IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LabMD, INC., 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339, Plaintiff, v. **FEDERAL TRADE COMMISSION**; **EDITH RAMIREZ,** in her official capacity as Commissioner and Chairwoman, Federal Trade Commission; **JULIE BRILL**, in her official capacity as Commissioner, Federal Trade Commission; **MAUREEN K. OHLHAUSEN**, in her official capacity as Commissioner, Federal Trade Commission; **JOSHUA D. WRIGHT**, in his official capacity as Commissioner, Federal Trade Commission; and **JESSICA RICH**, in her official capacity as Director, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, Defendants.	)	Civil Action No. _____

VERIFIED COMPLAINT
(For Declaratory and Injunctive Relief)

Plaintiff LabMD, INC. (LabMD), through its counsel, CAUSE OF ACTION, INC., hereby seeks declaratory and injunctive relief from the Defendants' unconstitutional abuse of government power and *ultra vires* actions.

NATURE OF THE CASE

1. This case arises due to Defendants' extralegal abuse of government power.

2. LabMD is a small medical laboratory providing doctors with cancer-detection services. Its patient-information data-security practices are regulated by the U.S. Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). LabMD has never been accused of violating HIPAA or HITECH by the Defendants, HHS, or anyone else.

3. In or about 2008, Tiversa Holding Corp. (Tiversa), a self-described "cyber-intelligence company" specializing in searching and copying files on peer-to-peer networks, took a LabMD patient-information file without LabMD's knowledge or consent.

4. Tiversa then contacted LabMD, advised it that Tiversa had taken its property, and offered a contract for Internet security services.

5. Upon information and belief, Tiversa did this while being paid by the federal government to obtain sensitive files that belong to third parties on peer-to-peer networks without their knowledge or permission.

6. LabMD turned down Tiversa's offer.

7. Tiversa then turned over a copy of LabMD's patient-information file to Defendants.

8. For reasons that have yet to be revealed, Defendants singled out LabMD for punitive action.

9. According to Tiversa, using its unique peer-to-peer monitoring technology, it had amassed "a treasure trove of sensitive documents," including "a spreadsheet from an AIDS clinic

with 232 client names, including Social Security numbers, addresses and birth-dates" and "databases for a hospital system that contained detailed information on more than 20,000 patients, including Social Security numbers, contact details, insurance records, and diagnosis information." However, Defendants apparently did not care about these other alleged patient-information data-breaches, for only LabMD was targeted for enforcement action.

10. Beginning in early 2010, Defendants launched an intrusive and exhaustive, multi-year civil investigation in which Commission staff issued burdensome voluntary access requests and civil investigative demands (CIDs) to LabMD, obtained thousands of pages of documents from LabMD, and deposed, under oath, LabMD principals, causing LabMD crippling economic hardship and reputational harm.

11. Defendants then demanded that LabMD sign a consent order admitting to an unfair trade practice under Section 5 of the Federal Trade Commission Act ("FTCA" or "Section 5"), 15 U.S.C. § 45, due to inadequate data-security practices, notwithstanding the fact that Defendants do not have the statutory authority to punish alleged patient-information data-security breaches and have never issued regulations, standards, or guidelines providing LabMD and others similarly-situated with constitutionally adequate fair notice of the data-security practices Defendants believe that Section 5 permits or requires.

12. LabMD refused to do this.

13. Instead, after years of Federal Trade Commission (FTC) investigation, pressure, and intimidation, LabMD's President and CEO, Michael Daugherty, spoke out regarding the company's ordeal and leveled sharp criticisms at the Defendants' conduct.

14. Upon information and belief, Defendants learned of the criticism in early 2012 and then retaliated against LabMD.

15. In fact, Defendants have repeatedly refused to recognize any limits to their power and demonstrated their willingness to "make an example" of LabMD.

16. On August 28, 2013, Defendants filed an Administrative Complaint (the "Complaint") against LabMD alleging that its data-security practices violated unspecified standards and were "unfair" acts or practices in violation of Section 5. That same day, Defendants issued a press release and posted a blog celebrating their actions and harshly criticizing LabMD, thereby harming LabMD's public reputation.

17. Then, almost immediately, they began engaging in highly irregular and abusive discovery tactics.

18. Although Defendants had spent years investigating LabMD's data-security practices, Defendants first round of "discovery" included twenty-one deposition notices, more than double the number allowed in the federal courts, and all initially set for the same time and date in cities across the Nation.

19. Defendants served LabMD's customers and other third parties, almost none of whom have anything to do with the matters at issue in the Complaint, with wrongfully intrusive and burdensome subpoenas. These persons must do what the FTC says, at their own expense, or suffer threatened legal sanctions by the federal government for non-compliance.

20. The FTC even demanded that Mr. Daugherty give up his book drafts and turn over the names of anyone who commented thereon (and their comments about his book).

21. Upon information and belief, this is all to punish and to make an example of LabMD, both for refusing to sign a consent order and for exercising its First Amendment right to engage in constitutionally protected speech about a matter of public concern and criticize the government without fear of government reprisal.

22. LabMD has challenged these abusive tactics in the FTC's administrative proceeding. But while an independent Article III court would not tolerate Defendants' conduct, here, it is Defendants who ultimately make the rules.

23. Defendants' conduct in this case is *ultra vires*, for they have grabbed power that Congress has not given them.

24. Neither Section 5 nor any other law empowers the FTC to do what it has done to LabMD. Even if Section 5 did empower the FTC to broadly regulate data-security, Congress gave HHS sole authority to regulate patient-information data-security. And, even if Section 5 does empower the FTC to regulate patient-information data-security on top of HHS, Defendants' refusal to issue regulations to give regulated parties fair notice of what data-security practices are permitted or proscribed renders Defendants' conduct here illegal and unconstitutional.

25. Finally, the FTC's Rules of Practice deny LabMD a fair and level review of its cause and therefore violate its due process rights.

26. As a proximate result of Defendants' abuses of power and disregard for core constitutional rights, LabMD has suffered significant economic and reputational damage, lost the benefit of its senior management's attention to growing the business for over three-and-one-half years, been forced to expend hundreds of thousands of dollars on legal fees, and now faces the ruination of its business. The FTC's conduct, statements, and discovery abuses have cost LabMD business opportunities and customer good will. *See, e.g.,* "FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy Commission Alleges Exposure of Medical and Other Sensitive Information Over Peer-to-Peer Network" (Aug. 29, 2013), *at* http://www.ftc.gov/opa/2013/08/labmd.shtm (last visited Oct. 28, 2013).

27. To stop the abuse, LabMD seeks an injunction stopping the FTC's action against LabMD, a declaration that Defendants lack jurisdiction over patient-information data-security practices and have violated LabMD's due process and First Amendment rights, and all of the attorneys' fees and litigation costs LabMD has been forced to bear.

PARTIES

28. Plaintiff LabMD, 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339, is a small, closely-held company providing cancer diagnoses. Physicians provide blood, urine, and tissue samples from their patients to LabMD for testing, LabMD tests the samples for cancer, tumor markers, organisms, and the like and then reports back to the physicians. The physicians, not their individual patients, are LabMD's "consumers" and customers.

29. Defendant Federal Trade Commission ("FTC" or "Commission"), 600 Pennsylvania Avenue N.W., Washington, D.C. 20580, is a federal "agency" under the Administrative Procedure Act (APA), 5 U.S.C. § 551 *et seq*.

30. Defendant Edith Ramirez is the Chairwoman and a Commissioner of the FTC and is named in her official capacity.

31. Defendant Julie Brill is a Commissioner of the FTC and is named in her official capacity.

32. Defendant Maureen Ohlhausen is a Commissioner of the FTC and is named in her official capacity.

33. Defendant Joshua K. Wright is a Commissioner of the FTC and is named in his official capacity.

34. Defendant Jessica Rich is the Director of the FTC's Bureau of Consumer Protection and is named in her official capacity.

JURISDICTION, VENUE, AND GROUNDS FOR RELIEF

35. This Court has jurisdiction under 28 U.S.C. § 1331, 28 U.S.C. § 2201, and 5 U.S.C. § 702.

36. LabMD's *ultra vires* and due process claims raise only pure questions of law and statutory interpretation that do not require any further fact-finding to adjudicate. This Court also has jurisdiction over LabMD's free speech, due process, and *ultra vires* claims under *Trudeau v. FTC*, 456 F.3d 178 (D.C. Cir. 2006). Also, for the reasons set forth in *Athalone Indus. Inc. v. Consumer Product Safety Commission*, 707 F.2d 1485 (D.C. Cir. 1983), the doctrine of exhaustion of administrative remedies does not bar this suit and Defendants' Complaint is a "final agency action" under 5 U.S.C. § 704.

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

38. The grounds for the relief requested include the free speech and due process guarantees of the United States Constitution, 5 U.S.C. §§ 701-706 (APA), 28 U.S.C. § 1651 (the All Writs Act), 28 U.S.C. § 2201 (the Declaratory Judgment Act), 28 U.S.C. § 2202 (further relief), and 28 U.S.C. § 1331 (federal question jurisdiction and implied non-statutory review).

39. This Court may grant LabMD all of its attorneys' fees and costs pursuant to the Equal Access to Justice Act, 28 U.S.C. § 2412.

FACTS

The Genesis of this Case

40. LabMD is a small cancer detection business.

41. Its physician-customers send LabMD blood urine and tissue samples for analysis and give LabMD their patients' medical and billing information along therewith.

42. LabMD's patient-information data-security practices are exclusively regulated by HHS under regulations promulgated pursuant to HIPAA and HITECH.

43. LabMD has never been accused of violating HIPAA or HITECH by the Defendants, HHS, or anyone else.

44. In or about February 2008, without LabMD's knowledge or consent, Tiversa 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) (the "Tiversa Complaint").

45. After taking LabMD's property, Tiversa telephoned LabMD, "offered Tiversa's remediation services," and "provided a contract regarding the cost of remediation." *Id.* ¶¶ 19-21.

46. That same day, Tiversa sent LabMD three emails following up on the phone call to sell its services.

47. Over the next two months, Tiversa sent six more emails soliciting business from LabMD.

48. Tiversa admits in its Complaint that communications between LabMD and Tiversa stopped after "LabMD did not retain Tiversa's services." *Id.* ¶ 22.

49. 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* Robert Boback, CEO, Tiversa, Inc., Testimony before the House Subcommittee on Commerce, Trade, and Consumer Protection 3-4 (May 4, 2009).

50. Tiversa said in a May 28, 2009 press release (since pulled from the Internet) that with its unique technology 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) (the "Tiversa Release").

51. Tiversa 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 health-care firms in the country and discovered "a treasure trove of sensitive documents." These included a spreadsheet from an AIDS clinic with 232 client names, including Social Security numbers, addresses and birth-dates, databases for a hospital system that contained detailed information on more than 20,000 patients, including Social Security numbers, contact details, insurance records, and diagnosis information, the LabMD PI file, and "350+ megabytes of data comprising sensitive reports relating to patients of a group of anesthesiologists."

52. After LabMD refused to hire Tiversa, Tiversa gave Defendants a copy of the purloined LabMD PI file. Tiversa Compl. ¶¶ 25-26.

53. Upon information and belief, there were at all times relevant extensive communications between Tiversa and Commission staff with respect to the circumstances of Tiversa's take and the information in its possession.

Defendants Target LabMD

54. Given Tiversa's very public disclosures of massive data-security breaches by large companies, it is not at all clear why Defendants singled out LabMD for enforcement action, especially given the absence of a complaining witness.

55. In any event, based on Tiversa's wrongful taking of the PI file, the FTC notified LabMD on January 19, 2010, of a "non-public inquiry into LabMD, Inc.'s, compliance with federal law governing information security." Defendants did not specify the regulations, standards, or requirements of the "federal law governing information security" that LabMD supposedly violated, because they had at that time, and still to this day have, failed to promulgate any such regulations, standards, or requirements.

56. Defendants justified their actions by a 2008 Commission Resolution that, according to them, allowed the FTC to create its own authority to target and investigate LabMD and others without the need for congressional sanction. *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"). This Resolution expired on January 3, 2013.

57. On February 24, 2010, LabMD responded to the FTC's inquiry with a fifteen (15) page detailed response and over 5,000 pages of responsive documents.

58. On June 4, 2010, LabMD supplemented its response to the FTC.

59. On July 16, 2010, LabMD once again supplemented its response with a written, narrative timeline of LabMD's ongoing audits, activities, and assessments; the security measures implemented by LabMD; and 617 Bates-labeled documents.

60. On July 23, 2010, LabMD met in person with the FTC. Present for LabMD was its President and CEO, Michael J. Daugherty, Vice-President of Operations and General Manager John Boyle, and outside counsel, Philippa Ellis. Present for the FTC were Mr. Alain Sheer and Ms. Ruth Yodaiken, both of whom conducted an exhaustive inquiry into LabMD's previous submissions and operations.

61. The FTC then launched an exhaustive "fishing expedition" into matters far beyond the PI file.

62. In response, LabMD again supplemented its responses to the FTC inquiry based upon the oral examination of LabMD's CEO and other key personnel and *for the fifth time*, on August 30, 2010, responded in narrative form and provided yet another 925 pages of documents.

63. On February 23, 2011, the FTC contacted LabMD to conduct an investigational hearing seeking additional information about the information-security policies, procedures, and practices LabMD implemented between January 1, 2009, and August 30, 2010.

64. On May 16, 2011, LabMD submitted an eight-page written narrative with 24 exhibits and 169 pages of supplemental materials.

65. On May 31, 2011, LabMD further clarified certain issues raised in the May 16, 2011, submission in a six-page written submission with 14 additional exhibits.

66. Nonetheless, on December 11, 2011, the FTC issued formal civil investigative demands (the "CIDs") to LabMD.

67. LabMD filed a Petition to Limit or Quash the CIDs on January 10, 2012, explaining that, among other things, the CIDs were vague, baseless, and overbroad.

68. Defendant Brill issued a letter on April 20, 2012, denying LabMD's petition. 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. 102 3099 (April 20, 2012) (the "Brill Letter").

69. She admitted that "[t]he FTC commenced its investigation into the adequacy of LabMD's information security practices in January 2010," after Tiversa obtained the PI file. Brill Letter at 2.

70. She also acknowledged that in response to FTC's so-called "voluntary information requests for documents and information," "LabMD produced hundreds of pages of documents, including supplements and responses to follow-up questions," but Commission "staff requested issuance of CIDs" to LabMD and its CEO anyway. *Id.* at 3.

71. But she ridiculed and rejected LabMD's contention "that the Commission must have a 'justifiable' belief that a law violation has occurred before it can issue CIDs…." Brill Letter at 3.

72. She claimed that Defendants have general authority to regulate data-security practices under Section 5, stating that "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." *Id.* at 6.

73. She also said that LabMD's "challenge to the FTC's regulatory authority is … without basis" and rejected, at length, LabMD's argument that HHS has exclusive jurisdiction over patient-information data-security practices. *Id.* at 10-13.

74. LabMD appealed, and on June 21, 2012, three Defendant Commissioners affirmed Defendant 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) (the "Commission

CID Letter"). The Commission refused to even give LabMD an opportunity to be heard on its petition to quash or limit the CIDs: "LabMD's and Mr. Daugherty's request for a hearing is **DENIED…."** *Id.* at 2 (emphasis in original).

75. However, then-Commissioner Thomas Rosch dissented, saying:

> Tiversa … 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 PI file], and then repeatedly solicited LabMD, offering investigative and remediation services regarding … [the PI file], 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.

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), *available at* http://www.ftc.gov/speeches/rosch/120621labdmdissent.pdf (last visited Nov. 12, 2013).

76. The FTC then filed a Petition for an Order to Enforce the CIDs in the U.S. District Court for the Northern District of Georgia. LabMD opposed the Petition.

77. In its decision, the court warned the FTC that "there is significant merit to … [LabMD's] argument that Section 5 does not justify an investigation into data security practices and consumer privacy issues…." *FTC v. LabMD*, Case No. 1:12-cv-3005-WSD, at *6-7 (N.D. Ga. Nov. 26, 2012). However, the court recognized its "sharply limited" role in proceedings to enforce administrative subpoenas, explaining that the "subpoena enforcement proceeding is not the proper forum to litigate the question of coverage of a particular statute." *Id.* at 6-7. Therefore, it upheld the CIDs, finding only that Defendants had made a "plausible" argument of

jurisdiction to civilly investigate whether LabMD had violated Section 5. *See id.* at 1-2, 7, 12-13 & n. 3.

78. LabMD complied with the CIDs, endured two more civil investigative hearings, and produced yet more documents.

Defendants Retaliate For LabMD's Public Criticism

79. In early 2012, Mr. Daugherty decided to speak out and warn the public about Defendants' abuses through the press and social media and through a book, all to express his outrage at the way that LabMD was being treated. Mr. Daugherty used, and continues to use, his website, http://michaeljdaugherty.com/, to criticize the government.

80. Upon information and belief, Defendants have known about Mr. Daugherty's comments and criticisms since at least September 10, 2012—over eleven months before they issued the Complaint—and they have retaliated against LabMD for them.

81. 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.*

82. Three days later, on September 10, 2012, a FTC paralegal downloaded this article from LexisNexis and, on information and belief, disseminated it to Defendants and to Commission staff, including Mr. Alain Sheer, lead Complaint Counsel. The LexisNexis printout states that this download was not in connection with any "Client/matter."

83. On July 19, 2013, Mr. Daugherty posted the trailer to his book, "The Devil Inside the Beltway," on his websitehttp://michaeljdaugherty.com/2013/07/19/the-devil-inside-the-beltway-book-trailer/ . The trailer referred to Defendants' actions as 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.

84. On July 22, 2013, Mr. Sheer told LabMD that Commission staff had recommended that Defendants issue a Complaint against LabMD.

85. On July 30, 2013, Defendant Ramirez's Senior Legal Advisor, Janis Claire Kestenbaum, provided LabMD a copy of a draft Complaint.

86. On August 28, 2013, Defendants issued the Complaint against LabMD. Mr. Sheer is lead Complaint Counsel.

87. On August 29, 2013, Defendants announced their intention to post LabMD's competitively sensitive revenue information on the Internet unless LabMD "files a motion for *in camera* treatment of portions of the Complaint on or before September 9, 2013—pursuant to and in the manner required by Commission Rule 3.45(b)…."

88. On August 29, 2013, several weeks before Mr. Daugherty's book was published, Defendants issued a press release harshly criticizing LabMD. That same day, Defendants also disseminated a "blog post" about their actions in which they made disparaging claims about LabMD and ominously framed the LabMD Complaint as a warning to other businesses: "If your clients are focused on data security —and they should be—here's a development they'll want to know about." Lesley Fair, "FTC Files Data Security Complaint Against LabMD," Business Center Blog (Aug. 29, 2013).

89. On September 5, 2013, Tiversa tried to muzzle Mr. Daugherty by filing a defamation suit. *See* Complaint, *Tiversa et al. v. LabMD et al.*, Dkt. 1, No. 2:13-cv-01296-NBF (W.D. Pa. Sept. 5, 2013). Upon information and belief, Tiversa has at all relevant times been in communication with the FTC and its staff, including Mr. Sheer, about the PI File, LabMD, and Mr. Daugherty.

90. On September 10, 2013, the FTC Administrative Law Judge (ALJ) found that Defendants had wrongfully attempted to post LabMD's confidential business information (which he described as "on its face competitively sensitive revenue information") on the Internet in violation of the Protective Order he had entered in this case. *See* Order Granting in Part and Denying in Part Joint Motion for Provisional *In Camera* Treatment, In the Matter of LabMD, Dkt. No. 9357, at 3 (Sept. 10, 2013). In that Order, the Administrative Law Judge explained that it was unnecessary to seek *in camera* treatment for materials that were already subject to the Protective Order, *see id.* at 1, such as those Defendants had attempted to post.

91. On October 24, 2013, Complaint Counsel served a subpoena duces tecum on Mr. Daugherty requesting the following documents concerning Mr. Daugherty's book:

- "All drafts of … [LabMD's CEO's book about the Defendants] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" LabMD's CEO's book about the Defendants.
- "All documents related to the source material for drafts of" LabMD's CEO's book about the Defendants, "including documents referenced or quoted in the" book. (Complaint Counsel has defined "related" broadly to "mean discussing, constituting, commenting, containing, concerning, embodying, summarizing, reflecting, explaining, describing, analyzing, identifying, stating, referring to, dealing with, or in any way pertaining to, in whole or in part.")

- "All promotional materials related to" LabMD's CEO's book criticizing Defendants, "including, but not limited to, documents posted on social media, commercials featuring … [LabMD's CEO], and presentations or interviews given by" LabMD's CEO.

Defendants' Abuse of Section 5 and the LabMD Complaint

92. Section 5 authorizes the FTC to prohibit and act against "unfair … acts or practices in or affecting commerce."

93. Historically, the FTC has repeatedly abused its Section 5 "unfairness" authority.

94. For example, the FTC once attempted to ban all advertising to children on the ground that it was an "unfair" act or practice.

95. In response, Congress tried to reign in Defendants by prescribing additional necessary but not sufficient conditions for declaring an act or practice "unfair":

> The Commission shall have no authority under [Section 5] to declare unlawful an act or practice on the grounds that such act or practice is unfair 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.… [P]ublic policy considerations may not serve as a primary basis for such determination.

96. Until recently, when it reversed course without explanation and without notice to and comment from affected stakeholders, the FTC told Congress that "as a general matter … [it] lacks authority to require firms to adopt information practice policies." *See* Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, at 34 (2000), *available at* http://www.ftc.gov/reports/privacy2000.pdf; Federal Trade Commission, Privacy Online: A Report to Congress, 41 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited Nov. 12, 2013).

97. However, Defendants now claim Section 5 "unfairness" authority to regulate patient-information data-security practices, even absent a claim of deception, by way of the "common law."

98. In September, 2010, Maneesha Mithal, the FTC's Associate Director of the Division of Privacy and Identity Protection, told Congress that the FTC "enforces the FTC Act's proscription against unfair or deceptive acts or practices in cases where a business failure to employ reasonable security measures causes or is likely to cause substantial consumer injury." *See* Prepared Statement of the Federal Trade Commission on Data Security, Senate Committee on Commerce, Science, & Transportation, Subcommittee on Consumer Protection, Product Safety & Insurance, 2 (Sept. 22, 2010), *available at* http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf (last visited Nov. 12, 2013).

99. In June, 2011, Defendant Brill told Congress that Section 5 requires companies to maintain reasonable safeguards for the consumer data they maintain. *See* Prepared Statement of the Federal Trade Commission on Privacy and Data Security: Protecting Consumers in the Modern World, Senate Committee on Commerce, Science, and Transportation (June 29, 2011) *available at* http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf (last visited Oct. 28, 2013).

100. On August 28, 2013, Defendants voted unanimously (4-0) to issue the Complaint because LabMD had supposedly failed to provide "reasonable and appropriate security" for patient information and that this was an "unfair" act or practice in violation of Section 5.

101. They alleged that (a) LabMD's data-security practices, "taken together," failed Defendants' unpublished, unspecified standards; (b) LabMD's "information security program" was not "comprehensive" because LabMD did not use "readily available measures" for e-mail

security; (c) LabMD wrongly failed to use "readily available measures to identify commonly known or reasonably foreseeable security risks" and, as a result, LabMD "could not adequately assess" data-security risks; (d) LabMD wrongly "did not use adequate measures" and "did not adequately train employees" and "did not employ readily available measures" relating to data-security; and (e) LabMD "could have corrected its security failures at relatively low cost using readily available security measures." Compl. ¶¶ 10(a)-(d), (g), 11.

102. Defendants neither named an individual complainant nor alleged that any specific consumer had been directly harmed by LabMD's supposedly wrongful conduct.

103. They did not allege that LabMD had violated HIPAA or HITECH.

104. They did not allege that LabMD had acted "deceptively."

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

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

107. In fact, they did not cite *any* data-security regulations, guidance, or standards at all.

108. 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) ("Trans.").

109. The FTC does not dispute that LabMD has complied with HIPAA and HITECH at all relevant times. Trans. 22:10-13.

Defendants' Have Predetermined the Outcome of LabMD's Case

110. In May, 2013, Defendants defended their use of Section 5 "unfairness" authority to create a common law of data-security standards in federal court against Wyndham Hotels. *See* Response in Opposition to the Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, *FTC v. Wyndham Worldwide Corp. et al.*, Case No. 2:13-cv-01887-ES-SCM, Dkt. No. 110, at 9-17 (D. N.J. May 20, 2013) (the "FTC's Opposition").

111. In these papers, filed about three months before the Complaint against LabMD was issued, Defendants claimed Section 5 authority to regulate data security and rejected assertions that their failure to promulgate rules and standards unconstitutionally deprives businesses of fair notice. *See id.* at 9-17.

112. Defendants have taken identical positions in the LabMD matter. For example, they defended their CIDs to LabMD by claiming that "Section 5 authority includes … data security" and that "Section 5 plainly reaches conduct that breaches … data security." *See* Reply Memorandum in Support of Federal Trade Commission's Petition for an Order to Enforce Civil Investigative Demands, *FTC v. LabMD et al.*, Case No. 1:12-cv-3005-WSD, at 5-6 (N.D. Ga. Sept. 12, 2012) (the "FTC's CID Reply"). And, the Commission has already specifically rejected LabMD's jurisdictional arguments in both the Brill Letter and the Commission CID Letter.

113. Yet no court has ever held that Defendants may require firms to adopt information practice policies under Section 5's "unfairness" prong. For example, when asked to cite a case that "says the FTC has the authority to investigate data security under Section 5," a FTC attorney

admitted that "the answer is I cannot point you to that case. It doesn't exist…." *FTC v. LabMD, Inc. et al*., Case No. 1:12-cv-3005-WSD, Hearing Trans. 16: 22-25 (Sept. 9, 2012).

114. For matters legitimately within Section 5's scope, Defendants are 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 proscribes federal agencies from creating legislative rules and substantive standards through consent agreements rather than through formal or notice and comment rulemaking.

115. Nevertheless, Defendants have never promulgated data-security regulations, guidance, or standards under Section 5 and apparently have 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 [which do not apply to LabMD]." Trans. 10:11-15.

116. Instead, Defendants claim that the consent orders, public statements, "educational materials" they have posted on the Internet, and documents generated by nongovernmental entities such as the SANS Institute concerning voluntary industry best practices establish substantive legal standards for data security practices that the FTC can enforce using its "unfairness" authority:

> JUDGE CHAPPELL: Have you—in that regard, has the Commission issued guidelines for companies to utilize to protect this information or is there something out there for a company to look to?
>
> [FTC]: There is nothing out there for a company to look to. 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. In addition, there have been public statements made by the Commission, as well as educational materials that have been provided. And in addition, the industry, the IT industry itself, 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, with one exception, and the exception is that the Commission's process as to the calculation of the potential consumer harm from unauthorized disclosure of information.

Trans. 9:13-10:7.

Defendants Have Rigged The Game

117. Due to Defendants' modifications to the Commission's Rules of Practice in 2009, and their course of conduct in this matter, LabMD has been denied a fair and level review of its case and forced to play a rigged game in which the outcome is a fait accompli.

118. To begin with, Defendants' modifications of the Commission's Rules of Practice to take from the ALJ and give to themselves the authority to decide jurisdictional motions have rendered the administrative process futile and violate due process especially where, as here, pure questions of law and statutory interpretation are involved.

119. As the Section of Antitrust Law of the American Bar Association and other commenters explained when the Defendants proposed taking for themselves the power to rule on dispositive motions in the first instance, such a change "could raise concerns about the impartiality and fairness" of the proceeding "by permitting the Commission to adjudicate dispositive issues, including motions to dismiss challenging the facial sufficiency of a complaint, shortly after the Commission has voted out the complaint finding that it has 'reason to believe' there was a law violation, without the benefit of an opinion by an independent ALJ." 74 Fed. Reg. 1,804, 1,809 (Jan. 13, 2009).

120. Commenters also pointed out that Amended Rule 3.22 would "compromise the independence of the ALJ" because he "will not write his initial decision on a 'clean slate,' but will be unduly influenced by the 'entirely transparent views of the Commission delivered on less than a full record,' and will lose his ability to effectively manage discovery." *Id.*

121. The Commission acknowledged then that "commenters (including the Section) criticized the proposed Rule change" to allow Defendants to rule on motions to dismiss complaints they had recently voted to issue "as unfairly invading the province of the independent ALJ and compromising the Commission's dual roles as prosecutor and adjudicator." *Id.*

122. But, undeterred, Defendants changed Commission Rule 3.22(a), 16 C.F.R. § 3.22(a), anyway, grabbing plenary power to rule on motions to dismiss and motions for summary decisions raising legal defenses. 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."

123. As Chief Administrative Law Judge Chappell warned LabMD's counsel during the initial pretrial conference:

> [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*….

Trans. 8:7-18 (emphasis added).

124. Defendants also changed the Commission's Rules of Practice to immediately force Respondents like LabMD to file an answer to a complaint and comply with Complaint Counsels' discovery requests even where, as here, the Respondent raised purely legal defenses to the FTC's actions. *See* 74 Fed. Reg. at 1,808.

125. Thus, unlike the Federal Rules of Civil Procedure, the Commission's Rules of Practice do not allow Respondents like LabMD to avoid the burden and expense of discovery

while threshold legal sufficiency questions are being resolved. *See* Commission Rule 3.12(a), 16 C.F.R. § 3.12(a).

126. In abuse of their authority and in violation of the Constitution's guarantee of due process, Defendants have assumed for themselves 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.

127. Furthermore, Defendants have abused the administrative litigation process simply to punish LabMD for standing by its rights and having the temerity to speak candidly and publicly about the Defendants' actions.

128. On September 17, 2013, LabMD filed an Answer to the Complaint challenging the Defendants' jurisdiction and affirmatively contesting the violations of LabMD's federal constitutional due process rights, among other things.

129. To punish LabMD, Defendants have filed burdensome, duplicative, and oppressive discovery requests that would not be allowed by an independent Article III court.

130. For example, in a three-hour period on October 24, 2013, Complaint Counsel noticed twenty (20) depositions to be taken in various parts of the country—all of which were scheduled at the same time on the same day; served eleven (11) subpoenas duces tecum; and served Complaint Counsel's First Set of Requests for Production and Interrogatories.

131. Therefore, LabMD has been denied even the pretense of administrative transparency, objectivity, and fairness and the Complaint should be deemed a "final agency action" for all relevant purposes.

Further Administrative Proceedings Are Futile

132. On November 12, 2013, LabMD filed a dispositive Motion to Dismiss the Complaint with Prejudice raising legal defenses that present pure issues of law and questions of statutory interpretation in the administrative litigation. It was filed for consideration by and will be ruled on by the named Defendant Commissioners.

133. Yet, Defendants have already determined that LabMD's claims lack merit, as evidenced by their decision to issue the Administrative Complaint *after* their statutory authority to regulate data-security practices as "unfair" acts or practices under Section 5 and the related due process issues were raised in the *Wyndham* litigation (and the FTC explained its legal position on those issues in almost twenty pages of briefing). *See* FTC Opposition at 9-27.

134. For that matter, Defendants have already rejected the jurisdictional arguments LabMD raised in its Motion to Dismiss in the Brill Letter as ratified and adopted by the Commission CID Letter.

135. For example, LabMD's Motion to Dismiss contains argument sections entitled "The Commission Lacks Section 5 'Unfairness Authority to Regulate Patient-Information Data-Security Practices" and "Congress Authorized HHS, Not the FTC, to Regulate Patient-Information Data-Security." The Commission has already validated the Brill Letter's conclusion that "HIPAA and its Rules do not serve to repeal FTC jurisdiction, which is overlapping and concurrent to HHS'." Brill Letter at 13.

136. In its Motion to Dismiss, LabMD also argued that "[t]he 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." FTC has already validated

the Brill Letter's conclusion that "under Section 5, a failure to implement reasonable security measures may be an unfair act or practice…." Brill Letter at 6.

137. Further administrative proceedings are futile.

The Defendants Have Intentionally Crippled LabMD

138. Defendants' power-grab has cost LabMD hundreds of thousands of dollars in costs, attorneys' fees, and damages.

139. They have intentionally interfered with LabMD's customer relationships and engaged in the equivalent of a campaign of commercial disparagement.

140. Their actions have caused, and continue to cause, irreparable injury to LabMD's business reputation and good will in the marketplace. Furthermore, LabMD's management has been forced to devote thousands of hours of time to defending the company from government overreach, time that could have been better spent building the business.

141. LabMD faces ruination due to Defendants' callous abuse of their authority and reckless disregard for LabMD's constitutional rights.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF: *For Abuse of Statutory Authority*.

142. LabMD repeats paragraphs 1–141.

143. Defendants' abuse of their authority as set forth herein 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.

144. Therefore, Defendants' enforcement action against LabMD should be enjoined and a declaration issued that the FTC lacks the authority under the FTCA, absent a specific

Congressional grant of power, to regulate data-security and/or patient-information data-security subject to HHS's jurisdiction.

SECOND CLAIM FOR RELIEF: *For Ultra Vires Agency Action*.

145. LabMD repeats paragraphs 1-144.

146. Under *Trudeau v. FTC*, 456 F.3d 178 (D.C. Cir. 2006), the FTC's *ultra vires* actions are ripe for judicial review regardless of the presence *vel non* of a "final agency action," as defined by the APA, and regardless of whether judicial review of Defendants' actions would otherwise be available under the APA at this time.

147. An agency literally has no power to act unless and until Congress confers the power upon it to do so.

148. Neither Section 5 nor any other federal statute grants Defendants authority to regulate patient-information data-security practices, such as those alleged in the Complaint, as "unfair" acts or practices under Section 5.

149. Congress has not given Defendants the power to do what they have done here to LabMD.

150. Defendants' actions as set forth herein exceed the limited power that Congress conferred upon Defendants in Section 5 and are thus *ultra vires*.

151. Judicial review of this claim is available because Defendants' *ultra vires* actions exceed the authority conferred to them by Congress and the United States Constitution.

152. Defendants' unauthorized extralegal actions are the direct and proximate cause of LabMD's injuries, as described above.

153. Therefore, LabMD is entitled to the declaratory and injunctive relief requested herein.

THIRD CLAIM FOR RELIEF: *For Denial of Due Process.*

154. LabMD repeats paragraphs 1-153.

155. 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.

156. The draft notice order ("Commission Notice Order") attached to Defendants' Complaint against LabMD, 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 PI 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 Defendants 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.

157. 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.

158. Defendants' actions, and the Commission Notice Order, thus implicate LabMD's property rights, which are protected by the Due Process Clause of the Fifth Amendment.

159. Defendants' conduct as set forth herein, including but not limited to their failure to provide fair notice of their claimed patient-information data-security standards, wrongly singling out LabMD for enforcement action, denying LabMD a fair and level administrative process, and retaliating against LabMD for the exercise of protected First Amendment rights, has violated and continues to violate LabMD's due process rights.

160. In light of LabMD's substantial private interests that are affected by Defendants' actions, the high risk of erroneous deprivation of LabMD's property interests and the high value of additional procedural safeguards, and Defendants' de minimis interest in the existing procedure, LabMD has not been provided the procedural safeguards that it is constitutionally entitled to have.

161. Defendants' failure 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, also means that their actions against LabMD violate LabMD's due process rights.

162. Due process requires that laws that regulate persons or entities must give fair notice of conduct that is forbidden or required; 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. Yet Defendants have failed to meet their burden of establishing reasonably ascertainable standards for what data-security practices they believe that Section 5 either forbids or requires.

163. Because Defendants' Section 5 patient-information 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.

164. Furthermore, Defendants' *ex post facto* enforcement action against LabMD for alleged violations of unspecified data-security standards in a proceeding in which the Defendants act in a legislative, prosecutorial, and an adjudicative capacity further violates due process.

165. Finally, Defendants have 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.

166. Defendants' willful and callous violation 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.

167. Under *Trudeau v. FTC*, 456 F.3d 178 (D.C. Cir. 2006), the Commission's unconstitutional actions are ripe for judicial review regardless of the presence *vel non* of a "final agency action," as defined by the APA, and regardless of whether judicial review of Defendants' actions would otherwise be available under the APA at this time.

FOURTH CLAIM FOR RELIEF: *For Retaliation Against LabMD for Protected First Amendment Speech.*

168. LabMD repeats paragraphs 1-167.

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

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

171. Upon information and belief, Defendants' actions against LabMD were retaliation for protected speech.

172. Defendants' actions against LabMD, as set forth herein, will likely chill a person of ordinary firmness from engaging in the protected First Amendment activity. Upon information and belief, Defendants' 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.

173. Even if Defendants and Commission staff 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.

174. Under *Trudeau v. FTC*, 456 F.3d 178 (D.C. Cir. 2006), the Commission's unconstitutional actions are ripe for judicial review regardless of the presence *vel non* of a "final agency action," as defined by the APA, and regardless of whether judicial review of Defendants' actions would otherwise be available under the APA at this time.

WHEREFORE LabMD requests the following relief:

A. Declaratory judgment that (1) Defendants lack statutory authority to regulate data-security practices, including those alleged in the Complaint, under Section 5; (2) Defendants' Complaint was *ultra vires*; (3) Defendants 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 CIDs were issued and the Complaint was filed; (4)

Defendants violated LabMD's due process rights by unconstitutionally combining prosecutorial and investigative functions, allowing the Defendants to rule on dispositive motions concerning complaints they voted to issue; and (5) Defendants violated LabMD's First Amendment rights when they unconstitutionally retaliated against LabMD.

B. Preliminary and permanent injunctive relief providing that Defendants, Defendants' officers, 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 data-security practices constitute "unfair" acts or practices in violation of Section 5; (2) investigate whether LabMD's or any other person's data-security practices violate Section 5 on the ground that they are "unfair" acts or practices; (3) attempt to establish substantive data-security standards under Section 5 and/or enforce Section 5 in administrative proceedings; or (4) undertake or pursue any enforcement proceedings until the Commission amends its Rules of Practice to supply constitutionally adequate due process, including but not limited to rescinding Commission Rule of Practice 3.22(a), 16 C.F.R. § 3.22(a), which allows the Commission to rule on motions to dismiss complaints it recently voted to issue on legal grounds.

C. Such attorneys' fees and litigation costs as it may be entitled to under the Equal Access to Justice Act and/or such other applicable law.

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

Respectfully submitted,

/s/ Daniel Z. Epstein
Daniel Z. Epstein
D.C. Bar No. 1009132
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Telephone: 202.499.4232
Fax: 202.330.5842
daniel.epstein@causeofaction.org.

/s/ Reed D. Rubinstein
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
As Counsel to Cause of Action, Inc.

Dated: November 14, 2013

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: 11/13/13
Michael Daugherty