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.	)	**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

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

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
Date: Commissioners

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