but it seems that even when you are in the enforcement process, that fundamentally I have to be satisfied that there is some jurisdictional hook.

And I think there was a case out of the D.C. Circuit involving cigarette labeling. *Carter* I think is the case.

MR. KAPPLER: Yes, sir, *Carter*.

THE COURT: In *Carter,* just looking at the discussion, it appeared that that was an enforcement action, but one of the things that the court did there is, well, let me start to see whether or not there is a grant of authority to the FTC, and that was a lot clearer because the Cigarette Labeling Act specifically granted to the Commission certain -- and they said there it's clear to us the FTC is doing what they are supposed to be doing.

So I think as a general legal principle that I have

to at least do some testing of whether or not what's being investigated is within the authority of the agency.

And just this morning in talking in my chambers, I said because theoretically if -- you know, I don't think the FTC is saying this, but that's because you are a trustworthy lawyer, but there might be other lawyers who are maybe a little more loose with the granted authority that's given.

If the argument is if it's within interstate commerce and it's a practice, then we get to investigate it, well, I could make an argument that a trucking company and the way that they drive trucks over the interstate highway system is -- the driving of trucks is a practice. Whether they do it safely is within interstate commerce, so I can go ahead and issue a CID because I'm investigating drivers' practices on interstate highways.

And then you could do all that, come back and say, well, you know, we have decided we are not going to bring it. Or you say, you know, we have decided the ABC Trucking Company, the practice in which they are engaged in in which they buy trucks, that we have looked at who they hire to drive and the kind of trucks, and we don't think that's the right fit, we are going to bring an action.

And to think that at that point when a complaint is brought, for somebody to say, wait a minute, that goes way

too far, that's not within their jurisdiction, but they have already spent a quarter of a million dollars complying, the court might say, you know, that's right, I don't think that that's what the Section 45 grants to the FTC.

MR. KAPPLER: Well, to be specific, Your Honor, I mean, the hypothetical you have offered, I believe that there is actually a cut-out of FTC jurisdiction for common carriers like --

THE COURT: Well, if you give me more time, I will come up with another example.

MR. KAPPLER: No. But to be clear, Your Honor, I mean, the FTC's jurisdiction is to investigate unfair or deceptive acts or practices in or affecting commerce. And when Congress wrote that language, they did so with the expectation that the Commission would apply it flexibly.

In fact, if you look at some of the cases we've cited --

THE COURT: I agree with all that.

MR. KAPPLER: Okay.

THE COURT: The question is whether or not this is -- but it didn't say it could do it indiscriminately and expansively by just saying I found something in interstate commerce and I found a practice.

MR. KAPPLER: No, Your Honor, it didn't say that. But the point is that the question I think at issue here

is -- the subject of this investigation involves, for example, data security. Does the Commission have the ability to investigate data security under its Section 5 grant of authority, and the answer is yes. And there really isn't anything that anyone can point to where the answer would be no, as a matter of fact.

But getting back to where we started, Your Honor, you looked at *Kloster Cruise,* for instance, from 1991. I mean, I think that case is a great example of the exact -- of the level of analysis that needs to be done here.

Because in that case, what the court said was as long as there is just a plausible argument for jurisdiction, the court should deal with the investigatory issue and let the case proceed to the merits.

And there is a real reason why we do this.

THE COURT: You might be totally right about that. What I'm saying is I don't have enough research and briefing on that issue to move beyond that today, because I think it has been fairly superficially briefed, because I didn't ask you to do it in more detail.

So I guess what I'm saying is I will tell you right now I'm not prepared to enforce the CIDs today until I answer that fundamental question and --

MR. KAPPLER: Well, Your Honor, it might be worth, if I might, sort of discussing a little bit of the law

here.

I mean, it was not briefed extensively, but it was briefed in the briefs in a way. It was raised by LabMD in their opposition, and we addressed it in our brief.

And, you know, really what it comes down to is, I mean, LabMD is taking the position -- has taken the position that at one point twelve years ago in the course of a single report in one sentence, that the FTC disclaimed or disavowed its authority to look at data security under Section 5.

And, first of all, if you read that report -- in fact, if you just read the paragraph in that report where that sentence appears --

THE COURT: See, I'm not -- you are not hearing me.

MR. KAPPLER: Okay.

THE COURT: That really is not one of the important points that they make, because somebody could have said that and been somebody without authority to have said that, and I don't care.

I'm looking at the law. There is a statute. The statute grants certain authorities. And my personal opinion is that that doesn't mean it's unlimited authority, and that the courts have said that there are some constraints on that.

And I don't -- I have not done personally enough research, and your research has not adequately fleshed this out for me, as to what the scope of that authority is and whether in this particular case there is a sufficient hook to the authority and what the defendant has been told about now the exercise of that authority for me to make sure that if I allow these to be enforced, that -- and this is a personal problem I have is that I really have to be comfortable in making legal decisions and going through the process. Maybe I'm too pedantic about that, but that's my nature, and you got me.

And all I want is more from you discussing the more fundamental issue, including the standard as it applies in this particular case as the FTC is asserting its jurisdiction, to conduct this investigation under Section 45 in this 2008 resolution.

MR. KAPPLER: Well, Your Honor, I want to make sure I understand exactly what you are asking from me. Because I mean, what I can do is I can point you to, for instance, the thirty or forty cases we have already brought applying Section 5 or Section 45 in the data security or consumer privacy context.

I can point you to the fact that we have testified to Congress on numerous occasions and told Congress that we view Section 5 as authorizing us to investigate and bring

enforcement actions under -- involving data security and consumer privacy.

We have spoken on panels. We have conducted workshops. We have published guidance for businesses just like LabMD about our view that data security practices can be enforceable under Section 5 if they become unfair or deceptive in some form or fashion. I mean, really --

THE COURT: Do you have any Eleventh Circuit authority or any authority out of my circuit --

MR. KAPPLER: No, Your Honor.

THE COURT: -- within those 45 cases?

MR. KAPPLER: No, I actually can't point to a case -- out of those 45 cases out of the Eleventh Circuit?

THE COURT: I don't think so.

MR. KAPPLER: No. The issue is, Your Honor, most of them have been settlement, they have not been litigated decisions.

On the other hand, though, there is actually no authority from any court saying that Section 5 does not include data security.

THE COURT: And there is no authority that says Section 5 does include it.

MR. KAPPLER: Yes.

THE COURT: So I'm writing on a blank slate, which is my issue.

MR. KAPPLER: Well, but, Your Honor, I think you can take some comfort from the perspective that, again, you are acting consistent with what Congress intended in the first place, which is flexible, broad authority.

THE COURT: Let me just explain something. I'm not here to be comforted. I'm here to do my duty as a judicial officer to interpret the law.

I'm trying as politely as I can tell you that, one, I am not enforcing these CIDs today. I'm asking for your cooperation. And if you need more direction, I'm happy to send you an e-mail telling you specifically the issue that I need addressed.

And that's what I would have done if I had been more thoughtful about this and realized that that's a fundamental issue that I have.

But I'm going to address that fundamental issue. I'm going to do it probably in a written order so that if anybody wants to complain about it to another court, that they will know at least what my reasoning was.

And I think that -- I think based upon my initial review of this that that is -- one of the issues is nobody really has litigated your authority in this area to do this, although you apparently have done a lot of it. That that doesn't mean a party doesn't have a right to raise a legal issue before me and have me decide it.

MR. KAPPLER: Oh, Your Honor, we don't disagree with that. But I think -- I understand your duty as a judicial officer, but I think the Eleventh Circuit has spoken clearly about what a court like this should do in a proceeding like this and the test that it needs to apply.

And that test comes out of *Kloster Cuise,* it comes out of *Genuine Parts v. FTC* from 1971, Fifth Circuit for that case actually.

THE COURT: I'm real good about following what my circuit tells me to do.

MR. KAPPLER: Right.

THE COURT: But I'm also real good about doing it in a way in which I am comfortable that I'm following it with integrity and properly.

MR. KAPPLER: Understood, Your Honor.

Well, Your Honor, let me --

THE COURT: This is only a process -- this is supposed to be a discussion about that process.

MR. KAPPLER: Well, Your Honor, let me put it this way. You are asking me and what I understand you to be saying is can you point me to a case that says my court, preferably in the Eleventh Circuit or even in Georgia, that says the FTC has the authority to investigate data security under Section 5. And the answer is I cannot point you to that case. It doesn't exist, not to my knowledge.

I also, though, can't point you to a case that says the FTC does not have authority under Section 5 to investigate data security in consumer practices.

THE COURT: So what we are going to have to do is we are going to have to go and look at authorities in other contexts to get the contours of the analysis that a district court is supposed to undertake to determine whether or not a grant of authority in an area is within Section 45 and that the passage of a resolution was properly exercised, and now an investigation is being appropriately conducted pursuant to that resolution under Section 45, because that's the original grant of authority.

MR. KAPPLER: Right.

THE COURT: And I know none of you have addressed that, but we need to. That's all I'm saying.

MR. KAPPLER: Well, again, Your Honor, I keep coming back to the fact that, you are right, I mean, the scales balance out, the case law balances out on the plain question at issue.

But on one side, though, there is ample case law discussing the broad grants of authority that have already been given to the FTC by Congress so that in questions like this, in questions where courts are asking what is the FTC's authority, there is a tendency and a deference to the Commission in the finding.

THE COURT: I know. You know, but if that's the case, then why did my friends at the D.C. Circuit write a published opinion in *Carter* going through the analysis? If it is so plain on its face that you can stand up here and I am supposed to say I confess that you are right, there is at least three other judges -- four other judges that said that was entitled to some deliberation.

MR. KAPPLER: Well, Your Honor, I would also point you to the D.C. Circuit's case in *Texaco,* which was an *en banc* decision by all of them, which granted the FTC broad authority, said that it was not appropriate in stages like this to get into these jurisdictional questions because that would hamper the agency's effectiveness in conducting investigations.

So the balance of that with *Carter* is *Texaco*.

Carter, by the way, also did affirm and enforce the subpoenas at issue in that case.

THE COURT: Because they found a specific grant to the Commission pursuant to a legislative act of Congress that entitled the Commission to conduct the investigation that they were conducting.

MR. KAPPLER: And that is Section 5, Your Honor. In this case, that is Section 5. It is a grant to us to investigate unfair and deceptive acts or practices in or affecting commerce.

The resolution in this case, the one passed in 2008, identifies the area that we are looking at. In fact, it's a procedural safeguard for parties just like LabMD and Mr. Daugherty to say we are using our authority, we are telling you exactly what we want to look at, we want to look at your practices related to privacy and data security.

THE COURT: I think you are just arguing to hear yourself argue right now.

I think what I have tried to tell you is there is a process I want to discuss, and I'm happy to do that. I'm happy to fast track it.

And I know this. And you were nice to say that this was prompt. You would not have had a hearing in this as quickly as you had in this Court in almost any court in the country, so you know that I'm paying attention to this and you know that I have a commitment to this.

What I'm asking for you is if you want that commitment to be maintained, then you need to cooperate in the process.

MR. KAPPLER: Your Honor, I want to fully cooperate in the process.

THE COURT: And you need to look at your colleague who is nodding his head, I think trying to give you a signal that we ought to talk about the process and move on.

MR. KAPPLER: Well, Your Honor, it sounds to me as

though you are suggesting we engage in some sort of further briefing on this issue?

THE COURT: Yes.

MR. KAPPLER: Well, Your Honor, I think we would submit we are happy to do that. If Your Honor needs more information or needs more authority, we are happy to produce that.

I think what we are saying is, as we understand the cases as they apply, that's not necessary, but if Your Honor wants to do that, we are happy to do that.

THE COURT: You know, the day that you become appointed an Article III judge, then you can decide what is or is not necessary. But you are an advocate now.

MR. KAPPLER: Yes, Your Honor.

THE COURT: I'm telling you that I need more information. And we can go from me trying to be collegial about this, or I can just order you to do it. What's your preference?

MR. KAPPLER: Your Honor, I really appreciate the Court's willingness to engage in this dialogue. I would like to be collegial about it. If you would like more briefing, I am happy to do that.

And I would ask the Court then how would you propose for us to do it?

THE COURT: I'm going to send you an e-mail, since

you have this I guess insatiable need to have specificity, because the only -- because you don't think I need this, but I'm telling you I do. So I will send you an e-mail today telling you the specific issues to address.

MR. KAPPLER: And will Your Honor lay out a briefing schedule?

THE COURT: Yes, we will.

MR. KAPPLER: Okay. Does Your Honor anticipate counter-replies and so forth?

THE COURT: I do.

MR. KAPPLER: We are happy to provide that, Your Honor.

THE COURT: Thank you. That's going to be put into place, today.

MR. FUSCO: Thank you, Your Honor.

THE COURT: I don't know why it was so hard to decide upon that.

But you know that the weight of authority is in favor of an investigative agency conducting this sort of process. You have already largely participated in the process.

And I'm telling you that this better be an important issue to you and one in which you probably will appeal for me to go through this process. Because if what we are doing is somehow delaying this because ultimately that

you think it's in your client's best interest to get whatever additional information to let the process move forward, and I find that out later, I will be disappointed.

MR. FUSCO: Yes, Your Honor.

THE COURT: I have a long memory.

MR. FUSCO: LabMD, the Section 5 authority under this issue is extremely important to them, and we are well aware of the novelty of the question being presented.

THE COURT: Well, that will be the process, and you will get instructions and a schedule from me today.

MR. FUSCO: Thank you, Your Honor.

MR. KAPPLER: Thank you, Your Honor.

THE COURT: Thank you for coming.

(Proceedings adjourn at 10:24 a.m.)

C E R T I F I C A T E

UNITED STATES OF AMERICA :
:
NORTHERN DISTRICT OF GEORGIA :

I, Nicholas A. Marrone, RMR, CRR, Official Court Reporter of the United States District Court for the Northern District of Georgia, do hereby certify that the foregoing 23 pages constitute a true transcript of proceedings had before the said Court, held in the city of Atlanta, Georgia, in the matter therein stated.

In testimony whereof, I hereunto set my hand on this, the 19th day of September, 2012.

/s/ Nicholas A. Marrone

NICHOLAS A. MARRONE, RMR, CRR
Registered Merit Reporter
Certified Realtime Reporter
Official Court Reporter
Northern District of Georgia

EXHIBIT 11

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

RESPONDENT LabMD, INC.'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

TABLE OF CONTENTS

PUBLIC

RESPONDENT LabMD, INC'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

Please take notice that, pursuant to Commission Rule 3.22(a), 16 C.F.R. § 3.22(a), Respondent LabMD, Inc. (LabMD), hereby moves to dismiss the Federal Trade Commission's (the "Commission" or "FTC") Administrative Complaint (the "Complaint") in its entirety with prejudice and to stay all proceedings before the Administrative Law Judge (ALJ) pursuant to Commission Rule 3.22(b), 16 C.F.R. § 3.22(b), while this Motion is under review.

INTRODUCTION

The only federal court to address the legitimacy of the FTC's claimed authority to regulate data-security practices as "unfair" acts or practices under Section 5 of the Federal Trade Commission Act (FTCA), 15 U.S.C. § 45, said "there is significant merit" to the argument that Section 5 does not provide general jurisdiction over data-security practices and consumer-privacy issues.[1] *FTC v. LabMD*, No. 1:12-cv-3005-WSD, Dkt. No. 23, at 6-7 (N.D. Ga. Nov. 26, 2012). When asked to cite a case that "says the FTC has the authority to investigate data security under Section 5," a Commission attorney admitted that "I cannot point you to that case. It doesn't exist…." Hearing Transcript, *FTC v. LabMD*, No. 1:12-cv-3005-WSD, at 16:20-25 (N.D. Ga. Sept. 19, 2012).

[1] The court, noting its "sharply limited" role, explained that the "subpoena enforcement proceeding is not the proper forum" to decide the scope of statutory jurisdiction. *FTC v. LabMD*, No. 1:12-cv-3005-WSD, Dkt. No. 23, at 6-7. It only found that the FTC had made a "plausible" argument that it had jurisdiction to *investigate* whether LabMD had engaged in unfair or deceptive practices. *Id.* at 1-2, 6-7, 12-13 & n.3. Notably, the FTC's Complaint does not allege that LabMD engaged in any deceptive practices whatsoever. *See* Compl. ¶¶22-23.

The FTC has not only repeatedly told Congress that the Commission does not have Section 5 jurisdiction over data-security practices but also repeatedly asked for the broad authority to regulate such practices. Congress, in turn, has repeatedly refused, delegating the FTC only very narrow and limited authority over data-security practices in circumstances that do not obtain here.[2] In fact, Congress has given the Department of Health and Human Services (HHS), and not the FTC, the sole and specific authority to regulate the patient-information data-security practices at issue in this case.

Even the President has rejected the FTC's power-grab approach to data-security regulation.[3] See Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

---

[2] Congress would not have made these specific delegations if it believed that the FTC had general Section 5 authority to regulate patient-information and other data-security practices. Rather, these delegations demonstrate that Congress ratified the Commission's historic understanding of the limits on its Section 5 jurisdiction and confirm that the FTC's Section 5 "unfairness" authority does not extend to the patient-information data-security practices at issue here. *See infra* Section I.B.

[3] The President apparently recognizes that the FTC's "sue now, offer guidance later" approach is bad policy and unconstitutional to boot. His Order requires the Department of Commerce, through the National Institute of Standards and Technology (NIST), to lead the creation of a baseline set of standards for a "Cybersecurity Framework" establishing a "set of standards, methodologies, procedures, and processes" and including implementation "guidance." *See* Exec. Order No. 13,636 § 7(b). The Framework must "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach" with specific "information security measures and controls" operators can implement to "identify, assess, and manage cyber risk." *Id.* NIST must "engage in an open public review and comment process." *Id.* § 7(d).

The FTC's attack on LabMD and other companies is contrary to each of the steps in the President's Executive Order for effective and lawful data-security regulation. The FTC has not (1) issued any standards, methodologies, procedures, or processes for Section 5 compliance; (2) established guidance for measuring implementation and performance of compliant data-security protections; (3) identified specific information security measures and controls that a business might adopt; or (4) engaged in an open public review and comment process. There is simply no reason why the FTC should not be required to follow the President's process of requiring rules, regulations, and standards *before* the government brings abusive enforcement actions and makes shifting and uncertain compliance demands.

The Complaint is a classic example of regulatory overreach and, accordingly, it should be dismissed in its entirety with prejudice for the following reasons.

First, Congress has not given the FTC the power to use its Section 5 "unfairness" authority to do what it has done to LabMD here, and so this action is illegal and illegitimate. *La. Pub. Serv. Com. v. FCC*, 476 U.S. 355, 374 (1986).

Second, even if Section 5 authorized the FTC to broadly regulate data-security practices as "unfair" acts or practices, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), as interpreted and enforced by HHS, control. More recent and more specific than the FTCA, HIPAA and HITECH manifest Congress's unambiguous intent to give HHS regulatory authority over patient-information data-security and to displace whatever Section 5 authority the FTC might have to regulate LabMD's data-security practices as "unfair" acts or practices.

Third, the FTC's failure to promulgate *any* data-security regulations, standards, or guidance that would allow LabMD to ascertain with reasonable certainty what data-security practices the Commission believes Section 5 to forbid or require, and its *ex post facto* enforcement practices, deny LabMD and others similarly situated of fair notice and violate the Constitution and the Administrative Procedure Act (APA).

Fourth, the acts or practices alleged in the Complaint are not "commerce" within the scope of the FTCA.

Fifth, the Complaint couches legal conclusions as factual statements and therefore fails to state a facially plausible claim for relief.

STATEMENT OF FACTS

LabMD is a small medical company providing its physician-customers with cancer diagnoses. These physicians send LabMD their patients' blood, urine, and tissue for sampling, together with relevant patient identification and insurance information. LabMD does the testing and then sends back a diagnosis to the requesting doctor.

LabMD's patient-information data-security practices are, and were at all times relevant, regulated under HIPAA and HITECH. Congress tasked HHS to implement and enforce these statutes, and it has promulgated regulations to do so.[4] LabMD has never been accused of violating HIPAA or HITECH by the FTC, HHS, or anyone else. *See* Initial Pretrial Conference Transcript, *In the Matter of LabMD, Inc.*, Dkt. No. 9357, at 22:10-13 (Sept. 25, 2013)(hereinafter "Trans.").

The genesis of this action appears to have been in early 2008, when, without LabMD's knowledge or consent, Tiversa, Inc. (Tiversa), a government contractor that created and exploited data breaches to generate business, took possession of a single LabMD physician patient-information spreadsheet file (the "PI file"). Complaint, *Tiversa et al. v. LabMD et al.*, Dkt. 1, No. 2:13-cv-01296-NBF, at 4 ¶¶18-19 (W.D. Pa. Sept. 5, 2013)(hereinafter "Tiversa Compl."). Tiversa has boasted to Congress about its practice of taking computer files from unsuspecting third persons without their knowledge or permission using a "unique technology" unavailable to the general public. *See Hearing Before the H. Subcomm. on Commerce, Trade, & Consumer Protection*, 111th Cong. 3-4 (2009)(statement of Robert Boback, CEO, Tiversa).

---

[4] *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1)("Security standards for health information" established and enforced by HHS); 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000)(HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003)(HHS's HIPAA Security Rule); 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013)(HHS's HITECH Breach Notification Rule).

Tiversa said in a May 28, 2009, press release (since pulled from the Internet) that in "a typical day" it might see sensitive information "of tens of thousands" being unknowingly "disclosed" by a hospital or medical billing company, a third-party payroll provider, or a Fortune 500 company. *See* Press Release, "Tiversa Identifies Over 13 Million Breached Internet Files in the Past Twelve Months" (May 29, 2009). It also said that, working with Dartmouth College researchers under a government contract, it searched file-sharing networks for key terms associated with the top ten publicly traded healthcare firms in the country, and "discovered" what it called "a treasure trove of sensitive documents," such as a spreadsheet from an AIDS clinic with Social Security numbers, addresses, and birth-dates; hospital databases with Social Security numbers, contact details, insurance records, and diagnosis information on 20,000 patients; the PI file; and "350+ megabytes of data comprising sensitive reports relating to patients of a group of anesthesiologists."

After taking LabMD's property, Tiversa telephoned LabMD offering "remediation services" and a cost estimate. Tiversa Compl. ¶¶19-21. That same day, Tiversa sent LabMD three follow-up sales-pitch emails. *See LabMD, Inc. v. Tiversa, Inc.*, 509 Fed. Appx. 842, 843 (11th Cir. 2013). Over the next two months, Tiversa sent six more sales-pitch emails to LabMD. *See id.* Communications between LabMD and Tiversa stopped only when "LabMD did not retain Tiversa's services." Tiversa Compl. ¶22.

Tiversa then gave the Commission the purloined PI file. Tiversa Compl. ¶¶25-26. Apparently, the PI file was the only file of those mentioned in Tiversa's Press Release given to the Commission. And, with this file in hand, the FTC began investigating LabMD. After years of intrusive and costly discovery, including multiple civil investigate demands (CIDs),

depositions, and document productions, on August 28, 2013, the Commission voted unanimously to issue the Complaint.

The Complaint alleges that LabMD violated Section 5's prohibition of "unfair" acts or practices by allegedly engaging in data-security practices that, "taken together," fail to meet the Commission's unspecified standards. *See* Compl. ¶10. The Complaint does not allege that LabMD engaged in "deceptive" acts or practices. *Id*. ¶¶22-23. Nor does it allege that any "consumers" have suffered any harm due to the Tiversa take.[5] *Id*. ¶¶17-19. Instead, it alleges in vague, conclusory terms that LabMD engaged in unspecified "unfair acts or practices."

Tellingly, the Complaint does not cite any regulations, guidance, or other standards for what patient-information data-security practices the Commission believes to be "adequate" or "readily available" or "reasonably foreseeable" or "commonly known" or "relatively low cost." *Id*. ¶¶10-11. It does not specify what regulations, guidance, or standards LabMD fell short of or what combination of LabMD's alleged failures to meet these unspecified requirements, "taken together," violate Section 5. *Id*. ¶10. It does not allege that LabMD's claimed "security failures" caused "consumers" to suffer any economic or other injury. *See id*. ¶¶10-11, 17-21.

The Complaint alleges that LabMD's "Day Sheets and a small number of copied checks" were found by the Sacramento Police "in the possession of individuals who pleaded no contest to state charges of identity theft." *Id*. ¶21. But it does not allege that those "individuals" in fact used LabMD's Day Sheets and copied checks to engage in identity theft or caused any of LabMD's "consumers" to suffer any injury. *See id.* Instead, the Complaint alleges that "[a] number of the SSNs in the Day Sheets are being, or have been, used by people

[5] As LabMD explained in its Answer, what the Complaint calls LabMD's "consumers" are in reality LabMD's referring physicians' patients. It is these physicians, and not their patients, who are LabMD's customers and the consumers of its diagnostic services.

with different names"—which, even if true, may be mere correlation (the Complaint does not allege any causation)—and speculates that this "*may indicate* that the SSNs have been used by identity thieves." *Id.* (emphasis added).

Asked about other sources of data-security standards, the FTC said the "Commission has entered into almost 57 negotiations and consent agreements that set out a series of vulnerabilities that firms should be aware of, as well as the method by which the Commission assesses reasonableness." Trans. 9:18-22. The FTC pointed to "public statements made by the Commission" and so-called "educational materials that have been provided" as standards. Trans. 9:23-25. In addition, 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 that the Commission is following in deciding reasonableness," except that the "Commission's process" involves "calculation of the potential consumer harm from unauthorized disclosure of information." Trans. 10:1-7. The FTC also referenced "guiding principles" and stated that "[t]here are lots of sources for the principles, such as materials published by the National Institute of Standards and Technology [NIST], continuing education for IT professionals, practical IT experience, and lessons learned from publicized breaches." Trans. 11:21-12:2.

But critically, the FTC did not claim that any of the above has the force of law or creates any binding duties and obligations.

The FTC also accused LabMD of violating Section 5 "by failing to provide reasonable security for sensitive information," opining "that reasonableness is a common sense balancing of cost and benefit and that common sense is available from many, many sources, including organizations—government organizations, such as the National Institute of Standards, private entities, such as the SANS Institute, and many others as well." Trans. 21:19-22:2. But again, the

FTC did not claim that LabMD violated any data-security standards that have the force of law, such as the patient-information data-security regulations implementing HIPAA.

In fact, the FTC has not accused LabMD of violating any data-security statutes, rules, or regulations. At the initial pretrial conference, 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?" Trans. 22:10-12. The FTC responded "No." Trans. 22:13. The FTC also admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Trans. 20:15-17. The FTC has never promulgated patient-information data-security regulations, guidance, or standards under Section 5 and, apparently, it has no plans to do so: "[T]here is no rulemaking, and no rules have been issued, other than the rule issued with regard to the Gramm-Leach-Bliley Act…for financial institutions." Trans. 10:11-15.

STANDARD OF REVIEW

A Respondent may raise jurisdictional and other legal defenses in a motion to dismiss, which is treated like a Fed. R. Civ. P. 12(b)(6) motion for failure to state a claim upon which relief can be granted. *In re Union Oil Co.*, 138 F.T.C. 1, 16 (F.T.C. 2004). The FTC bears the burden of establishing jurisdiction. *See* Commission Rule 3.43(a), 16 C.F.R. § 3.43(a); *In re POM Wonderful LLC*, 2012 FTC LEXIS 106, 463-65 (F.T.C. May 17, 2012)(Initial Decision). It may not do this by pleading legal conclusions, as it has done here. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Instead, there must be facts showing grounds for a plausible claim for relief, not merely labels and conclusions and a formulaic recitation of the elements. *Id. at 679; Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

ARGUMENT

I. THE COMMISSION LACKS SECTION 5 "UNFAIRNESS" AUTHORITY TO REGULATE PATIENT-INFORMATION DATA-SECURITY PRACTICES.

Section 5 prohibits unfair acts or practices in or affecting commerce. 15 U.S.C. § 45(a)(1). The Commission does not have carte blanche to regulate anything and everything it unilaterally deems "unfair." *See, e.g., Scientific Mfg. Co. v. FTC*, 124 F.2d 640, 644 (3d Cir. 1941)(holding that Section 5 does not authorize the Commission to regulate publications "concerning an article of trade by a person not engaged or financially interested…in that trade," because otherwise it "would become the absolute arbiter of the truth of all printed matter"). In fact, in 1994 Congress enacted limiting language to control the FTC's misuse of its Section 5 unfairness authority. *See* 15 U.S.C. § 45(n); Howard Beales III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. PUB. POL'Y & MKTG. 192 (2003)(former Director of FTC's Bureau of Consumer Protection describing how Congress "reigned in" Commission "abuse" of its Section 5 unfairness authority), *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm (accessed Nov. 7, 2013).

The FTC must show that it has congressionally delegated authority to regulate LabMD's patient-information data-security practices. *City of Arlington v. FCC*, 133 S. Ct. 1863, 1869 (2013)(agencies' power to act and how they are to act is authoritatively prescribed by Congress, so when they act beyond their jurisdiction, what they do is ultra vires); *see, e.g., ABA v. FTC*, 430 F.3d 457, 468-71 (D.C. Cir. 2005)(holding that the FTC's interpretation of the Gramm-Leach-Bliley Act to authorize it to regulate attorneys engaged in the practice of law exceeded the Commission's statutory authority and was therefore invalid). And, the law requires the FTC to exercise its Section 5 unfairness authority consistent with the congressionally enacted administrative structure. *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125, 133

(2000). Finally, the controlling authorities hold the scope of Section 5 authority must be viewed in the light of other relevant statutes, "particularly where Congress has spoken subsequently and more specifically to the topic at hand."[6] *Id.* at 133; *see also FTC v. Nat'l Cas. Co.*, 357 U.S. 560, 562-63 (1958), *superseded by statute* (examination of subsequent statute and its legislative history demonstrates that it limits the FTC's Section 5 regulatory authority).

Section 5's plain language does not authorize patient-information data-security regulation, and Congress has enacted many statutes that, taken together, independently prohibit the FTC from regulating patient-information data-security and strictly cabin its authority to regulate data-security practices in other economic sectors. The FTC does not have the authority to regulate LabMD's patient-information data-security practices. Therefore, the Complaint should be dismissed.

A. Congress Authorized HHS, Not The FTC, To Regulate Patient-Information Data-Security Practices.

Congress has enacted specific legislation, HIPAA and HITECH, setting patient-information data-security standards and delegating to HHS the relevant interpretative and enforcement authority. Consequently, even if Section 5 does authorize the FTC to regulate data-security, which it does not, the Commission lacks legal sanction for the things that it has done to LabMD.

1. Controlling interpretative canons hold the FTC's general Section 5 authority (if any) must yield to the specific patient-information statutes and regulations.

To begin with, the well-known interpretative canon that a general statute must yield to a more specific one applies here. As the Supreme Court recently held:

[6] The Commission has admitted to Congress that this is how Section 5 should be interpreted. *See* FTC, *Policy Statement on Unfairness* 2 (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

> The general/specific canon...has full application as well to statutes such as the one here, in which a general authorization and a more limited, specific authorization exist side-by-side. There the canon avoids not contradiction but the superfluity of a specific provision that is swallowed by the general one, "violat[ing] the cardinal rule that, if possible, effect shall be given to every clause and part of a statute."

RadLAX Gateway Hotel, LLC v. Amalgamated Bank, 132 S. Ct. 2065, 2070-71 (2012)(citation omitted).

HIPAA requires LabMD to meet security standards for electronic health information, such as the PI file. HITECH requires HIPAA-regulated entities to provide notice of unsecured breaches of health information in certain circumstances and strengthens protections for such data. Congress vested HHS with exclusive administrative and enforcement authority with respect to HIPAA-covered entities under these laws.[7] *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1)("Security standards for health information"). Recognizing this, the FTC has repeatedly told Congress that HIPAA and its privacy rule are not enforced by the Commission.[8]

---

[7] Unlike the Commission, HHS has actually promulgated regulations establishing reasonably ascertainable patient-information data-security standards.

[8] For example, in March 2005, Commission Chairwoman Deborah Majoras said that HIPAA is "not enforced by the Commission." *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Statement Before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs*, 109th Cong., 6 (2005). This understanding was reaffirmed before Congress in 2007. *See Protecting the Privacy of the Social Security Number from Identity Theft: Statement Before the Subcommittee on Social Security of the House Committee on Ways and Means*, 110th Cong. 10 (2007)(prepared statement of Joel Winston, FTC). The preambles to HHS's HIPAA rules refer to the single national standard the HIPAA regulations establish. *See* 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000)(Privacy Rule)("This…rule establishes, for the first time, a set of basic national privacy standards and fair information practices…."); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003)(Security Rule)("The purpose of this…rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information."); *see also* U.S. Dep't of Health & Human Servs., *Security 101 for Covered Entities, HIPAA Security Series*, Vol. 2/Paper 1, 3 (2007)("Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry."), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (accessed Nov. 3, 2013).

HITECH's plain language confirms Congress's intent that data-security standards for HIPAA-covered entities be regulated exclusively by HHS, not the FTC. HITECH §13422(b)(1) directs HHS, in coordination with the FTC, to study data-security requirements for non-HIPAA-covered entities and determine "which Federal government agency is best equipped to enforce such requirements recommended to be applied to…[non-HIAPA-covered entities]…and a timeframe for implementing regulations based on such findings." Pub L. 111-5 § 13422(b)(1), 123 Stat. 226, 277 (2009); *see also* 42 U.S.C. § 17937 (giving the FTC authority to establish temporary data-breach notification requirements for non-HIPAA-covered entities).

If the Commission already had such authority, HITECH and many other data-security statutes would be superfluous. Indeed, if Congress intended to give the FTC authority to regulate patient-information data-security (or believed that the FTC already had this authority), then it would not have drawn a clear distinction between HIPAA-covered and non-HIPAA-covered entities and specifically given the FTC such limited authority to regulate non-covered entities, for the mention of one thing suggests the exclusion of another.[9] *See, e.g., United States v. Lopez*, 938 F.2d 1293, 1297 (D.C. Cir. 1991); *see Indep. Ins. Agents of Am., Inc. v. Hawke*, 211 F.3d 638, 645 (D.C. Cir. 2000)("[T]he cannons of avoiding surplusage and expressio unius are at their zenith when they apply in tandem."). Clearly, Congress charged HHS, and not the FTC, with regulating LabMD's patient-information data-security practices, and it is inappropriate for the Commission to bulldoze these boundaries. *See* 78 Fed. Reg. at 5,687-5,702.

[9]As HHS recently explained, the "entities operating as HIPAA covered entities and business associates are subject to HHS' and not the FTC's, breach notification rule." 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013); *accord* 74 Fed. Reg. 42,962, 42,964-65 (Aug. 25, 2009)("HIPAA-covered entities and entities that engage in activities as business associates of HIPAA-covered entities will be subject only to HHS' rule and not the FTC's rule….").

2. The *Billing* doctrine controls and so the FTC has no authority.

Because there is a "clear repugnancy" between the specific and targeted regulatory enactments of HIPAA and HITECH, on the one hand, and Section 5's general unfairness language, on the other, the later must yield to the former, and so the FTC has no authority over LabMD's patient-information data-security. *See Credit Suisse Sec. LLC v. Billing*, 551 U.S. 264, 275 (2007).

In *Billing*, the Supreme Court held that the regulatory provisions of the securities laws, by implication, precluded the more general antitrust law. Preclusion obtained in that case based on an analysis of (1) the existence of regulatory authority under the securities law to supervise the activities in question; (2) evidence that the responsible regulatory entities exercise that authority; (3) a resulting risk that the specific securities and general antitrust laws, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct; and (4) the possible conflict between the laws with respect to affected practices that lie squarely within an area of financial market activity that the securities laws seek to regulate. *See id.* at 275-76.

HIPAA/HITECH and the FTC's claimed Section 5 authority to regulate patient-information data-security practices are "clearly incompatible," and so *Billing* holds that Section 5 and the FTC must yield. This is because (1) Congress gave HHS specific regulatory authority over patient-information data-security practices; (2) HHS exercises that authority, as evidenced by its repeated promulgation of data-security standards for healthcare providers, *see e.g.* 78 Fed. Reg. 5,566 (Jan. 25, 2013); (3) as demonstrated by this proceeding, there is a risk of conflicting standards of conduct (notably, the FTC agrees that LabMD has not violated HIPAA or HITECH, Trans. 22:10-13); and (4) this possible conflict with Section 5 affects practices that lie squarely within an area of healthcare activity regulated under HIPAA/HITECH. *See supra* notes 4 & 9.

Thus, HIPAA/HITECH preclude application of Section 5 to LabMD's patient-information data-security practices. *See Billing*, 551 U.S. at 275-76.

B. Congress Has Not Given The FTC The Plenary Power To Regulate Data-Security Through Its Section 5 "Unfairness" Authority.

The FTC claims its general Section 5 "unfairness" authority allows it to regulate LabMD's patient-information data-security. However, Congress has never given the Commission such authority and has, in fact, repeatedly made it clear that the FTC's power is very limited in application and very narrow in scope.

1. The FTC's claim of general Section 5 "unfairness" authority to regulate data-security practices is contradicted by Congress's many specific data-security delegations.

The FTC's claim of general Section 5 "unfairness" authority to regulate LabMD and other companies is contradicted by Congress's many specific delegations of data-security authority.

To begin with, when Congress has wanted the FTC to have data-security authority, it has said so. To date, Congress has specifically authorized the Commission to regulate data-security practices in at least three statutes, including the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Act (COPPA).[10] The FTC has argued elsewhere that the FCRA, GLBA, and COPPA merely "enhance FTC authority

[10] The FCRA, 15 U.S.C. § 1681 *et seq.*, as amended by the Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 111 Stat. 1952 (2003), establishes requirements for the collection, disclosure, and disposal of data collected by consumer reporting agencies and requires the FTC and other agencies to develop rules for financial institutions to reduce the incidence of identity theft. The GLBA, Pub. L. 106-102, 113 Stat. 1338 (1999)(codified 15 U.S.C. §§ 6801-6809), mandates data-security requirements for financial institutions and instructs the FTC and federal banking agencies to establish standards for financial institutions "to protect against unauthorized access to or use of such records or information," 15 U.S.C. § 6801(b)(3). The COPPA, Pub. L. 105-277, 112 Stat. 2681 (1998)(codified 15 U.S.C. § 6501 *et seq.*), requires website operators to establish and maintain reasonable procedures to protect the confidentiality and security of information gathered from children.

with new legal tools," such as "rulemaking and/or civil penalty authority…." Plaintiff's Opposition to Motion to Dismiss, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-SCM, Dkt. No. 110, at 12 (D. N.J. May 20, 2013)(the "FTC Opposition"). But this argument fails, for these statutes explicitly authorize the Commission to set substantive data-security standards. *See* 15 U.S.C. §§ 1681m(e)(1), 6804(a)(1)(C), 6502(b), and to enforce those standards under the FTCA, *see* 15 U.S.C. §§ 1681s(a), 6805(a)(7), 6505(d). If Section 5 generally authorized the FTC to do these things, these provisions would be meaningless exercises, *Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47, 58 (2006), as "there would have been no reason for Congress to have included" them, *Stone v. INS*, 514 U.S. 386, 397 (1995). The Commission cannot assume that Congress passes purposeless legislation. *Babbitt v. Sweet Home Chapter of Cmtys. for a Great Or.*, 515 U.S. 687, 701 (1995). Therefore, FCRA, GLBA, COPPA, and other narrowly tailored statutes are the only authorities authorizing the FTC to regulate data-security practices of any sort.

At the same time, Congress has enacted numerous other targeted statutes specifically delegating statutory authority over data-security, including HIPAA, HITECH, the Cable Television Consumer Protection and Competition Act, Pub. L. 102-385, 106 Stat. 1460 (1992)(codified at 47 U.S.C. § 521 *et seq.*); the Video Privacy Protection Act, Pub. L. 100-618, 102 Stat. 8195 (1988)(codified at 18 U.S.C. § 2710); Driver's Privacy Protection Act of 1994, Pub. L. 103-322, 106 Stat. 2099 (1994)(codified at18 U.S.C. § 123); and the Computer Fraud Abuse Act of 1986, Pub. L. 99-474, 100 Stat. 1213 (1986)(codified as amended at 18 U.S.C. § 1030 *et seq.*).[11] If the FTC's Section 5 unfairness authority included general, economy-wide authority to regulate data-security, then all of these statutes, creating and delegating regulatory

[11] This list is illustrative, not exhaustive.

authority to HHS and other agencies, would also necessarily be superfluous nullities. The Commission's Section 5 power-grab here therefore offends the rule against attributing redundancy to Congress, *Gutierrez v. Ada*, 528 U.S. 250, 258 (2000), and is at odds with the interpretive canon that no statute should be interpreted in a fashion that renders its parts "inoperative or superfluous." *See Corley v. United States*, 556 U.S. 303, 314 (2009).

2. The Commission's claim of Section 5 "unfairness" authority to regulate data-security economy wide is contrary to congressional intent and to controlling Supreme Court authorities.

As the Commission itself frequently acknowledged—until it recently reversed course without explanation or opportunity for notice and comment from stakeholders, both in violation of the law, *see FCC v. Fox TV Stations, Inc.*, 556 U.S. 502, 514-15 (2009)(an agency must explain policy change)—Section 5 does not give the FTC the authority to regulate data-security practices as "unfair" acts or practices or the authority to require firms to adopt information practice policies.[12] This is why Congress enacted FCRA, GLBA, COPPA, HIPAA, HITECH, and numerous other targeted data-security laws.

[12] For many years, the Commission said its authority over data-security matters was "limited...to ensuring that Web sites follow their stated information practices." *Consumer Privacy on the World Wide Web, Hearing before Subcomm. on Telecomm. of the H. Comm. on Commerce Subcomm. on Telecomm.*, 105th Cong. n.23 (1998)(statement of Robert Pitofsky, Chairman, FTC), *available at* http://www.ftc.gov/os/1998/07/privac98.htm; *see also* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 137 (2008). As a Commission official explained in 2001, "'[t]he agency's jurisdiction is (over) deception….The agency doesn't have the jurisdiction to enforce privacy.'" Jeffrey Benner, *FTC Powerless to Protect Privacy*, Wired (May 31, 2001), http://www.wired.com/politics/security/news/2001/05/44173 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC); *accord* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, 34 (2000)(hereinafter "*2000 Privacy Report*"), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (accessed November 3, 2013); FTC, *Privacy Online: A Report to Congress*, 41 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf ("Commission [generally] lacks authority to require firms to adopt information practice policies….")(accessed Nov. 3, 2013); *see also Protecting Information Security and Preventing Identity Theft, Hearing before Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census of H. Comm. on Gov't Reform,*

The Commission's lack of power to regulate data security through its general Section 5 "unfairness" authority also explains why the Commission has, for over a decade, asked Congress for legislation authorizing it to do what it has done to LabMD.[13] In May 2012, John Leibowitz, then-Commission Chairman, asked once more for the power to enforce data-security measures.[14] Yet, Congress has consistently refused, over a period of many years, to give the Commission what it wants,[15] considering and rejecting several proposals to give the

---

108th Cong. 7 (statement of Orson Swindle)(2004)("To date, the Commission's security cases have been based on its authority to prevent deceptive practices."), *available at* http://www.ftc.gov/os/2004/09/040922infosecidthefttest.pdf (accessed Nov. 3, 2013).

[13] *See, e.g.*, *2000 Privacy Report* at 36-37 (asking Congress to enact legislation requiring websites to "take reasonable steps to protect the security of the information they collect" and providing "the authority to promulgate more detailed standards"); *see also Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011)(statement of David C. Vladeck, Director of the Bureau of Consumer Protection, FTC)("[T]he Commission reiterates its support for federal legislation that would…impose data security standards on companies…."); *Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011)(statement of Edith Ramirez, Commissioner, FTC)(same); *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before H. Comm. on Energy & Commerce*, 111th Cong. 12 (2009)(prepared statement of Eileen Harrington, FTC)(The FTC "has recommended legislation requiring all companies that hold sensitive consumer data to take reasonable measures to safeguard it.").

[14] *Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing Before S. Comm. on Commerce, Science, and Transportation* 112th Cong. 1-2 (2012)(statement of John Leibowitz, Chairman, FTC). Leibowitz noted in a footnote that then-Commissioner Thomas Rosch believed that "in contravention of our promises to Congress, [the Commission's] privacy framework is based on an improper reading of our consumer protection 'unfairness' doctrine…." *Id.* at 3 n.2. Indeed, even the Commission's 2008 Resolution did not claim that the Commission can regulate data-security practices under a pure unfairness theory. *See* Resolution Directing Use of Compulsory Process In Nonpublic Investigation of Acts and Practices Related to Consumer Privacy And/Or Data Security, File No. P954807 (Jan. 3, 2008)(authorizing an investigation into "deceptive or unfair acts or practices related to consumer privacy and/or data security…in violation of Section 5"). The Complaint has not alleged that LabMD engaged in deceptive practices. *See* Compl. ¶¶22-23.

[15] *See, e.g.*, Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Breach Notification Act of 2011, S.1408, 112th Cong. (2011); Data Security Act of 2011, S.1434, 112th Cong. (2011); Personal Data Protection and Breach Accountability Act of 2011,

Commission the general authority to regulate data security. *Cf. Brown & Williamson*, 529 U.S. at 147. In other words, Congress has ratified the Commission's previous position that it lacks general jurisdiction to regulate data-security practices under Section 5.[16] *See id.* at 156.

If Congress had intended for the Commission's Section 5 "unfairness" authority to include patient-information data-security practices, it could have said so in the Federal Trade Commission Act Amendments of 1994, codified at 15 U.S.C. § 45(n). Instead, due to a long history of Commission abuses, Congress stripped it of the authority "to declare unlawful an act or practice" under Section 5 unless "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *Id.*; *see* Statement by Director of Consumer Protection Howard Beales, *FTC's Use of Unfairness Authority*, *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm (accessed Nov. 3, 2013). Congress also said that public policy concerns are not a primary basis for the exercise of jurisdiction, 15 U.S.C. § 45(n), thereby legislatively overruling prior judicial Section 5 interpretations. *See, e.g.*, *Atl. Ref. Co. v. FTC*, 381 U.S. 357, 369 (1965), *superseded by statute.*

At the time, the Commission did not claim Section 5 "unfairness" authority to regulate patient-information (or any other) data-security practices. But now it has changed its tune and

---

S. 1535, 112th Cong. (2011); Data Accountability and Trust Act, H.R 1707, 112th Cong. (2011); Data Accountability and Trust Act of 2011, H.R 1841, 112th Cong. (2011); SAFE Data Act, H.R. 2577, 112th Cong. (2011).

[16] The Commission's extralegal approach to data-security regulation also violates the core principles espoused in Executive Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013), which directs the Department of Commerce (not the Commission) to identify specific data-security practices through the notice-and-comment process, *see id.* § 7; *see also* Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, at 29 n.33 (Feb. 2012)("[T]he FTC does not currently have authority to enforce Section 5…against certain corporations that operate for profit…."), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

grabs for massive plenary powers over the entire economy. Yet, Section 5 does not and was not intended to give the Commission authority to do this. Congress does not hide massive regulatory schemes in statutory mouseholes. *Whitman v. Am. Trucking Ass'ns., Inc.*, 531 U.S. 457, 468 (2001); *see also Brown & Williamson*, 529 U.S. at 160. This holds true *a fortiori* where, as here, the Commission claims its broad authority from vague general statutory terms in the face of both an amended Section 5 that was designed to rein in the Commission's abuse of its "unfairness" authority and a raft of specific, targeted data-security statutes, including HIPAA and HITECH.

Simple "common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude," *Brown & Williamson*, 529 U.S. at 133, as general regulatory authority over the data-security practices of all private businesses in the United States reinforces the conclusion that the FTC lacks the authority to regulate the acts or practices alleged in the Complaint. As in *Brown & Williamson*, to conclude that Section 5 gives the FTC jurisdiction over data-security requires not only an "extremely strained understanding" of a vague term ("unfairness") in the FTCA, *cf. id.* at 160-61 (discussing FDA's misinterpretation of the word "safety" in the Food, Drug, and Cosmetic Act), "but also ignor[ing] the plain implication of Congress' subsequent…[data-security]-specific legislation," *id.* at 160. There, as here, Congress could not have intended to grant unfettered power to prescribe data-security standards for private companies, a topic of intense debate with immense economic consequences, to the Commission "in so cryptic a fashion." *Id.* at 160.

In *Brown & Williamson* the Supreme Court rejected the FDA's overreaching. *See id.* at 125. There, as here, the agency pestered Congress to pass legislation expanding its authority but Congress instead chose a more targeted, narrowly tailored regulatory scheme. *See id*. at 153-

54, 156, 158 (Congress enacted numerous tobacco-specific statutes incrementally expanding regulatory authority). Thus, *Brown & Williamson* controls and requires rejection of the Commission's claimed Section 5 "unfairness" authority to regulate LabMD's patient-information data-security practices.

C. *ABA v. FTC* Stands For Dismissal.

The case of *ABA v. FTC*, 430 F.3d at 470-71, stands for dismissal.

There, the D.C. Circuit denied the FTC's attempted power-grab to regulate attorneys under the GLBA, ruling that Congress had not directly and plainly granted the Commission the authority to regulate and rejecting the FTC's claim that statutory gap-filling justified a massive expansion of its authority. *See id.* at 470-71. The court said that Congress's decision not to specifically authorize attorney regulation in the GLBA "makes an exceptionally poor fit with the FTC's apparent decision that Congress, after centuries of not doing so, has suddenly decided to regulate the practice of law." *Id*. at 470. It also said that attorney regulation was historically the province of the states and that federal law "'may not be interpreted to reach into areas of State sovereignty unless the language of the federal law compels the intrusion.'" *Id.* at 472 (citation omitted).

ABA's reasoning applies with equal force here. First, there is nothing in Section 5 explicitly authorizing the FTC to directly regulate patient-information data-security practices. Instead, as in *ABA*, the Commission is simply grabbing power to "fill in" what it perceives to be a regulatory gap. But Congress has already filled the patient-information data-security regulatory "gap" through HIPAA and HITECH, and it is not for the FTC to second-guess Congress. The FTC's assault on LabMD is contrary to the administrative structure Congress has constructed for patient-information data-security and entirely illegitimate. *See id.* at 470-71; *see also Brown & Williamson*, 529 U.S. at 160.

Second, Congress has generally left healthcare-provider data-security regulation to the states. This is because regulation of privacy and healthcare is traditionally a matter of local concern.[17] *See* 65 Fed. Reg. at 82,463 ("Rules requiring the protection of health privacy in the United States have been enacted primarily by the states."); *see also Hill v. Colo.*, 530 U.S. 703, 715-18 (2000)(upholding statute protecting patient privacy as valid exercise of state's traditional police power to protect health and public safety); *Hillsborough Cnty. v. Automated Med. Laboratories*, Inc., 471 U.S. 707, 719 (1985)(The "regulation of health and safety matters is primarily, and historically, a matter of local concern."). In those cases where Congress has determined federal regulation of patient-information data-security practices is appropriate, it has explicitly said so. *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1). Because Section 5 does not contain a clear and manifest statement from Congress to authorize the Commission's intrusion into patient-information data-security, its brazen fabrication of authority and grab for power should be rebuffed. *See ABA*, 430 F.3d at 472.

[17] Pub. L. No. 104-191, 110 Stat. 1936, § 264(c)(2) states that HIPAA regulations "shall not supersede a [more robust] contrary provision of State law," consistent with traditional state regulation of public health and welfare. *See Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996); *see also* John R. Christiansen, *Legal Speed Bumps on the Road to Health Information Exchange*, J. HEALTH & LIFE SCI. L., January 2008, at 1, 1 ("Before HIPAA, state privacy and confidentiality laws were almost the exclusive source of information protection requirements. HIPAA still defers to state laws that are more protective of PHI…."); Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies And Laws*, 19 ALB. L. J. SCI. & TECH. 91, 104-105 & n.66 (2009)(noting that "all but six states and the District of Columbia have passed legislation requiring entities, particularly businesses that maintain computerized personal information…, to notify those residents if their personal information has been disclosed through a data breach" and listing statutes).

II. THE COMMISSION HAS FAILED TO GIVE FAIR NOTICE OF WHAT DATA-SECURITY PRACTICES IT BELIEVES SECTION 5 FORBIDS OR REQUIRES THEREBY VIOLATING LABMD'S DUE PROCESS RIGHTS.

The Commission has refused to publish data-security regulations, guidance, or standards explaining what is either forbidden or required by Section 5. Therefore, it has denied LabMD and others similarly situated constitutionally required fair notice, engaged in prohibited *ex post facto* enforcement, and, through this action, violated LabMD's due process rights. *See Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987)(traditional concepts of due process incorporated into administrative law preclude agencies from penalizing private parties for violating rules without first providing adequate notice of their substance); *Trinity Broad. of Fla., Inc. v. FCC*, 211 F.3d 618, 632 (D.C. Cir. 2000)(where the regulations and other policy statements are unclear, where the petitioner's interpretation is reasonable, and where the agency itself struggles to provide a definitive reading of the regulatory requirements, a regulated party is not "on notice" and may not be punished).

A. Due Process Requires Fair *Ex Ante* Warning of Prohibited or Required Conduct.

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). Administrative law has thoroughly incorporated this constitutional fair notice requirement to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. *See Satellite Broad. Co. v. FCC*, 824 F.2d at 3. Where, as here, a party first receives notice of a purportedly proscribed activity through an enforcement action, due process rights are violated. *See, e.g., United States v. Chrysler Corp.*, 158 F.3d 1350, 1355 (D.C. Cir. 1998)(due process requires fair notice of standard before company could be ordered to recall vehicles for alleged noncompliance with standard).

B. The Commission Has Denied LabMD Fair Notice.

The test for constitutionally adequate notice is whether by reviewing the regulations and other public statements issued by the agency, a regulated party acting in good faith would be able to identify, with ascertainable certainty, the standards to which the agency expects parties to conform. *Trinity Broad.*, 211 F.3d at 632. The Commission "has the responsibility to state with ascertainable certainty" what standards third parties must follow. *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986)(citation omitted). It has failed to do so in this case.

The Commission is authorized to prescribe regulations specifically defining unfair acts or practices. 15 U.S.C. § 57a(a)(1). However, Section 5 independently bars the Commission from attempting to enforce consent orders against non-parties. 15 U.S.C. § 45(m)(1)(B). And the APA categorically prohibits federal agencies from creating legislative rules and substantive standards through mechanisms other than formal or notice-and-comment rulemaking. Consequently, the Commission cannot point to any legally-binding data-security standards, and so its attack against LabMD violates the company's due process rights.

1. The Commission has wrongfully failed to provide *ex ante* notice through regulations.

Section 5's general prohibition of "unfair" acts or practices is constitutionally too vague to provide adequate *ex ante* notice of the patient-information data-security practices that it purports to forbid or require. *See Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926)(statute that either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates due process); *Trinity Broad.*, 211 F.3d at 632. Furthermore, the FTC admits that it has not prescribed regulations or legislative rules under Section 5 establishing patient-information (or any other) data-security standards that have the force of law. Trans. 21:11-22:13.

The FTC's refusal to issue regulations is wrongful and makes no sense. It has in the past issued data-security regulations after notice-and-comment rulemaking in a number of areas. For example, 16 C.F.R. Pt. 314 sets forth specific standards under the GLBA "for developing, implementing, and maintaining reasonable" technical safeguards to protect consumer information. *See* 16 C.F.R. § 314.1. Also, 16 C.F.R. Pt. 682 implements the FCRA by articulating specific guidelines regarding the proper destruction of consumer information. *See* 16 C.F.R. § 682.3. Therefore, there is no reason the FTC could not have announced similar *ex ante* rules here, other than the FTC's admission that it prefers the "regulatory flexibility" of employing a vague standard such as "reasonableness." *See* FTC Opposition at 21-22; Trans. 21:11-25. But unchecked discretion is not a virtue of the FTC's current interpretation of its Section 5 "unfairness" authority, and it is for that very reason that such a regime cannot be lawful. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999)(boundless enforcement discretion violates due process); *Connally*, 269 U.S. at 391.

2. <u>The FTC's alleged "standards" are legally meaningless.</u>

The FTC has claimed that its "public statements," "educational materials," and "industry guidance pieces" establish standards and provide LabMD and others similarly situated with notice of the data-security practices they must keep to avoid Section 5 "unfairness" liability. Trans. 9:23-10:3. This claim is untenable for several reasons.

First, general statements of policy are prospective and do not create obligations enforceable against third parties like LabMD. *See Am. Bus. Ass'n. v. United States*, 627 F.2d 525, 529 (D.C. Cir. 1980)("The agency cannot apply or rely upon a general statement of policy as law because a…policy statement announces the agency's tentative intentions for the future." (citation omitted)); *Wilderness Soc'y v. Norton*, 434 F.3d 584, 595-96 (D.C. Cir. 2006)(in holding agency manuals to be nonbinding, the court said that "it is particularly noteworthy that

NPS did not issue its management policies through notice and comment rulemaking under 5 U.S.C. § 553" because failure to do so is evidence that the material in question was not supposed to be a rule binding regulated companies' conduct).

Second, if the FTC truly considers "public statements," "educational materials," and "industry guidance pieces" to be enforceable standards, then it necessarily concedes an APA violation. The APA requires agencies to "publish in the Federal Register for the guidance of the public…substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency…." 5 U.S.C. § 552(a)(1)(D). It further provides that except to the extent "that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published." 5 U.S.C. § 552(a)(1).

Therefore, the Internet postings of "Guides for Business," links to SANS Institute and NIST publications, and similar materials on the Commission's official website do not replace Federal Register publication.[18] The D.C. Circuit has never found that Internet notice is an acceptable substitute for publication in the Federal Register, and has affirmatively refused to do so. *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 754 (D.C. Cir. 2001). Here, the Complaint does not even allege that LabMD had actual notice of any of these sources. Thus, the FTC has breached its statutory duty.[19]

---

[18] Curiously, other Commission "business guides" that have been posted on the Internet have also been published in the Federal Register. *See, e.g.*, Guides for Jewelry, Precious Metals, and Pewter Industries, 16 C.F.R. § 23 (2013), *available at* http://www.ftc.gov/os/2012/06/120622jewelryguidesfrn.pdf.

[19] The FTC claims that NIST publications allegedly setting forth "principles" about what they call the "general approach" of "[d]efense in depth," Trans. 11:18-24, establish ascertainable standards. That claim is contradicted by NIST itself. A NIST publication

Third, the FTC cannot regulate by consent order. *See Gen. Elec. Co. v. EPA*, 290 F.3d 377, 382-83 (D.C. Cir. 2002)(holding that an agency guidance document that imposes binding duties and obligations violates the APA). Consent orders "do not establish illegal conduct," *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001), and are "only binding upon the parties to the agreement," *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008). They do not restrict the FTC's discretion in future actions and therefore do not provide the fair notice that due process requires. *See Morales*, 527 U.S. at 63-64.

Furthermore, Congress specifically barred the Commission from binding third parties by consent order, prohibiting the FTC from enforcing a "consent order" against anyone who is not a party to it.[20] 15 U.S.C. § 45(m)(2); *see Good v. Altria Group, Inc.*, 501 F.3d 29, 53 (1st Cir.

---

addressing the HIPAA Security Rule states: "This publication is intended as general guidance only…*and is not intended to be, nor should it be construed or relied upon as legal advice or guidance to nonfederal entities or persons*. This document does not modify…[]HIPAA[] or any other federal law or regulation." Scholl et al., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Pub. 800-66 Revision 1, at iv (2008)(emphasis added). Another NIST publication regarding computer security that the FTC may cite specifically disclaims any intent to establish standards: "*The purpose of this handbook is not to specify requirements*…." *An Introduction to Computer Security: The NIST Handbook*, NIST Special Pub. 800-12, at 3 (1995)(emphasis added). That argument therefore fails.

The FTC also argues that the SANS Institute establishes data-security standards that LabMD should have complied with. That, too, is wrong. The SANS Institute is merely a "cooperative research and education organization." SANS, About, http://www.sans.org/about/. It does not have the authority to prescribe legislative rules or otherwise establish binding standards. Voluntary industry standards are not law and do not purport to reveal what the Commission (or any other entity) believes Section 5 to require. *See, e.g., Romero v. Buhimschi*, 2007 U.S. Dist. LEXIS 73024, at *11 (E.D. Mich. 2007)(illustrating proposition that voluntary adoption of private standards of conduct does not create legal duty). Private standards cannot provide the fair notice the Commission has refused to give.

[20] The FTC may assert that consent orders in *other* data-security cases establish reasonably ascertainable standards. *See* FTC Opposition at 19. But, as the Commission has admitted, *see id.*, its prior consent orders are not "controlling precedent for later Commission action" and do not in any way limit the Commission's enforcement powers. *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976). Even if Commission consent orders involving data-security practices could provide notice, which they cannot, Commission consent orders made

2007)(The FTCA "specifically provides that the Commission cannot enforce them against non-parties.").

Finally, none of the alleged standards cited by the FTC, whether NIST and SANS Institute publications, the Commission's patchwork-quilt of nonbinding consent orders (most of which, unlike this matter, involved allegations of deception), or general "Guides for Businesses" and "Consumer Alerts" purport to establish specific patient-information data-security standards that businesses "shall" or "must" abide by. Instead, these alleged sources of data-security standards are couched in, at best, precatory language: "may," "best practices," "recommendations," and the like.[21]

---

publicly available for the first time years after LabMD's alleged "security incidents" cannot give LabMD constitutionally adequate *ex ante* warning. *See, e.g.*, FTC, EPN, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 35,387 (June 13, 2012); FTC, Franklin Budget Car Sales, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 35,391 (June 13, 2012).

[21] The FTC may dismiss LabMD's arguments by claiming, as the Commission has elsewhere, that "[LabMD] may argue that it did not know *which* standard it was supposed to follow. This argument misses the point." FTC Opposition at 18 n.5 (emphasis in original). But that is one of LabMD's core points, for "baffling and inconsistent" rules do not give fair notice. *Satellite Broad.*, 824 F.2d at 2-4. Also, the FTC may argue that its Internet postings such as "Protecting Personal Information: A Guide for Business (2007), http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf (hereinafter "PPI Guide"), are enough. *See* FTC Opposition at 18-19. But this "Guide for Business" states that "there's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers." PPI Guide at 23. This is hardly "fair notice" of anything at all.

In 2011, the Commission also posted on the Internet a document entitled "Peer-to-Peer File Sharing: A Guide for Business." But the Complaint's allegations regarding a "P2P file sharing application" occurred in 2008, three years *before* this document was posted on the Internet. Moreover, it does not cite Section 5 or *any* regulations or binding standards. It does not make clear what, if anything, businesses are legally required or prohibited from doing, e.g., "[w]hether you decide to ban P2P file sharing programs on your network or allow them, it's important to create a policy and take the appropriate steps to implement and enforce it…." FTC, *Peer-to-Peer File Sharing: A Guide for Business* 3 (2011), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.pdf. Simply put, this document contains nothing resembling an intelligible, much less enforceable, binding legal standard.

Consequently, the FTC has denied LabMD and others similarly situated the fair notice they are entitled to as a matter of constitutional right. *Gates & Fox Co.*, 790 F.2d at 156.

III. THE ACTS OR PRACTICES ALLEGED IN THE COMPLAINT DO NOT AFFECT INTERSTATE COMMERCE.

FTCA Section 4 defines "commerce" as commerce "among" or "between" states. 15 U.S.C. § 44; *see FTC v. Buntes Bros., Inc.*, 312 U.S. 349, 351-55 (1941). Section 5 allows the Commission to regulate "unfair…acts or practices in or affecting commerce" that have actually caused substantial (usually monetary) harm. 15 U.S.C. § 45(a)(1); *In the Matter of Int'l Harvester,* 104 F.T.C. 949, at 248 (1984)(unfairness cases usually involve "actual and completed harms," often monetary but sometimes health and safety). LabMD's principal place of business, where all of the alleged acts or practices allegedly occurred, is located in Georgia. Compl. ¶1. All of its servers and its computer network are located in Georgia. None of the alleged FTCA violations allegedly occurred outside of Georgia and there are no allegations of monetary loss or other actual harm. Therefore, dismissal with prejudice is appropriate.

IV. THE COMPLAINT DOES NOT COMPLY WITH THE COMMISSION'S PLEADING REQUIREMENTS.

Although the Commission's "unfairness" claim hinges on proving that LabMD's data-security practices were not "industry standard" or "commercially reasonable," the Complaint contains no allegations at all explaining what data-security practices were "standard" in the medical industry between 2008 and 2012, when the alleged "Security Incidents" occurred, or how LabMD's practices fell short of this unspecified benchmark. Further, the addition of technical jargon surrounding the Commission's claim of unreasonableness does not change that the Complaint's allegations are nothing more than inadequate "legal conclusion[s] couched as…factual allegation[s]." *Twombly*, 550 U.S. at 555 (citation omitted).

The FTC does not dispute that LabMD complied with HIPAA and HITECH. Trans. 22:10-13. Moreover, the Complaint fails to allege any actual, completed economic harms or threats to health or safety. Therefore, the Complaint does not state a plausible claim for relief and should thus be dismissed.

V. THIS MATTER SHOULD BE STAYED PENDING DISPOSITION OF THIS MOTION.

Under its Rules of Practice, the Commission has the discretion to stay this matter pending its resolution of this Motion. Rule 3.22(b), 16 C.F.R. § 3.22(b)(Commission authorized to stay proceedings); Rule 3.21(c)(1), 16 C.F.R. § 3.21(c)(1)(Commission may continue evidentiary hearing for good cause); Rule 3.41(b), 16 C.F.R. § 3.41(b)(same). The Commission should exercise its discretion here and grant LabMD's request for a stay pending the resolution of its Motion to Dismiss.

In support of its action against LabMD, the FTC has undertaken extensive and abusive discovery. Notwithstanding years of investigation, multiple CIDs, depositions of LabMD's principals, and the production of thousands of pages of documents, the FTC has served burdensome, repetitive, and oppressive discovery requests that would not be allowed under the Federal Rules of Civil Procedure. For example, in a three-hour period on October 24, 2013, the FTC noticed twenty (20) depositions to be taken in various parts of the country, all of which were initially scheduled at the same time on the same day;[22] served eleven (11) subpoenas duces tecum; and served the FTC's First Set of Requests for Production and Interrogatories.

[22] In recognition of the burden and expense of depositions for private litigants that, unlike large federal agencies, do not have unlimited resources, in federal court, leave of court is (quite sensibly) required if a party wishes to take more than ten depositions. Fed. R. Civ. P. 30(a)(2)(A)(i). For that matter, Complaint Counsel has already deposed one of the named deponents during its investigation of LabMD. In federal court, leave of court would also be required for this, for obvious reasons. Fed. R. Civ. P. 30(a)(2)(A)(ii).

LabMD has moved for a protective order. However, it is clear that the FTC's intentions include the punishment of LabMD and subjecting it to ruinous litigation costs, perhaps to chill others from contesting Commission overreach,[23] and all at taxpayer expense. Forcing LabMD to litigate a case that the Commission does not even have jurisdiction to bring is inherently unjust and violates its due process rights. Therefore, a stay of the administrative proceedings until LabMD's Motion to Dismiss is finally resolved would be appropriate.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion to Dismiss and ORDER that the Complaint be dismissed with prejudice. LabMD further requests that the Commission GRANT its Motion for a Stay of Administrative Proceedings pending the disposition of its Motion to Dismiss.

[23] Notably, the Complaint (along with a FTC press release making disparaging claims about LabMD) was issued shortly before publication of LabMD's CEO's book, *The Devil Inside the Beltway*, in which he exercises his First Amendment right to speak candidly about a matter of public concern and criticizes Complaint Counsels' actions and the Commission's treatment of LabMD in great detail. Complaint Counsels' burdensome and oppressive discovery requests—which run afoul of norms of conduct that obtain in Article III courts and *flagrantly* violate Fed. R. Civ. P. 30(a)(2)(A)'s limits on depositions—followed shortly after the book's publication. The First Amendment prohibits government agencies from retaliating against private citizens for engaging in constitutionally protected speech by bringing baseless enforcement actions. *See Trudeau v. FTC*, 456 F.3d 178, 190-91 nn.22-23 (D.C. Cir. 2006).

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and administrative proceedings before federal agencies.

Dated: November 12, 2013

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE

This matter came before the Commission on November 12, 2013, upon a Motion to Dismiss the Complaint with Prejudice ("Motion") filed by Respondent LabMD, Inc. ("LabMD") pursuant to Commission Rule 3.22(a), 16 C.F.R. §3.22(a), for an Order dismissing the Federal Trade Commission's ("FTC") Complaint with prejudice. Having considered LabMD's Motion and all supporting and opposition papers, and good cause appearing, it is hereby ORDERED that the FTC's Complaint is DISMISSED with prejudice.

ORDERED:

_____
Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Commissioners

Date:

CERTIFICATE OF SERVICE

I hereby certify that on November 12, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I certify that I delivered via first-class mail twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

I also certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: November 12, 2013

By: _____
Michael D. Pepson

EXHIBIT 12

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

RESPONDENT LabMD, INC.'S REPLY TO COMPLAINT COUNSEL'S RESPONSE IN OPPOSITION TO RESPONDENT'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Senior Vice President for Litigation and Counsel to Cause of Action.

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

INTRODUCTION

FTC's Opposition to LabMD's Motion is remarkable in only two respects. First, it demonstrates FTC has discarded rule-of-law and constitutional values for boundless bureaucratic power and discretion. Second, it shows FTC will distort the law and even re-write history to justify its power-grab.

FTC's Opposition's admissions and arguments demonstrate only that FTC lacks Section 5 authority over patient-information data-security, and that its standardless, blame-the-victim *ex post* enforcement tactics violate due process and fail to provide LabMD with constitutionally-adequate fair warning of the data-security standards FTC believes Section 5 forbids or requires.

STANDARD OF REVIEW

FTC does not respond to many arguments made in LabMD's Motion to Dismiss (Mot.). "[F]ailure to respond to an argument…acts as a concession" and thus an admission. *CREW v. Cheney*, 593 F. Supp. 2d 194, 229 (D.D.C. 2009).

FTC admits it must prove Congress intended to delegate it specific authority to regulate patient-information data-security. *La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). FTC also admits the FRCP 12(b)(6) standard controls here under *In re S.C. State. Bd. of Dentistry*, 138 F.T.C. 229, 232 (F.T.C. 2004). *See* FTC Opp. to Mot. (Opp.) 3. Yet FTC claims without citing any controlling (or on-point) authority that the *Iqbal/Twombly* standard for 12(b)(6) motions does not apply. Opp. 25. Because FRCP 12(b)(6) applies here, as FTC admits, *Iqbal*/*Twombly* apply as well. *See Jones v. Horne*, 634 F.3d 588, 595-96 & n.4 (D.C. Cir. 2011)(*Iqbal/Twombly* sets standard for 12(b)(6) motions).

ARGUMENT

I. FTC LACKS SECTION 5 "UNFAIRNESS" AUTHORITY OVER DATA-SECURITY.

A. HIPAA/HITECH Control, And FTC May Not Over-File.

Citing no controlling authority or explicit statutory command, FTC wrongly claims "concurrent" jurisdiction over HIPAA/HITECH patient-information data-security.

FTC admits LabMD is and always has been a HIPAA-covered entity regulated exclusively by HHS under HIPAA/HITECH.[1] It also admits LabMD is specifically exempted from FTC's HITECH rule. *Cf.* Mot. 12 & n.9. It offers no explanation why HITECH, Pub. L. 111-5 §13424(b)(1), directs HHS and FTC to determine *which* agency is best equipped to enforce HITECH against non-HIPAA-covered entities (FTC agrees that HHS exclusively regulates HIPAA-covered entities like LabMD). It also ignores HIPAA's directive to HHS—not FTC—to "adopt [data-]security standards" for "health information." 42 U.S.C. §1320d-2(d)(1); 42 U.S.C. §1320d(4)(defining "health information").

Even if Section 5 covered data-security, HIPAA/HITECH are "precisely drawn, detailed statute[s that] pre-empt" Section 5's "more general remedies." *EC Term of Years Trust v. U.S.*, 550 U.S. 429, 433 (2007). Through HIPAA/HITECH, Congress deliberately targeted specific data-security problems with specific solutions, and these specific statutes govern over whatever "general" Section 5 authority FTC might have. *See RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-72 (2012). Otherwise, HIPAA-covered companies like LabMD lack data-security safe-harbor and certainty, contrary to HHS's regulatory intent.

[1] FTC incorrectly claims LabMD only cites one HITECH provision to support its argument. But LabMD cites multiple HIPAA provisions. Mot. 11-13 & nn.4,9.

See 78 Fed. Reg. 5,566, 5,644 (Jan. 25, 2013)(encouraging covered entities to use encryption safe-harbor); 65 Fed. Reg. 82,462, 82,543 (Dec. 28, 2000)(discussing safe-harbor).

FTC says "Congress's intent to preempt or repeal…FTC's unfairness authority" must be clear-and-manifest. Opp. 6. This distorts the law, for implied repeal may be found even "absent 'a clearly expressed congressional intention'" where, as here, two statutes irreconcilably conflict. *Carcieri v. Salazar*, 555 U.S. 379, 395 (2009).

FTC attempts to avoid *Credit Suisse v. Billing*, 551 U.S. 264 (2007), with the specious argument that the Court explicitly limited the rule there to conflicts between antitrust and securities laws. Opp. 7. But nowhere in *Billing* does it say this.[2] Instead, *Billing* fleshes out the analysis for determining a "clear repugnancy." *Billing* confirms that HIPAA/HITECH irreconcilably conflict with Section 5, and, being more recent and more specific than Section 5, control. *See Billing*, 551 U.S. at 276, 285. Even if the canon against implied repeal is applied here, Section 5 is displaced by HIPAA/HITECH. *See EC Trust*, 550 U.S. at 434-36.

FTC claims that because HITECH was enacted "*after*…[FTC] had brought a half-dozen unfairness cases relating to data security," Congress has blessed its power-grab. Opp. 7 n.4. That, too, distorts the law. Congress's failure to express any opinion is not probative of legislative intent. *Rapanos v. U.S.*, 547 U.S. 715, 749-50 (2006).

Finally, FTC's reliance on *two recent consent orders* in cases also involving allegations of Section 5 "deception" and HIPAA violations is another irrelevant distraction.[3] Here, the question is not whether Section 5 and HIPAA/HITECH authorities might be "complementary"

---

[2] *See* Jesse Markham, *The Supreme Court's New Implied Repeal Doctrine*, 45 GONZ. L. REV. 437,475 (2009)(*Billing* "not limited to…interplay between antitrust law and economic regulation.").

[3] *In re CVS Caremark* "is the first instance in which [HHS] OCR…coordinated …with…FTC." http://www.hhs.gov/news/press/2009pres/02/20090218a.html.

under some circumstances. Instead, it is whether FTC's "unfairness" authority allows FTC to over-file HHS and punish a company FTC admits *complied* with HIPAA/HITECH in all respects. FTC's interpretation of Section 5 wrongly eviscerates Congress's HIPAA/HITECH enactments and HHS's regulatory scheme.

B. FTC Lacks "Unfairness" Authority Over Data-Security.

FTC says its position that "companies *should* engage in 'reasonable' [data-security] practices…is premised on Congress's mandate" in 15 U.S.C. §45(n). Opp. 2 (emphasis added). This claim, yet again, distorts the law. Congress's subsection (n) mandate was to rein in FTC's abuse of its "unfairness" authority by, *inter alia*, prohibiting FTC from using public-policy considerations "as a primary basis for…determin[ing]" that a practice is "unfair." 15 U.S.C. §45(n).

1. Distorted History And Law Cannot Give FTC Data-Security Authority.

FTC distorts the legislative history to serve its power-grab. *See* Opp. 9. It cites "unfair-*competition*" materials from 1914 predating by twenty-four years the 1938 Wheeler-Lea Amendments to the FTC Act, which added "unfair or deceptive acts or practices" to Section 5, and predating by eighty years the 1994 Amendments, which added 15 U.S.C. §45(n). Therefore, FTC's alleged "legislative history" is irrelevant to its Section 5 "unfairness" authority here.[4]

FTC's case authority illustrates only that FTC lacks jurisdiction here. First, none of their cases are legally controlling. FTC admits that no court has ever affirmed its Section 5 authority

[4] FTC cites dicta from *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972), interpreting legislative history from the 1914 pre-Wheeler-Lea Amendments version of Section 5. But Congress was aware of this when it limited FTC's "unfairness" authority in 1994 in 15 U.S.C. §45(n) and overruled FTC's "unfairness" authority claims. *See Miles v. Apex Marine*, 498 U.S. 19, 32 (1990)("Congress…aware of existing law when it passes legislation"). Because *Sperry* was decided over twenty years before §45(n) was enacted, it is irrelevant.

to regulate patient-information or any other data-security. *Cf.* Mot. 1. Second, none of the cases cited are even factually analogous.

Unlike this case, where LabMD's property was taken by a third party without its knowledge or permission, in *FTC v. Neovi*, the defendant affirmatively participated in fraudulent creation and delivery of unverified checks. *See* 604 F.3d 1150, 1155-57 (9th Cir. 2010). Similarly, in *FTC v. Accusearch*, Accusearch was held liable for maintaining a website selling GPS locations of individual cell phones and other confidential, personal information, where every time Accusearch ordered phone records, they caused use of false pretenses and other fraudulent means to obtain this information. *See* 2007 U.S. Dist. LEXIS 74905, at *17-18 (D.Wyo. Sept. 28, 2007).

Unlike this case, where FTC admits LabMD has always complied with all applicable data-security regulations, *cf.* Mot. at 4,8,13, *Orkin Exterminating Co. v. FTC*—decided years *before* 15 U.S.C. §45(n)'s enactment limiting FTC's "unfairness" authority—involved unilateral breaches of unambiguous contracts through which Orkin wrongfully obtained money from consumers. *See* 849 F.2d 1354, 1363-66 (11th Cir. 1988).

Unlike this case, where FTC admits LabMD has not engaged in any deception, *cf.* Mot. 6, in *FTC v. Verity Int'l, Ltd.*, the defendant not only told its customers they were liable for payments for services they did not use or agree to but "misrepresented…services provided." 335 F. Supp. 2d 479, 484 (S.D.N.Y. 2004).

In re Int'l Harvester Co., 104 F.T.C. 949, 1984 FTC LEXIS 2 (1984), is a Commission decision predating Congress's attempt to rein in FTC via 15 U.S.C. §45(n). It is also factually inapposite. The "unfair" trade practice in that case was a deceptive material omission, i.e., the

company's failure to warn its customers about serious safety risks associated with its products. *Int'l Harvester*, 1984 FTC LEXIS at *255-62.

2. Congress's Preference for Sector-Specific Data-Security Statutes Trumps the Commission's Data-Security Power-Grab.

FTC again distorts the law, arguing FCRA, GLBA, and COPPA simply provide new "tools," such as "APA rulemaking authority…." Opp. 10. But Section 5 already gives FTC authority to promulgate rules. 15 U.S.C. §57a(a)(1). It just refuses to do so.

FTC also says LabMD "does not grasp the significance of civil penalties" and that under Section 5 FTC can seek only equitable relief. Opp. 11 (citing 15 U.S.C. §45(b)). Yet Section 5 authorizes civil penalties for cease-and-desist order violations of up to $10,000-per-violation, 15 U.S.C. §45(l), *and* authorizes substantial civil penalties for violations of "rules" respecting unfair acts or practices,[5] 15 U.S.C. §45(m).

Finally, FTC says FCRA, GLBA, and COPPA "enhance" FTC's general data-security authority because it need not prove a likelihood of substantial injury thereunder. Opp. 11. But if FTC actually issued data-security rules, as it is both authorized and constitutionally-required to do if Section 5 covered data-security, *see* 15 U.S.C. §57a(a), it would not need to prove substantial injury, 15 U.S.C. §45(m), and would have the same enforcement powers as it does under FCRA, GLBA, and COPPA, thereby rendering these statutes nullities. However, Congress recognized that FTC has no general Section 5 "unfairness" data-security authority and thus enacted these sector-specific statutes. FTC's "enhancement" argument therefore fails.

[5] Civil penalties under subsections (l) and (m) are *four times* higher than those available under the FCRA, 15 U.S.C. §1681s(a)(2)(A); COPPA incorporates FTC Act penalties, 15 U.S.C. §6505(d); and GLBA is enforced under the FTC Act, 15 U.S.C. §6805(a)(7). Thus, the monetary penalty in *U.S. v. Choicepoint*, No. 06-0198 (N.D.Ga. Feb. 15, 2006), was issued "pursuant to…Section(m)(1)(A) of the FTC Act." Stip. Final Judgment 4. Likewise, the Consent Decree in *U.S. v. Path*, No. 13-0448, ¶18 (N.D.Cal. Feb. 8, 2013), expressly states that the civil penalties are imposed "pursuant to Section 5(m)(1)(A) of the FTC Act…."

C. FTC Disclaimed Authority to Regulate.

Complaint Counsel says "FTC has consistently maintained its ["unfairness" data-security] authority" and that "[a] contrary conclusion requires…tortured application" of a Supreme Court case involving a different agency. Opp. 12. As a matter of fact, this claim straddles the line between distortion and outright deception. As a matter of law, this is breathtakingly wrong.

1. Against the Backdrop of FTC's Admitted Lack of Authority, Congress Enacted Numerous Targeted Data-Security Statutes.

FTC claims that "[s]ince 2000, the FTC has brought nearly fifty data-security cases, more than eighteen of which alleged…unreasonable security is an unfair…practice," citing a string of consent orders. Opp. 12 & n.9. But the *earliest* consent order they cite is dated "Sept. 20, 2005." Opp. 12 n.9. The earliest Commission statements they cite are dated "Mar. 21, 2007" and "Sept. 22, 2004," respectively. Opp. 13 & n.10. Even taking FTC's citations at face value, their world seemingly was created in late 2004.

Furthermore, FTC's out-of-context cherry-picked statement from a footnote in Orson Swindle's testimony must be addressed. *See* Opp. 13 n.10. He never suggested that the Commission has general substantive data-security authority under Section 5, for the very next sentence in footnote 24 states: "[FTC] has used this ["unfairness"] authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing'" and cites two "phishing" cases.

Complaint Counsel does not mention FTC's statement in *Privacy Online: A Report to Congress*, 41 (1998), that FTC generally "lacks authority to require firms to adopt information practice policies," or its statement in *Privacy Online: Fair Information Practices in the Electronic Marketplace*, 34 (2000), that FTC "lacks authority to require firms to adopt

information practice policies or…abide by…fair information practice principles on their Websites" not directed to children. *Cf.* Mot. 16 n.12. They do not deny that Chairman Pitofsky told Congress the FTC's data-security authority is "limited…to ensuring…Websites follow their stated information practices." Mot. 16 n.12. They offer no response to a FTC official's 2001 statement that "'[t]he agency's jurisdiction is (over) deception….If a practice isn't deceptive,…[FTC] can't prohibit…collecting information." Mot. 16 n.12. They also concede that even FTC's 2008 Resolution did not claim authority to regulate data-security under a pure "unfairness" theory. *Cf.* Mot. 17 n.14.

FTC admits it pestered Congress to confer data-security authority, Opp. 14; *cf.* Mot. 15-16 nn.12-15, but argues that "FTC's requests for additional [data-security] authority showcase…FTC's unfairness authority," Opp. 13. This non-sequitur fails. Asking Congress for the authority to regulate data-security "showcases" only that FTC lacked this authority, for there would be no need to ask for power FTC already had.

FTC's recent statements claiming general Section 5 "unfairness" data-security authority cannot erase FTC's many prior statements disavowing Section 5 data-security jurisdiction or cloud the fact that Congress enacted many targeted data-security statutes against that backdrop.

FTC's reliance on *Smiley v. Citibank*, 517 U.S. 735 (1996), fails. First, here FTC's newfound Section 5 authority is a "[s]udden and unexplained change…." *Id.* at 742. Second, *Smiley* involved an agency regulation entitled to *Chevron* deference. *See id.* at 740-41. No deference is owed to FTC here, because it has not engaged in formal adjudication or rulemaking. *U.S. v. Mead Corp.*, 533 U.S. 218, 227 (2001).

2. Rejected Legislation Confirms FTC Lacks Authority.

FTC says "savings clauses" in four of *ten* or more bills Congress has rejected that would have given FTC general data-security authority supports its claimed authority. Opp. 14. This is bizarre.

First, all four cited bills were proposed in 2011, Opp. 14, *after* Congress had given FTC sector-specific data-security authority through GLBA, FRCA, and COPPA, Mot. 14 & n.10. Of course, these "[p]reservation clauses would be unnecessary if…FTC lacked existing authority," Opp. 14, under GLBA, FCRA, COPPA, and other targeted statutes. But the "savings clauses" are general, do not refer to Section 5, and protect FTC's data-security authority under these other statutes. *See* S. 1207, §6(d)(protecting "Commission's authority under any other provision of law"); H.R. 2577, §6(d)(same); H.R. 1841, §6(d)(same); H.R. 1707, §6(d)(same). None of these bills address, much less endorse, FTC's claimed Section 5 authority.[6] Indeed, H.R. 2577, §4(d)(1), would have *exempted* HIPAA-covered entities like LabMD from compliance.

Second, FTC ignores *six other* 2011 cybersecurity bills that included no language "preserving" FTC data-security authority. *See* S. 1151, S. 1408, S. 1434, S. 1535, S. 2105, H.R. 624.

D. *Massachusetts v. EPA* Supports LabMD's Arguments.

FTC's reliance on *Massachusetts v. EPA*, 549 U.S. 497 (2007), is misplaced. Unlike Section 5, the Clean Air Act unambiguously defined "air pollutant" to embrace "all airborne compounds of whatever stripe…." *Id.* at 528-29. Moreover, the Court noted two "critical" considerations absent from that case but present in *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), and present here. *See Massachusetts*, 549 U.S. at 530-31. First, Section 5

[6] A single Senator's remark during a hearing has no weight, even if it did support FTC.

data-security jurisdiction for the *entire private economy* is not only "counterintuitive" but leads to "extreme measures," because it would require *substantive* data-security standards for the entire economy to be classified as "unfair" practices and eviscerate Congress's longstanding, deliberate policy of regulating data-security through narrow, targeted statutes. *Cf. id*.

Second, like *Brown & Williamson*, there is "an unbroken series of congressional enactments that ma[k]e sense only if adopted 'against the backdrop of…[FTC's] consistent and repeated statements that it lacked authority'" to regulate data-security. *Cf. id.* For FTC to prevail, Congress's many specific, narrow delegations of data-security regulatory authority enacted against the backdrop of FTC's repeated disavowal of general regulatory authority must be deemed superfluous nullities.[7] Furthermore, unlike *Massachusetts*, many of these statutes, including HIPAA/HITECH, directly conflict with FTC's claimed authority.

E. *ABA v. FTC* Illustrates Why Dismissal Is Required.

FTC dismisses *ABA v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), claiming "there is no debate about the meaning of the term 'unfairness.'" Opp. 16 (citing 15 U.S.C. §45(n)). Given that the one court that actually considered FTC's claimed Section 5 authority to regulate patient-information data-security said "there is significant merit" to LabMD's argument against FTC's power-grab, *see* Mot. 1, and 15 U.S.C. §45(n) does not define "unfairness" but rather cabins FTC's authority,[8] that argument fails.

In truth, FTC concedes that nothing in Section 5 explicitly authorizes it to regulate patient-information data-security practices. Instead, as in *ABA*, FTC is simply grabbing power to "fill in" what it perceives as a regulatory gap. But Congress has already filled that "gap" through

---

[7] *See* Mot. 11-16 & nn.10-11 (listing and discussing specific statutes).

[8] Statutory language always trumps section titles. *R.R. Trainmen v. Balt.&Ohio R.R.*, 331 U.S. 519, 529 (1947).

HIPAA/HITECH, and FTC cannot second-guess Congress. FTC's assault on LabMD is contrary to the administrative structure Congress has constructed for patient-information data-security and entirely illegitimate. *See ABA*, 430 F.3d at 469-71.

Furthermore, FTC concedes Congress has generally left patient-information data-security to the states, and where Congress has found federal regulation of patient-information data-security practices appropriate, it has explicitly said so. *Cf.* Mot. 21; 42 U.S.C. §1320d-2(d)(1). Because Section 5 does not clearly authorize FTC's conduct here, its brazen power-grab must be denied. *See ABA*, 430 F.3d at 472.

II. FTC'S LACK OF STANDARDS VIOLATES DUE PROCESS.

A. FTC's Admitted Lack of Standards.

FTC admits LabMD has not violated any data-security statutes, rules, or regulations and concedes LabMD has not engaged in a "deceptive" trade practice. *Cf.* Mot. 6,8. It admits LabMD's data-security practices are regulated under HIPAA/HITECH and that HHS exclusively implements and enforces these statutes as applied to LabMD. *Cf.* Mot. 4,13. FTC's sole claim against LabMD is unspecified "unfair" acts or practices. *Cf.* Mot. 7-8.

FTC also admits that Section 5 statutorily bars FTC from enforcing consent orders against non-parties and that its consent orders do not establish illegal conduct and only bind the parties thereto. *Cf.* Mot. 23,26. It has not alleged LabMD had actual notice of the business guides, consumer alerts, links to Sans Institute/NIST publications, and other Internet postings. *Cf.* Mot. 24-28 & nn.19-21. It admits that none of these materials were published in the Federal Register and that *none* of their alleged sources of data-security standards create *any* legally binding duties and obligations. *Cf.* Mot. 7-8. Instead, FTC says Section 5 alone provides

constitutionally and statutorily adequate *ex ante* notice of what data-security practices are forbidden or required. Opp. 16-17.

B. Section 5 Does Not Establish Proper Standards.

FTC does not acknowledge, much less address, the authorities cited by LabMD holding that FTC was required to provide fair notice of prohibited or required conduct. FTC has never alleged that LabMD's patient-information data-security practices did not meet objective medical-industry standards in effect and applicable to businesses of its size and nature at the time of the alleged violation. *Cf. S&H Riggers & Erectors v. OSHRC*, 659 F.2d 1273, 1280-83 (5th Cir. 1981)(reasonable-person standard divorced from industry standards or regulations violates due process). Instead, FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations. *Cf.* Mot. 4,8,13.

No case has ever held, and no plausible argument can be made, that Section 5 provides constitutionally-adequate data-security fair notice. *See* Stegmaier & Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 706 (2013)("[S]tatutory language does not provide notice of required data-security safeguards."). Section 5's broad "unfairness" prohibition, which does not even refer to "data security," let alone prescribe or proscribe data-security practices, is far more offensive than the statutes at issue in cases like *Connally v. General Constr. Co.*, 269 U.S. 385 (1926)(cited by LabMD but ignored by FTC) finding fair-notice due-process violations. And even if data-security "reasonableness" standards could provide regulated entities with constitutionally-adequate notice if codified in a regulation or statute, FTC says it has not done so and will not do so.

To claim fair notice, FTC again distorts the law. It cites *U.S. v. Merrill*, 513 F.3d 1293, 1306 (11th Cir. 2008), but this is not a fair-notice case. The cherry-picked portion of *Merrill* it cites discusses *a jury instruction*, not statutory fair notice. Opp. 18. Unlike Section 5, the *Merrill* statute (Controlled Substance Act, 21 U.S.C. §841) is quite detailed and hence provides fair notice.

FTC claims OSHA's General Duty Clause is the best analogy to their standardless *ex post* data-security regime. Opp. 19 n.12. It is a poor fit. Cases interpreting OSHA's General Duty Clause prove LabMD's point and confirm why FTC's actions violate due process, particularly because FTC admits LabMD has always complied with HIPAA/HITECH's specific data-security requirements.

The General Duty Clause is a regulatory tool of last resort—a stop-gap—which "was not meant…[as] 'a general substitute for reliance on standards'" and only applies to "'special circumstances for which no standard has yet been adopted.'" *Ramsey Winch v. Henry*, 555 F.3d 1199, 1205 (10th Cir. 2009). It only controls where there are no other standards, because "standards preempt the [G]eneral [D]uty [C]lause…." *In re Samsonite Corp.*, 756 F. Supp. 498, 500 (D.Colo. 1991). FTC claims that even though LabMD has always complied with HIPAA/HITECH *data-security standards*, it remains liable under Section 5 for compliance with FTC's unstated data-security standards. This is the antithesis of how the General Duty Clause works.[9] *See Teal v. E. I. du Pont*, 728 F.2d 799, 804 (6th Cir. 1984)(Congress "enacted…general duty clause to cover serious hazards…not otherwise covered by specific regulations.").

---

[9] *See* OSHA's Field Operations Manual, CPL02-00-148, pp.4-14-4-30 (2009)(detailed elements of General-Duty-Clause violation and strict limits). Unlike Section 5, there are 30-plus years of concrete agency guidelines specifying General-Duty-Clause-imposed obligations. *E.g.*, *ConAgra, Inc.*, 1983-84 O.S.H. Dec. (CCH) ¶26,420, 33,523 (1983)(formal agency interpretation).

The "objective" industry-specific reasonableness standard at issue in *Voegle v. OSHA*, 625 F.2d 1075 (3d Cir. 1980), is fundamentally different from what FTC is doing here. *Voegle* involved a fair-notice challenge to a construction-industry-specific *regulation* (not the General Duty Clause), *see id.* at 1077, far more specific than Section 5's text. Furthermore, *numerous* agency enforcement actions applying occupational-safety regulations far more specific than Section 5 have been dismissed on fair-notice grounds. *E.g.*, *Fabi Const. Co. v. SOL*, 508 F.3d 1077, 1088 (D.C. Cir. 2007); *Gates & Fox v. OSHRC*, 790 F.2d 154,156-57 (D.C. Cir. 1986).

FTC enforcement actions are fundamentally different from garden-variety tort suits, and common-law negligence cases do not displace the APA's and Fifth Amendment's due-process fair-notice requirements. *See Satellite Broadcasting v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987). Also, given FTC admits LabMD has not engaged in "deception," *cf.* Mot. 4, their reliance on dicta from *In re Zappos.com*, No. 12-00325, 2013 U.S. Dist. LEXIS 128155 (D.Nev. 2013), is badly misplaced, for they omit mention of the court's decision to treat the data-security claims as "negligent misrepresentation claims" based on false website statements,[10] *id.* at *15-16.

FTC v. National Urological Group (NUG), 645 F. Supp. 2d 1167 (N.D.Ga. 2008), also deals with "deceptive" advertising allegations not at issue here. FTC itself has explained why "deception" actions do not raise the same fair-notice concerns as "unfairness" actions: "[U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset." *Int'l Harvester*, 1984 FTC LEXIS at *246. Further, the *NUG* court found it critical that, unlike here, FTC had at least expressly defined "competent and reliable scientific evidence" (this definition is omitted from FTC's block-quote) and articulated a definite

[10] *Loschiavo v. City of Dearborn* (overruled) is also not a fair-notice case; inapposite dicta FTC cites refers to the test for whether a private-right-of-action-against-the-government exists under Section 1983. *See* 33 F.3d 548, 551 (6th Cir. 1994).

standard. *See* 645 F.Supp.2d at 1186. That standard is exponentially more detailed than FTC's proposed "reasonableness" standard here.

Unlike FTC's nebulous, standardless concept of data-security "unfairness," "deception" has a well-established, clear meaning in Section 5 and elsewhere in the law and does not raise the same fair-notice concerns. *E.g.*, FTC Policy Statement on Deception, appended to *Cliffdale Assoc., Inc.*, 103 F.T.C. 110, 174 (1984)(*detailed* explication of deception elements). Thus, "deception" cases cited by FTC do not support its fair-notice argument.

Tellingly, FTC's discussion of the "reasonableness" analysis they believe Section 5 requires contains no citations whatsoever and appears to be cut from whole cloth—the only citation on the page is *In re Zappos.com*, addressed above. Opp. 21.

FTC dismissively argues that "ascertainable certainty does not require agencies to provide…guidance at the level of detail…[LabMD] seems to think appropriate." Opp. 20. They brazenly admit that neither the Complaint nor the notice order prescribe *any* specific data-security practices LabMD *should* (let alone must) implement going forward. *Cf.* Mot. 8. Elsewhere, FTC has boldly stated that the argument that a regulated entity "did not know which standard it was supposed to follow…misses the point." Mot. 27 n.21. They blithely explain that they "do[] not endorse any [industry] standards"—"[they] don't say…how you should set up your router…[they] don't say you should have…white…and black lists for IP addresses"—because "[they] are not tech support." Hearing Transcript, *FTC v. Wyndham*, 53:2-10 (Nov. 7, 2012).

The cases they cite—like the cases LabMD cites to which they do not bother to respond, *see* Mot. 22-28 & nn.19-21—make clear that this violates due process. For example, *U.S. v. Lachman*, 387 F.3d 42 (1st Cir. 2004), which, unlike here, involved a detailed technical

regulation and interpreted the phrase "specially designed," *id.* at 50-53, notes that the line of D.C. Circuit cases LabMD cites (and FTC ignores) invalidate agency *ex post* enforcement actions where, as here, the statute "is so ambiguous that a regulated party cannot be expected to arrive at the correct interpretation using standard [interpretive] tools…, must therefore look to the agency for guidance, and the agency failed to articulate its interpretation before imposing a penalty," *id.* at 57. Indeed, even FTC's patchwork-quilt of consent orders is inconsistent. *See* Stegmaier & Bartnick, *supra*, at 700 ("FTC has not explained why data-security practices in one [fact-specific consent-order] case may violate Section 5 while those same practices may not violate Section 5 in another case…apparently expect[ing] entities to piece together…complaints and consent orders in thirty-six cases, without any authoritative commentary, to arrive at…[FTC's] interpretation of adequate data-security practices….").

Finally, again without responding to LabMD's arguments and thereby conceding the points, *cf.* Mot. 25-26 & n.19, FTC—incredibly—suggests that NIST and HIPAA publications supply standards LabMD should have followed. Opp. 22 n.15. The NIST Handbook they cite is from 1995, does "not…specify requirements," and only "provides a broad overview of computer security." NIST, Special Publication, 800-12, §1.1 (1995). Section 1.1 of NIST Special Publication 800-30 states: "The guidelines herein are not mandatory and binding standards." With respect to HIPAA Guidance they cite, even if LabMD was required to follow it, FTC has admitted that LabMD *has always complied with all data-security obligations under HIPAA/HITECH.*

C. FTC Cannot Announce New Rules Through Adjudication Punishing Past Conduct.

The fact that, subject to fair notice, FTC may fill in Section 5's interstices through adjudication does not allow FTC to deliberately evade its constitutional and statutory fair-notice

obligations. FTC cannot regulate through intimidation by bullying companies into signing consent decrees. Yet FTC brags about the myriad consent decrees secured from 2005 to present, Opp. 12-13 n.9, and says they are "not obligated to engage in a rulemaking…," Opp. 23. *SEC v. Chenery*, 332 U.S. 194 (1947), where, unlike here, the agency "had not previously been confronted with the problem," *id.* at 203, explains that "[t]he function of filling in…[statutory] interstices…should be performed, as much as possible, through…quasi-legislative promulgation of rules to be applied in the future," *id.* at 202. *Chenery* is not a fair-notice case; unlike here, SEC did not seek liability for past conduct, *see id.* at 203-04. *PBW Stock Exch. v. SEC*, 485 F.2d 718 (3d Cir. 1973), also not a fair-notice case, involved *a challenged regulation*, not adjudication, *id.* at 721; dicta FTC cites is inapposite.

In *Beazer v. EPA*, 963 F.2d 603 (3d Cir. 1992), EPA had actually promulgated regulations through normal notice-and-comment rulemaking and the statute and regulations prescribed detailed requirements, *see id.* at 604-05. In that context, the court found adjudication permissible. *Cf. id.* at 609 (APA "expressly prohibit[s]…agency from retroactively imposing…interpretive rule upon…regulated party."). Unlike *Beazer*, here FTC brazenly admits that they do not have legislative or even interpretive rules explaining what data-security practices they believe Section 5 forbids or requires. *Cf. id.* at 606.

NLRB v. Bell Aerospace, 416 U.S. 267 (1974), is not a fair-notice due-process case and thus inapposite. Rather, the issue was Bell Aerospace's *future* collective-bargaining obligations. *See id.* at 269. Even in that very different context, the Court recognized situations where NLRB reliance on adjudication would be unlawful, noting that "this is not a case in which some new liability is sought to be imposed…for past actions" and that "fines or damages" were not involved. *Id.* at 294-95. Due-process-based fair-notice requirements are heightened where, as

here, the agency alleges violation of law based on *past* conduct. *See PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51-52 (D.C. Cir. 2000).

III. FTC'S FAILURE TO STATE PLAUSIBLE SECTION 5 VIOLATION.

FTC concedes it lacks even *one* complaining witness who has suffered *any* injuries because of LabMD's alleged patient-information data-security failures. FTC admits LabMD complied with HIPAA/HITECH—the only applicable patient-information data-security requirements. FTC does not allege what the objective medical-industry-standard data-security practices are or were or that LabMD's data-security practices fell short of meeting them. As explained above, the *Iqbal/Twombly* standard applies here. The Complaint fails to meet that standard and must be dismissed.

IV. STAY NECESSARY TO STOP DISCOVERY ABUSE.

FTC does not deny that its discovery tactics are barred in federal courts and does not substantively respond to LabMD's arguments or deny LabMD's assertions. At minimum, the Commission should stay the proceedings.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion in full.

PUBLIC

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Senior Vice President for Litigation and
Counsel to Cause of Action

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and
administrative proceedings before federal agencies.

Dated: December 2, 2013

PUBLIC

CERTIFICATE OF SERVICE

I hereby certify that on December 2, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I certify that I delivered via first-class mail twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

I also certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: December 2, 2013 By: /s/ Michael D. Pepson

EXHIBIT 13

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

ORDER DENYING RESPONDENT LABMD'S MOTIONS FOR STAY

In two separate motions, Respondent LabMD, Inc. ("LabMD") has requested that the Commission stay the ongoing proceeding before the Administrative Law Judge in this case. First, as part of its Motion to Dismiss with Prejudice and to Stay Administrative Proceedings, filed on November 12, 2013 ("Motion to Dismiss"), LabMD requested a stay pending our resolution of the merits of that motion. *See* Motion to Dismiss at 29-30. Second, on November 26, 2013, LabMD filed a Motion to Stay Proceedings Pending Review in the U.S. Court of Appeals for the Eleventh Circuit and the U.S. District Court for the District of Columbia ("Motion for Stay Pending Judicial Review").

For the reasons set forth below, we deny both the stay request incorporated into LabMD's Motion to Dismiss and LabMD's Motion for Stay Pending Judicial Review. In this Order, we do not address the merits of LabMD's Motion to Dismiss.

BACKGROUND

This case concerns allegations that LabMD – a provider of clinical laboratory testing services – failed to implement reasonable and appropriate measures to prevent unauthorized access to consumers' personal data stored on its computer systems. The Complaint initiating this case, issued on August 28, 2013 ("Complaint"), alleges that, as a result of LabMD's inadequate data security practices, identity thieves were able to obtain access to highly sensitive information – including patients' names combined with their dates of birth, social security numbers ("SSNs"), and information about their bank accounts, insurance coverage, or lab test results. *See* Complaint at 2-5 (¶¶ 6-21). The Complaint alleges that LabMD's conduct constituted an "unfair act or practice," in violation of Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a). *See* Complaint at 5 (¶¶ 22-23).

LabMD filed its Answer to the Complaint on September 17, 2013 ("Answer"), and as noted above, filed a Motion to Dismiss on November 12, 2013. Complaint Counsel filed a

Response in Opposition to the Motion to Dismiss ("CC Opp. to MTD") on November 22, 2013; and LabMD filed a Reply on December 2, 2013. The deadline for a Commission order resolving the merits of LabMD's Motion to Dismiss is January 16, 2014. *See* 16 C.F.R. §§ 3.22(a), 4.3(a). Factual discovery in this proceeding is scheduled to close on March 5, 2014, and the evidentiary hearing before the Administrative Law Judge is scheduled to begin on May 20, 2014. *See* Administrative Law Judge's Revised Scheduling Order (issued Oct. 22, 2013).

On November 14, 2013, LabMD filed a Verified Complaint for Declaratory Relief against the Commission in the U.S. District Court for the District of Columbia (docketed as Case No. 1:13-cv-01787-CKK) ("District Court Complaint"). On November 18, 2013, LabMD filed a "Petition for Review of Unlawful Federal Trade Commission Attempt to Regulate Patient-Information" in the U.S. Court of Appeals for the Eleventh Circuit (docketed as Case No. 13-15267) ("11th Circuit Petition"). On November 26, 2013, LabMD filed its Motion for Stay Pending Judicial Review in this proceeding. Complaint Counsel filed an Opposition to the latter motion on December 5, 2013. ("CC Opp. to MSPJR").

ANALYSIS

I. Request for Stay Pending a Decision on the Merits of LabMD's Motion to Dismiss

Our rules provide that, as a general matter, a motion to dismiss filed prior to evidentiary hearings is to be referred directly to the Commission for decision, 16 C.F.R. § 3.22(a), and the fact that such a motion is pending "shall not stay proceedings before the Administrative Law Judge unless the Commission so orders." *Id.* § 3.22(b). When we most recently revised this rule, we stated that that the "purpose of . . . paragraph (b) is to ensure that discovery and other prehearing proceedings continue while the Commission deliberates over the dispositive motions, . . . [so as] to expedite the proceedings." FTC, *Rules of Practice*, Interim Final Rules with Request for Comment, 74 Fed. Reg. 1804, 1809, 1810 (Jan. 13, 2009).

In deciding whether to grant LabMD's request for a stay of the proceeding pending our resolution of its Motion to Dismiss, we exercise our discretion to oversee this adjudication, comparable to the broad discretion of a court "to stay proceedings[,] . . . incidental to the power inherent in every court to control the disposition of the [cases] on its docket with economy of time and effort for itself, for counsel, and for litigants. How this can best be done calls for an exercise of judgment." *Landis v. North Am. Co.*, 299 U.S. 248, 254 (1936). We conclude that there is no good cause for the stay LabMD requests.

LabMD contends that a stay pending resolution of the merits of its Motion to Dismiss is justified, in part, because Complaint Counsel has sought "extensive and abusive discovery" that would impose "ruinous litigation costs" on the company. Motion to Dismiss at 29, 30. Complaint Counsel responds that this argument is no more than a "rehash" of arguments over third-party discovery that are already pending before the Administrative Law Judge. CC Opp. to MTD at 26. Significantly, the Administrative Law Judge recently issued an order resolving pending discovery disputes. *See* Administrative Law Judge's Order on Respondent's Motion for a Protective Order at 7-8 (issued Nov. 22, 2013). By precluding discovery on conduct prior to 2005 and discovery of materials relating to a book by LabMD's CEO, this Order may ameliorate

LabMD's burdens and costs to some extent. If further disputes between LabMD and Complaint Counsel emerge during the course of the discovery process, the Administrative Law Judge is well equipped to address them in the first instance.

LabMD further argues that a stay pending resolution of the Motion to Dismiss would be proper because "[f]orcing LabMD to litigate a case that the Commission does not even have jurisdiction to bring is inherently unjust and violates its due process rights." Motion to Dismiss at 30. Without expressing any view on the merits of the Motion to Dismiss, we conclude that the fact that LabMD has challenged the Commission's authority to bring this case does not justify a stay. As discussed above, when we adopted the current version of Section 3.22 of our Rules of Practice, we anticipated that parties might file dispositive pre-hearing motions, but concluded that the public interest in expediting our adjudicatory process supports allowing the proceedings before the Administrative Law Judge to continue notwithstanding the pendency of such motions. Thus, in past adjudications, we have declined to grant motions for stay of pretrial proceedings pending resolution of motions to dismiss.[1] Consistently, reviewing courts have held that litigants must participate fully in the Commission's adjudications even where they "have challenged the very authority of the agency to conduct proceedings against them." *Ticor Title Ins. Co. v. FTC*, 814 F.2d 731, 739 (D.C. Cir. 1987) (opinion of Edwards, J.). The Supreme Court has clearly ruled that the "expense and disruption [incurred by the respondent in] defending itself in protracted adjudicatory proceedings" before the Commission do not justify halting those proceedings prior to their conclusion, even where, as here, the respondent "alleged unlawfulness in the issuance of the complaint." *FTC v. Standard Oil Co. of Cal.*, 449 U.S. 232, 244 (1980).

II. <u>Motion for Stay Pending Judicial Review</u>

Under our rules, "[t]he pendency of a collateral federal court action that relates to the administrative adjudication shall not stay the proceeding unless a court of competent jurisdiction, or the Commission for good cause, so directs." 16 C.F.R. § 3.41(f). The stay of administrative proceedings pending judicial review sought by LabMD, like stays of trial court proceedings pending appellate review in federal court, would be "an intrusion into the ordinary processes of administration and judicial review." *Nken v. Holder*, 556 U.S. 418, 427 (2009) (quoting *Virginia Petroleum Jobbers Ass'n v. FPC*, 259 F.2d 921, 925 (D.C. Cir. 1958)). Thus, a party requesting a stay in an administrative adjudication – as in federal court – bears the burden of demonstrating that the applicable criteria are fully satisfied.[2] "The first two factors of the traditional standard" – likelihood of success and irreparable injury – "are the most critical." *Id.* at 434.

---

[1] *See, e.g., N.C. State Bd. of Dental Exam'rs*, 150 F.T.C. 851 (2010). The U.S. District Court denied the same respondent's motion to halt the same pending proceeding. *See N.C. State Bd. of Dental Exam'rs v. FTC*, 768 F. Supp. 2d 818, 820 n.1 (E.D.N.C. 2011).

[2] Our procedural decisions in administrative adjudications are governed by the FTC Act and our own Rules of Practice, rather than the rules and standards that govern federal courts. The same factors, however, apply to motions for stay pending appeal in both types of fora. *Compare* 16 C.F.R. § 3.56(c) (factors governing stay motions under 15 U.S.C. § 45(g)(2) and 16 C.F.R. § 3.56(a)), *with Hilton v. Braunskill*, 481 U.S. 770, 776 (1987) (factors under Fed. R. Civ. P. 62(c) and Fed. R. App. P. 8(a)). These factors are: "[1] the likelihood of the applicant's success on appeal; [2] whether the applicant will suffer irreparable harm if a stay is not granted; [3] the degree of injury to other parties if a stay is

Applying this analytical framework, we conclude LabMD has failed to satisfy its burden of showing "good cause" to grant its Motion for Stay Pending Judicial Review.[3]

A. Likelihood of Success on the Merits

A party seeking a stay must "make a strong showing that [it] is likely to succeed on the merits . . . . [M]ore than a mere 'possibility' of relief is required." *Nken*, 556 U.S. at 434. LabMD has not shown that it is likely to prevail on the merits before the District Court or the Eleventh Circuit. We reach this conclusion without addressing the substantive merits of LabMD's District Court Complaint or 11th Circuit Petition – both of which present issues that substantially overlap the substantive issues LabMD raised in its Motion to Dismiss pending before us, which we are not considering or addressing in this Order. Nonetheless, we conclude that neither the District Court nor the Eleventh Circuit is likely to grant LabMD's request for declaratory or injunctive relief to halt this adjudication.

First, neither the District Court nor the Court of Appeals has jurisdiction to entertain LabMD's premature challenge to this adjudicatory proceeding. The FTC Act sets forth a detailed judicial review scheme that makes clear that a respondent in a Section 5 adjudication may obtain judicial review *only* if it (1) identifies "an order of the Commission" requiring it "to cease and desist from using any method of competition or act or practice;" (2) files "a written petition praying that the order of the Commission be set aside" with one of a specified set of U.S. Courts of Appeals; and (3) does so "within sixty days of the service of such order." 15 U.S.C. § 45(c). The Act also makes clear that this judicial review process implicates the courts' jurisdiction. *See id.* (filing of such petition triggers the court's "jurisdiction"); *id.*, § 45(d) ("[T]he jurisdiction of the [C]ourt of [A]ppeals of the United States to affirm, enforce, modify, or set aside orders of the Commission shall be exclusive."). Statutory requirements specifying which courts may review which types of agency decisions – such as provisions limiting judicial review to agency rulings that "are 'final' and 'made after a hearing'" – are deemed "central to the requisite grant of subject-matter jurisdiction." *Weinberger v. Salfi*, 422 U.S. 749, 764 (1975). Where, as here, it is "fairly discernible" from the text and overall structure of a statute that Congress intended that appeals of agency actions "proceed exclusively through the statutory review scheme," then that statute "precludes . . . courts from exercising jurisdiction over [a] pre-enforcement challenge" outside the prescribed procedures, and does not allow parties to "evade the statutory-review process by enjoining the [agency] from commencing enforcement proceedings, as petitioner sought to do here." *Thunder Basin Coal Co. v. Reich*, 510 U.S. 200, 216 (1994); *accord Elgin v. Dept. of Treasury*, 132 S. Ct. 2126, 2132-33 (2012).

---

granted; and [4] whether the stay is in the public interest." 16 C.F.R. § 3.56(c). *See also N.C. State Bd. of Dental Exam'rs*, 151 F.T.C. 640 (2011) (denying respondent's motion for stay pending district court review).

[3] LabMD's request that the Commission rule on this motion by December 5, 2013 – a day before the due date for Complaint Counsel's response – is now moot. *See* Motion for Stay Pending Judicial Review at 8; 16 C.F.R. § 3.22(d).

Both LabMD's District Court Complaint and its 11th Circuit Petition fail this test. "The District Court is without jurisdiction to enjoin hearings because the power 'to prevent any person from engaging in any unfair practice affecting commerce' has been vested by Congress in the [agency] and in the Circuit Court of Appeals . . . ." *Myers v. Bethlehem Shipbuilding Co.*, 303 U.S. 41, 48 (1938).[4] And the Court of Appeals is authorized by the FTC Act to review only an "order of the Commission to cease and desist from using any method of competition or act or practice." 15 U.S.C. § 45(c). *See Texaco, Inc. v. FTC*, 301 F.2d 662, 662 (5th Cir. 1962) (per curiam) ("The jurisdiction of this Court to review an order of the Federal Trade Commission is found in 15 U.S.C. § 45(c). Such jurisdiction arises only from a cease and desist order entered by the Commission."). The Commission has issued no cease and desist order in this proceeding.

LabMD's attempt to short-circuit this adjudicatory proceeding by going straight to court is "at war with the long-settled rule of judicial administration that no one is entitled to judicial relief for a supposed or threatened injury until the prescribed administrative remedy has been exhausted[,] . . . . [even] in cases where, as here, the contention is made that the administrative body lacked power over the subject matter." *Bethlehem Shipbuilding Corp.*, 303 U.S. at 50-51. *See also Ewing v. Mytinger & Casselberry, Inc.*, 339 U.S. 594, 599 (1950) ("it has never been held that the hand of government must be stayed until the courts have an opportunity to determine whether the government is justified" in instituting such proceedings). The law is clear that a party may not halt a legitimate law enforcement proceeding that a federal agency is conducting against that party by seeking an injunction or declaratory order, provided that the party has a meaningful opportunity to obtain judicial review after the proceeding concludes and a final order is issued. *See, e.g.*, *FTC v. Claire Furnace Co.*, 274 U.S. 160, 174 (1927) (where respondents have a "full opportunity to contest the legality of any . . . proceeding against them[,] . . . they [could] not . . . ask relief by injunction"); *cf. Thunder Basin Coal Co. v. Reich*, 510 U.S. at 212-13 (distinguishing *Leedom v. Kyne*, 358 U.S. 184 (1958) and its progeny).

Moreover, LabMD has no probability of success on the merits before either the District Court or the Eleventh Circuit because there is no "final agency action" in this proceeding. The Commission has merely averred "reason to believe" that violations have occurred and found "good cause" to issue a Complaint. "Serving only to initiate the proceedings, the issuance of the complaint has no . . . . legal or practical effect, except to impose upon [the respondent] the burden of responding to the charges made against it." *Standard Oil Co.*, 449 U.S. at 242. The Eleventh Circuit has found that "the 'final agency action' requirement implicates federal subject matter jurisdiction," *Nat'l Parks Conservation Ass'n v. Norton*, 324 F.3d 1229, 1240 (11th Cir. 2003), while the D.C. Circuit treats the absence of final agency action as a failure to state a claim upon which relief can be granted. *See, e.g.*, *Reliable Automatic Sprinkler Co. v. CPSC*, 324 F.3d 726, 731-32 (D.C. Cir. 2003). Either way, LabMD loses.

LabMD contends the Commission has already made up its mind, and therefore, further participation in this proceeding would be futile. *See, e.g.*, District Court Complaint at 25-26

---

[4] Although *Myers v. Bethlehem Shipbuilding Co.* concerned the National Labor Relations Act, the Court quoted and relied upon the legislative history of the FTC Act, which revealed Congress' unequivocal intent that this mode of review is exclusive. *See* 303 U.S. at 48 n.5.

(¶¶ 132-37). LabMD is wrong. "Although [respondent] claims that it is highly unlikely that the agency will change its position and that resort to the agency's adjudicatory proceeding would be futile, nothing in the record indicates that the outcome of a hearing, where [respondent] will have the opportunity to present its arguments to the agency, is preordained." *Reliable Automatic Sprinkler Co.*, 324 F.3d at 733. Even assuming, *arguendo*, that the Commission has expressed views in the past about some of the legal and policy issues in this case, that would "not necessarily mean that the minds of its members [are] irrevocably closed on the subject of respondents' . . . practices[,]" nor that they are "prejudiced and biased" against LabMD, so that it "could not receive a fair hearing from the Commission." *FTC v. Cement Inst.*, 333 U.S. 683, 700 (1948).[5] The Commission's ultimate ruling in this case "is contingent on a number of factors" – including an assessment of whether the facts alleged in the Complaint actually occurred, and whether those facts are sufficient to sustain a finding that LabMD committed unfair acts and practices. "Under these circumstances, where [a court] can have no idea whether or when [a sanction] will be ordered, the issue is not fit for adjudication." *Texas v. United States*, 523 U.S. 296, 300 (1998) (quoting *Toilet Goods Assn., Inc. v. Gardner*, 387 U.S. 158, 163 (1967).

B. Irreparable Harm

A party seeking a stay must show that it "will be irreparably injured absent a stay; simply showing some 'possibility of irreparable injury' fails to satisfy the second factor." *Nken*, 556 U.S. at 434-35. LabMD asserts that, absent a stay, the pendency of this proceeding "damages LabMD's business reputation, causing it to lose customer goodwill and market share," "threaten[s] the very existence of [its] business," and "eviscerates LabMD's due process rights." Motion for Stay Pending Judicial Review at 4-5. To be sure, "[t]he harm to property and business can . . . be incalculable by the mere institution of proceedings . . . . Yet it is not a requirement of due process that that there be judicial inquiry before discretion can be exercised" to commence an adjudication. *Mytinger & Casselberry Inc.*, 339 U.S. at 599. Indeed, "every respondent to a Commission complaint" – and every litigation defendant – "could make the [same] claim[.]" *Standard Oil Co.*, 449 U.S. at 242-43. "Irreparable harm cannot be established by a mere reliance on the burden of submitting to agency hearings. This is a risk of litigation that is inherent in society, and not the type of injury to justify judicial intervention." *Sears, Roebuck & Co. v. NLRB*, 473 F.2d 91 (D.C. Cir. 1972). "[T]he expense and annoyance of litigation is 'part of the social burden of living under government[,]' [and] . . . '[m]ere litigation expense, even substantial and unrecoupable cost, does not constitute irreparable injury." *Standard Oil Co.*, 449 U.S. at 244 (quoting *Petroleum Exploration, Inc. v. Pub. Serv. Comm'n*, 304 U.S. 209, 222 (1938), and *Renego. Bd. v. Bannercraft Clothing Co.*, 415 U.S. 1, 24 (1974)).

---

[5] *See also N.C. State Bd. of Dental Exam'rs*, Opinion Denying Respondent's Motion to Disqualify the Commission, 151 F.T.C. 644, 648-54 (2011) (citing, *inter alia*, *Cement Institute*, *Cinderella Career & Finishing Schools, Inc. v. FTC*, 425 F.2d 583 (D.C. Cir. 1970), and *Am. Med. Ass'n v. FTC*, 638 F.2d 443 (2d Cir. 1980)).

C. Effect on Other Parties and Public Interest

Finally, LabMD fails to satisfy the other relevant factors. Its contention that "[a] stay of this matter will injure no one at all," Motion for Stay Pending Judicial Review at 7, is ably countered by Complaint Counsel's argument that a stay could expose "consumers [to] the risk of identity theft, medical identity theft, and other harms." CC Opp. to MSPJR at 6. And needlessly delaying the pending adjudicatory proceeding could frustrate the public interest in expeditious resolution of adjudicatory matters. We cannot conclude that the stay sought by LabMD would be in the public interest.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s request for a stay of administrative proceedings pending disposition of the merits of its Motion to Dismiss **IS DENIED;** and

IT IS FURTHER ORDERED THAT Respondent LabMD's Motion to Stay Proceedings Pending Review in the U.S. Court of Appeals for the Eleventh Circuit and the U.S. District Court for the District of Columbia **IS DENIED.**

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: December 13, 2013

EXHIBIT 14

UNITED STATES DISTRICT COURT.
FOR THE DISTRICT OF NEW JERSEY
Civil 13-1887 ES

FEDERAL TRADE COMMISSION,

Plaintiff, MOTIONS TO DISMISS

V.

WYNDHAM WORLDWIDE CORPORATION, ET AL,

DEFENDANTS.

- -

NEWARK, NEW JERSEY
NOVEMBER 7, 2012

B E F O R E: HONORABLE ESTHER SALAS,
UNITED STATES DISTRICT JUDGE

A P P E A R A N C E S:

KEVIN HYLAND MORIARTY, ESQ.
KRISTIN KRAUSE COHEN, ESQ.
JONATHAN ELI ZIMMERMAN, ESQ.
FOR THE FEDERAL TRADE COMMISSION.

GIBBONS
BY: JUSTIN T. QUINN, ESQ.
AND
KIRKLAND & ELLIS
BY: EUGENE ASSAF, ESQ.
AND: K. WINN ALLEN, ESQ.
For the Defendants.

Pursuant to Section 753 Title 28 United States Code, the following transcript is certified to be an accurate record as taken stenographically in the above-entitled proceedings.

S/LYNNE JOHNSON

- -

LYNNE JOHNSON, CSR, CM, CRR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT
P.O. BOX 6822
LAWRENCEVILLE, NEW JERSEY 08648
CHJLAW@AOL.COM

THE COURT: Good morning to everyone. Please be seated.

We are on the record in the matter of Federal Trade Commission versus Wyndham Worldwide Corporation et al, civil 13-1887. Let me have appearances by counsel.

MR. MORIARTY: Kevin Moriarty on behalf of the Federal Trade Commission.

MR. ZIMMERMAN: Jonathan Zimmerman on behalf of the Federal Trade Commission.

MS. COHEN: Kristin Cohen for the FTC.

MR. QUINN: Justin Quinn for the defendants. Along with me at counsel table is Eugene Assaf, K. Winn Allen and Douglas Meal. Also with me are representatives from Wyndham, Marcus Banks and Korin Neff.

Mr. Assaf will be arguing the authority question. Mr. Allen will be answering any questions with respect to the common enterprise and if your Honor has any questions on the motion to stay, I will be addressing those.

THE COURT: Perfect. Be seated.

Let me tell you the order we are going to go today. We are going to start with whether Section 5, unfair authority extends to data security and if so,

MR. MORIARTY: We are pretty squarely within the fair notices category there. I think there are a lot of answers to that question, the principal one being that Wyndham in its privacy policy tells the consumers that they are going to take commercially reasonable steps to adequately protect their data. So you know, it is an objective standard, reasonableness, and for them to claim that it is now kind of a meaningless standard, it sort of rings hollow.

But as far as advisory opinions, there are not advisory opinions. But the way companies determine what is reasonable and what is not reasonable is the same way companies Act in any other legal context. The entire foundation of the common law negligence is requiring companies to Act reasonably under the circumstances. For example, in the context of data privacy they should evaluate the size and complexity of their network, evaluate the type of consumer data they are collecting and storing. They should evaluate industry standards. There are industry standards out there that are not associated with the FTC. There are experts out there that consult with companies routinely about the data security.

THE COURT: I am sorry to interrupt you,

1 counsel.
2 Does the FTC sort of endorse any particular
3 industry standards that are out there? Are they
4 published? How is that information disseminated in
5 terms of what the industry standard should be?
6 MR. MORIARTY: Industry standards are well
7 known. There are industry standards that specifically
8 apply to the collection and transmission of credit
9 card data. The FTC does not endorse any standards,
10 particular standards. There is a Third Circuit case
11 called Vogel which talked about whether a
12 reasonableness standard should be pinned to industry
13 standards. The Third Circuit said no, it should
14 evaluate other reasonable things that companies in
15 that position should look at.
16 The other thing I wanted to mention about FTC
17 guidance is we have these books that we issue,
18 guidance books. Also the adjudications are very
19 valuable.
20 In this case in particular, I think it is
21 that at page 19 of our brief, we identify a good
22 number of the other, there is, at the time we wrote
23 the brief, there were 19 unfairness cases. I think
24 there is two more that are public. But we identified
25 the particular types of things that companies should

be looking for in order to evaluate whether their data security is reasonable.

Now, we don't say here is how you should set up your router. We don't say you should have, you know, white lists and black lists for IP addresses. We are not tech support. We do say to them, companies, these are the types of things the FCC is looking at, you should make sure your house is in order on these things. The FTC provides guidance through these opinions, through these consent decrees.

THE COURT: Thank you. I will let you address any points you want to address after counsel argues with respect to whether the FTC has provided fair notice.

MR. MORIARTY: Thank you, your Honor.

THE COURT: Thank you. Mr. Assaf.

MR. ASSAF: May I have permission to make two reply points?

THE COURT: Sure.

MR. ASSAF: First of all, with respect to the FTC's point that Graham-Leach-Bliley, COPPA, that these were all cases in which Congress enacted them in order to avoid the FTC having to prove injury. That was kind of how they reconcile these cases. First of all, that is not in their brief. In fact, on page 12

1 section, your Honor, that Graham-Leach-Bliley, the
2 Fair Credit Reporting Act, and COPPA, they have
3 authority to publish rules. But under Section 57 (a)
4 they also have the authority to prescribe rules and
5 general statements of policy, and they have not done
6 that for data security. There is no dispute about
7 that.
8 This is where again it is not just Wyndham.
9 I would suggest there is academic commentary saying
10 the nature, format and content of the agency's data
11 security related pronouncements raise equitable
12 considerations that create serious due process
13 concerns, what I call fair notice.
14 So what are the arguments?
15 Now, I understand, your Honor, I am going to
16 get to the agency's arguments, and I understand that
17 these are requests for admissions, but I think they
18 actually filed them in this Court. And again, there
19 is not any dispute here. The FTC has not published
20 public information about what security software should
21 be used by a company. Admitted.
22 And the FTC has not published any substantive
23 rules or regulations pursuant to their statutory
24 authority explaining what data security protections an
25 individual or entity must employ to be in compliance.

unreasonable security practices. We are in court, I will make this argument. The FTC he will never ever worry about a motion to dismiss under their view. All they have to say is we alleged unreasonable security practices. Let's go forward with discovery. That is all they have to allege, no matter what the violation is.

So your Honor, I have no way, as a defendant, to know what I need to do to stay out of the FTC's aim, or more importantly what I can do in front of an Article III Judge to say, here re the regulations with ascertainable certainty, and my client abided by those regulations. Right now, I can't do either. And I think that is inconsistent with the Third Circuit law. Then we get to deception.

So I am happy to answer any questions, your Honor, but that is the outline of my argument. Again, I don't think there is going to be any dispute that there are rules or regulations, there are none out there.

Thank you, your Honor.

THE COURT: Okay. I will hear from counsel for the FTC.

Do you concede there are no rules and regulations that are currently available?

MR. MORIARTY: Regarding FTC Act liability, no, there aren't for data security. There are for GLB, which counsel pointed out. Graham-Leach-Bliley regulations were issued by the SEC, which goes back to the expertise.

I actually would like to touch on the guidelines from GLB for just a second. Those are the guidelines that if a company violates those guidelines they can be held liable under the FTC Act without injury.

The guidelines, if you look at them, require companies, I mean there are several, I think there are four different steps, but sort of the linchpin of the guidelines is that companies must take steps that are reasonably designed to protect consumer data. And this idea that through the GLB guidelines the FTC has created very elaborate technological regimes where companies can know precisely how to protect their data is inaccurate.

Just to step back for a second, I think the basic premise of Wyndham's fair notice argument is that they don't know how to comply with the reasonableness standard when it comes to protecting consumer information. The argument is problematic. First Wyndham states in its privacy policy it is going

time.

So the last point that I want to make is with these consent decrees, there are consent decrees and then there are also complaints. And the idea that they are not binding on this Court, we don't argue that they are binding on this Court. It is a red herring.

What we argued, the purpose of decrees is to provide parties with notice about the application of the FTC Act and about the types of things that the FTC evaluates when determining whether a company is engaged in reasonable practices with regards to consumer data.

THE COURT: So you say, counsel is arguing that they are not binding, and you never submitted that they are binding. But what you are saying, the real issue here is do these consent decrees provide notice to businesses as to what you need to be doing, and if you are not doing, there is danger.

And so you say that by -- counsel, I don't know whether it was in, it is probably in the reply brief, one of the things they say is all these consent decrees are very -- they are a case that deals directly with this particular company. And it is very difficult for us to say, well, based on those facts

are we in danger? And that they don't provide, you know, adequate warning or adequate notice as to what they need to be doing. And you would say what to that?

MR. MORIARTY: So the answer is that they do provide a lot of information, but we are not exclusively leaning on those adjudications, those consent decrees and complaints as the only source of fair notice. Nor would industry, I believe, accept it if the FTC stated we are the sole arbiter of what is reasonableness.

Reasonableness is an objective standard. It is not the FTC's reasonableness and Wyndham's reasonableness. Reasonableness is objective. There are a lot of sources companies can look to. There is no single answer. That is what happens all the time in the law.

So if a company is trying to figure out, if the grocery store is trying to avoid slip and fall accidents, the common law that they might look at won't be exactly their grocery store, you know, circumstances won't be the same, the type of threats to consumers might not be the same, but they can still make reasonable judgments based on previous cases and a variety of industry standards and just the general