PUBLIC

ORIGINAL

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

RESPONDENT LabMD, INC.'S REPLY IN SUPPORT OF MOTION FOR SUMMARY DECISION

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9100
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.

INTRODUCTION

Complaint Counsel's Opposition and supporting materials confirm that LabMD ("LabMD Inc.") is entitled to summary decision as a matter of law because the FTC lacks jurisdiction over LabMD's PHI data-security and has not provided constitutionally adequate notice of what PHI data-security practices it thinks Section 5 prohibits or requires HIPAA-covered healthcare providers like LabMD to implement.

Granting LabMD's motion is also in the interest of justice and fundamental fairness. For example, a federal District Court recently noted that since late 2012, there was "already a history of acrimony and … on behalf of the agency the exertion of authority in a mean-spirited way" against LabMD. Hearing Trans., *LabMD v. FTC*, No. 1:14-cv-810-WSD, at 47:19-21 (May 7, 2014) (the "PI Trans.") (Ex. 1). After learning that the Federal Trade Commission ("FTC") has been monitoring LabMD's CEO's website and hearing the FTC counsel's explanation, the Court said: "This is taking an interesting and troubling turn which … [the Court] never expected" due to "an admission by an FTC lawyer that they monitor blogs routinely of companies for whatever purposes…." PI Trans. 27:5-9. The Court described parts of the FTC investigation of LabMD as "a sad comment on your agency" and "strik[ing the Court] as almost being unconscionable." PI Trans. 77:9-10, 15. The Court told the FTC that "by your conduct, you have taken" a cancer-detection healthcare provider "out of the market it looks like." PI Trans. 89:2-3.

More broadly, the Court explained:

> [T]here are no security standards from the FTC. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes.…
>
> [H]ow does any company in the United States operate when they are trying to focus on what HIPAA requires and to have some other agency parachute in and say, well, I know that's what they require, but we require something different, and some company says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did. And if you

> want to conform and protect people, you ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.
>
> [I]t's hard for a company that wants to—even a company who hires people from the outside and says what do we have to do, and they say you have to do this, but I can't tell you what the FTC rules are because they have never told anybody. Again, I think the public is served by guiding people beforehand rather than beating them…after-hand.

PI Trans. 94:14-17, 94:25-95:3, 95:7-15. Thus, in consideration of the above commentary and for the reasons explained below, LabMD's Motion for Summary Decision should be granted.

ARGUMENT

As LabMD has previously argued, the FTC lacks Section 5 "unfairness" authority to regulate data-security generally, and specifically for PHI, and Section 5(n)'s text, standing alone, cannot under any circumstances provide constitutionally adequate fair notice of prohibited or required data-security practices. *See* Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357 (Nov. 12, 2013); Reply ISO Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357 (Dec. 2, 2013). For the reasons set forth therein, the Commission's Order Denying Respondent LabMD's Motion to Dismiss ("MTD Order" or "January 16 Order"), *In the Matter of LabMD*, Inc., FTC Dkt. 9357 (Jan. 16, 2014), correctly used the standard for motions to dismiss.

Using the standard for deciding motions for summary judgment, the Commission should grant LabMD's motion for at least two reasons.

First, as applied to LabMD specifically, this enforcement action violates due process under controlling law because LabMD never received constitutionally adequate notice of what PHI data-security practices it was required to or prohibited from implementing that are different

from and in addition to those required by HIPAA, HITECH, and HHS regulations implementing those statutes.[1]

Second, Health and Human Services ("HHS") and state attorneys general have exclusive jurisdiction over healthcare providers' PHI data-security practices under HIPAA and HITECH, and the FTC's Section 5 "reasonableness" test conflicts with and layers inconsistent and additional requirements on top of those statutes. Thus Section 5 "unfairness" is plainly repugnant to these statutes and thus the FTC lacks Section 5 "unfairness" jurisdiction over HIPAA-covered entities' PHI data-security.

I. AS APPLIED TO LabMD, THE FTC'S "REASONABLENESS" STANDARD VIOLATES DUE PROCESS.

A. Due Process Requires Fair Notice of Prohibited Or Required Conduct.

Due process requires fair ex ante warning of prohibited or required conduct.[2] *Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926)). A regulatory standard fails to give fair warning if it "'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.'" *Georgia Pac. Corp. v. OSHRC*, 25 F.3d 999, 1005 (11th Cir. 1994) (quoting *Connally*, 269 U.S. at 391). The Supreme Court has repeatedly affirmed this principle. *See Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2168 (2012); *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012).

---

[1] Courts are obligated to construe statutes to avoid constitutional problems if it is fairly possible to do so. *Boumediene v. Bush*, 553 U.S. 723, 787 (2008). The Commission should apply this principle to the Commission's January 16 Order. Under the facts of this case, due process requires granting this motion.

[2] Due process fair notice requirements apply here. *Ga. Pac. Corp. v. OSHA*, 25 F.3d 999, 1001 (11th Cir. 1994) (due-process fair-notice requirements apply to $480 administrative citation); *U.S. v. Chrysler Corp.*, 158 F.3d 1350, 1355-56 (D.C. Cir. 1998) (car recall); *In re Bogese*, 303 F.3d 1362, 1368 (Fed. Cir. 2002) (forfeiture); *PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51 (D.C. Cir. 2000) (license revocation); *Trinity Broad. v. FCC*, 211 F.3d 618, 619 (D.C. Cir. 2000) (license renewal). Complaint Counsel admits this. MSD Opp. at 10 (FTC "did not state … it is exempt from fair notice doctrine.").

The FTC, "as enforcer of the Act, retains the responsibility to state with ascertainable certainty what is meant by" its putative Section 5 "unfairness" PHI data-security standards. *Georgia Pac. Corp.*, 25 F.3d at 1005; *see Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) (if statute and "policy statements" are unclear and regulated entity's interpretation reasonable, that entity may not be punished). The FTC has not stated with ascertainable certainty PHI data security standards that meet its section 5 "unfairness" tests.

An FTC Commissioner with "a significant amount of experience operating with the model … [they] use at the Federal Trade Commission" candidly and accurately described the FTC's Section 5 "unfairness" data-security regime thus:

> The FTC's process is enforcement-centric rather than rulemaking-centric. As such, it is *ex post* rather than *ex ante* and case-by-case rather than one-size-fits-all. And because an enforcement action requires a complaint and a case to move ahead, the FTC's method typically focuses on actual, or at least specifically alleged, harms rather than having to predict future harms more generally.

LabMD Motion for Summary Decision, *In the Matter of LabMD*, FTC Dkt. 9357 ("MSD") at Ex. 9 pp. 10-11 (Remarks of Commissioner Ohlhausen, FTC, "The Procrustean Problem with Prescriptive Regulations,") (Mar. 18, 2014) (the "Commissioner Statement").

But it is fundamentally unfair, unjust, and unconstitutional to punish a company for allegedly doing or not doing something without first providing fair warning of prohibited or required conduct. Complex, new, and novel academic legal theory about "systemic knowledge problems" allegedly associated with normal, traditional rulemaking processes that not only are transparent and involve meaningful public participation but also provide fair ex ante notice of required or prohibited conduct does not change this. *Cf. id.* Though some may find it "Procrustean," the notion that basic due process requires fair warning of prohibited or required

conduct is simple, timeless, and constitutionally required. *Connally*, 269 U.S. at 391; *SmithKline*, 132 S. Ct. at 2168; *Fox TV Stations, Inc.*, 132 S. Ct. at 2317.

At a minimum, if the FTC wishes to impose PHI data-security requirements on HIPAA-covered entities more rigorous than, inconsistent with, and different from those set by HIPAA, HITECH, and HHS regulations and objective medical-industry custom and practice, as Complaint Counsel is admittedly doing here, it must give those entities some notice that it is doing so. *S&H Riggers & Erectors, Inc. v. OSHRC*, 659 F.2d 1273, 1283 (5th Cir. 1981) (discussing duty to promulgate regulations). The FTC's lack of fair notice violates LabMD's due process rights.

B. Complaint Counsel's "Guidance On Reasonable Data Security."

Complaint Counsel "disputes" LabMD's claim that the FTC has never promulgated data-security regulations, guidance, or standards under Section 5. Complaint Counsel's Public Statement of Material Facts ("CC SOF"), *In the Matter of LabMD, Inc*., FTC Dkt. 9357, at 13 (May 7, 2014). They cite three examples of what they describe as FTC "guidance on reasonable data security." *See id.* Each is addressed in turn below.

First, they cite FTC Facts for Business, Security Check: Reducing Risks to your Computer Systems (June 2003). This document was not published in the Federal Register. It correctly indicates that the FTC only has data-security enforcement authority with respect to financial institutions, which LabMD is not: "For financial institutions, it's an imperative; The Gramm-Leach-Bliley Act and the Safeguards Rule…require financial institutions to have a security plan…." CC SOF at Ex. 33. This document omits mention of HIPAA-covered healthcare providers. It does not say that failure to implement "reasonable and appropriate" PHI

data security is an "unfair" trade practice banned by Section 5. In fact, Section 5 is not mentioned at all.

Next, they cite congressional testimony: Protecting Information Security and Preventing Identity Theft, Prepared Statement of the FTC before Subcomm. on Tech., Info. Policy, Intergov't Relations, and Census, Comm. On Gov't Reform, U.S. House of Representatives. (Sept. 22, 2004) (the "Swindle Testimony"). First, businesses, particularly small businesses, have no obligation to scour congressional testimony before a subcommittee for clues about what an agency most doctors are not familiar with thinks. Second, what the FTC tells Congress cannot establish binding duties and obligations. Third, this testimony provides no meaningful guidance or notice.

Orson Swindle's discussion of "reasonable security procedures" is limited to the Gramm-Leach-Bliley Safeguards Rule, which only applies to financial institutions, and even then just outlines what he calls "principles." CC SOF at Ex. 34 pp 3-4. Swindle does mention Section 5 of the FTC Act but says: "To date, the Commission's security cases have been based on its authority to prevent deceptive practices." CC SOF at Ex 34 p. 7. In footnote 24, he elaborates, mentioning in passing Section 5 "unfairness" and "deception" authority and explaining that "[t]he Commission has used this authority in appropriate case to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing.'" CC SOF at Ex 34 p. 14 n.24.

Swindle's subcommittee testimony is irrelevant and is not notice of anything at all. LabMD has not been accused of a "deceptive" trade practice like Internet "phishing." Businesses cannot be expected to go rooting around in footnotes of congressional subcommittee testimony to attempt to divine compliance obligations.

Finally, Complaint Counsel cites a FTC consent order as "guidance," *In re The TJX Cos.*, FTC Dkt. No. C-4227 (July 29, 2008), even though, as explained below, Section 5 specifically bars the FTC from seeking to enforce these against third parties. Another problem with this putative Section 5 "unfairness" data-security "guidance" is that Complaint Counsel admits that the alleged P2P "security incident" occurred *after* this consent order was issued, and that LabMD removed Limewire from the billing computer *before* then in May 2008. *See* Complaint Counsel's Pre-Trial Br. ("CC Pretrial Br."), *In the Matter of LabMD*, Inc., FTC Dkt. 9357, at 46-47 (May 2, 2014). A third problem is that it pre-dates the first consent order involving an entity partially covered by HIPAA and a joint, parallel HHS enforcement action in the context of dumpster diving. HHS, "CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case," http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html (noting that *In re CVS Caremark Corp.* consent order (June 18, 2009) "is the first instance in which OCR has coordinated investigation and resolution of a matter with the FTC").

More fundamentally, this consent order says nothing about what the respondent allegedly did wrong, *i.e.*, why the FTC thought its alleged data-security practices constituted "unfair" trade practices banned by Section 5. The consent order says nothing about the underlying facts, does not mention what TJX's business is, and does not mention in even general terms what data-security practices TJX allegedly implemented or did not implement. It only notes that "The TJX Companies, Inc." is a Delaware corporation. CC SOF at Ex. 35 p. 2. It does not even outline with any specificity what TJX is required to do or why it is required to do it.

Tellingly, however, the *twenty-nine* pages of Complaint Counsel's Pretrial Brief in which they argue that "LabMD Failed to Provide Reasonable and Appropriate Security for Personal

Information on its Computer Networks" solely cites the spring 2014 Hill paid litigation expert reports (dozens of times) and does not mention any of this alleged FTC "guidance." *See* CC Pretrial Br. at 22-51; PI Trans. 68:20-25 ("Q. … [D]oes Dr. Hill rely on any published materials from FTC? A. She doesn't, which I found interesting. I would have thought that … the expert witness for the FTC would have been referencing FTC guidance for security requirements. She did not….").

There is no genuine dispute as to this material fact.

C. Section 5 and APA Statutory Bar On Use of Consent Orders and Other Internet Postings as "Guidance."

i. APA Federal Register Publication Requirement.

The APA statutorily bars Complaint Counsel from enforcing requirements it claims are set forth in the above-described materials except insofar as these materials are duly published in the Federal Register. 5 U.S.C. § 552(a). Specifically, the APA obligates the FTC to "separately state and currently publish in the Federal Register for the guidance of the public … *statements of general policy or interpretations of general applicability* formulated and adopted by the agency…." 5 U.S.C. § 552(a)(1)(D)(emphasis added). The APA statutorily bars agencies like the FTC from enforcing against companies like LabMD statements of general policy and interpretations of general applicability "[e]xcept to the extent that a person has actual and timely notice of the terms thereof…." 5 U.S.C. § 552(a); *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 754 (D.C. Cir. 2001) (Internet notice is not an acceptable substitute for publication in the Federal Register). There is no allegation that LabMD had actual notice of any of this.

Compliance Counsel's suggestion that LabMD had any duty to comply with or even to consult for "guidance" any of these materials should be rejected. *See also Gen. Elec. Co. v.*

EPA, 290 F.3d 377, 382-83 (D.C. Cir. 2002) (holding that agency guidance document that imposes binding duties and obligations violates the APA).

Even the FTC's own Operating Manual belies Complaint Counsel's claim that the FTC has provided Section 5 data-security "guidance," as the chapter on "Industry Guidance" says nothing about use of consent orders, congressional testimony, and assorted Internet postings. *See* FTC Operating Manual, Ch. 8, *available at* http://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch08industryguidance.pdf (accessed May 8, 2014). Instead, it recognizes that "[t]he Administrative Procedure Act requires … that interpretative rules and policy statements be published in their final form in the Federal Register." *Id.* at 5, §.3.6.4.

ii. Section 5's Statutory Bar on Use of Consent Orders as "Guidance."

Section 5 also statutorily bars Complaint Counsel from attempting to enforce alleged "standards" set forth in the FTC's putative "common law" of consent orders. Congress *specifically barred* the Commission from enforcing a "consent order" against anyone who is not a party to it. 15 U.S.C. § 45(m)(1)(B); *see Good v. Altria Group, Inc.*, 501 F.3d 29, 53 (1st Cir. 2007) ("[T]he FTC Act … with regard to consent orders … specifically provides that the Commission cannot enforce them against non-parties."). Agencies cannot regulate by consent orders, *see Gen. Elec. Co.*, 290 F.3d at 382-83, which "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). Moreover, consent orders do not bind the Commission and restrict its discretion in future actions and thus cannot provide fair notice. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999).

The Commission's January 16 Order also rejected Complaint Counsel's claim that consent orders create a "common law" of data-security that LabMD should have followed. *See* MTD Order at 15-16.

D. Complaint Counsel's Application of "Reasonableness" Violates Due Process.

As noted above, Complaint Counsel's Opposition, Statement of Facts, and Pretrial Brief confirm that PHI data-security standards set by HIPAA, HITECH, and HHS regulations implementing those statutes (and LabMD's compliance or noncompliance with those standards) are "irrelevant" to their case-in-chief and that they are holding LabMD to "standards" sprung on LabMD for the first time in spring 2014 in their paid litigation "expert's" reports. They thereby confirm that summary decision in LabMD's favor is constitutionally required. *See* CC Pretrial Br. 22-51; PI Trans. 58:10-69:14.

Under controlling law, because Section 5(n) is too general, standing alone, to provide fair notice, as the Commission acknowledges by layering upon it a "reasonableness" test, *see* MTD Order at 18-19, "due process requires" that the Commission's Order's "reasonableness" standard be read to incorporate an "objective industry practice standard."[3] *S&H Riggers*, 659 F.2d at 1285; *Fla. Mach. & Foundry, Inc. v. OSHRC*, 693 F.2d 119 (11th Cir. 1982) (industry-specific standards control).

Complaint Counsel wrongly claims that HIPAA/HITECH compliance is, at best, an "affirmative defense." CC SOF at 6, 10-12. But binding precedent holds that Complaint Counsel "bears the burden of proving that" LabMD failed to adopt PHI data-security practices

---

[3] The sole exception requires proof of "clear actual knowledge" of problems and failure to act. *Fla. Mach. & Foundry, Inc.*, 693 F.2d at 120; *S&H Riggers*, 659 F.2d at 1285. Complaint Counsel has never alleged (and no evidence supports) that. In fact, the Complaint alleges the contrary—when LabMD learned of Limewire, it promptly took remedial steps, including but not limited to removing it. *See* Compl.¶ 20 (LabMD "removed … [Limewire] from the billing computer in May 2008, after receiving notice.").

that were customary in the medical industry at the time of the alleged violations. *S&H Riggers*, 659 F.2d at 1285; *Fla. Mach. & Foundry*, 693 F.2d at 120 ("[A] standard of this generality requires only those protective measures which the *employers' industry* would deem appropriate…." (emphasis added)); *see B&B Insulation*, 583 F.2d at 1370 (industry-specific standard, e.g., what is customary for sausage industry or roofing industry).

Complaint Counsel thus has the affirmative burden of proving that LabMD's PHI data-security practices were inconsistent with and less protective of PHI than the objective medical-industry practice standard for PHI data-security practices that were customary for businesses of LabMD's size and nature to adopt at the time that such LabMD practices were used. For example, Complaint Counsel must prove that LabMD's PHI data-security practices in 2005 fell below those that were customary in 2005 for a *healthcare provider* (not IT company) of LabMD's size and nature in 2005 in the medical industry to use—as opposed to IT industry best practices in 2014. HIPAA, HITECH, and HHS PHI data-security regulations reflect the objective medical-industry practice standard for data-security.

When Complaint Counsel says that HIPAA, HITECH, and HHS regulations are "irrelevant," they admit they cannot prove this and have no intention of attempting to do so. Complaint Counsel has offered no evidence as to what medical-industry PHI data-security practices are or were at any specific point in time for healthcare providers of LabMD's size and nature during the relevant time period. They have not accused LabMD of violating medical-industry PHI data-security statutes and regulations that apply to LabMD. Therefore, Complaint

Counsel cannot even establish the constitutionally mandated objective medical-industry practice standard of care, let alone prove that LabMD's conduct fell below it.[4]

Thus, the Commission's January 16 Order's "reasonableness test, as applied to LabMD by Complaint Counsel, violates due process. Under controlling precedent, Complaint Counsel's case is constitutionally defective as a matter of law.

II. THE FTC LACKS SECTION 5 "UNFAIRNESS" JURISDICTION OVER HIPAA-COVERED ENTITIES.

Complaint Counsel argues that whether their after-the-fact paid-litigation-expert "reasonableness" standard is plainly repugnant to and irreconcilably conflicts with PHI data-security *standards* for HIPAA-covered healthcare providers like LabMD—set by Congress and HHS through duly-enacted legislation and normal notice-and-comment rulemaking (specifically, HIPAA, HITECH, and HHS regulations implementing those statues) in a transparent manner with meaningful public participation—"should be addressed at trial…." Complaint Counsel's Resp. in Opp. to Respondent's Mot. for Summary Decision ("CC Opp."), *In the Matter of LabMD, Inc*., Dkt. No. 9357, at 12 (May 5, 2014).

But there is no factual dispute about PHI data-security standards set by HHS regulations (unlike "unfairness reasonableness," regulations specify standards).[5] Complaint Counsel admits

---

[4] There can be no genuine disputes about her "reasonableness" opinions because her reports must "contain a complete statement of all opinions to be expressed and the basis and reasons therefore…." 16 C.F.R. § 3.31A(c).

[5] *See* 42 U.S.C. § 1320d-2(d)(1) (establishing "Security standards for health information" and providing HHS with enforcement authority); 65 Fed. Reg. 82,462 (Dec. 28, 2000) (HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334 (Feb. 20, 2003) (HHS's HIPAA Security Rule); 78 Fed. Reg. 5,566 (Jan. 25, 2013) (HHS's HITECH Rule). LabMD is a HIPAA-covered entity. Opp'n to Mot. to Dismiss, *In the Matter of LabMD,* Inc., FTC Dkt. No. 9357, at 22 n. 15 (Nov. 22, 2013) ("HHS published guidance to entities subject to HIPAA, such as LabMD …."); Compl. ¶¶ 3-4, 6, 9; see 42 U.S.C. §1320d(3)-(4) (defining terms); 45 C.F.R. § 160.103 (same).

that HIPAA, HITECH, and HHS regulations are "irrelevant" to their case-in-chief.[6] CC SOF at 6, 10-12; CC Opp. at 4-5; *see* CC Pre-Trial Br. at iv-vii, 1-72 (not citing or mentioning HIPAA, HITECH, or HHS regulations); LabMD MSD at 6. Their Pretrial Brief shows they solely rely on Hill's reports for "standards." CC Pretrial Br. 22-51 (solely citing Hill dozens of times). Their expert, Hill, does not apply HIPAA, HITECH, or HHS regulations to LabMD's PHI data-security, and her "standards" are different from, inconsistent with, and more rigorous than PHI data-security standards set by applicable statutes and regulations. *See* LabMD MSD at 19-22 & Ex. 12; PI Trans. 58:10-69:13. HHS (and state attorneys general) has exclusive jurisdiction under HIPAA and HITECH. The FTC enforces neither. MTD Order at 12 & n.19.

Section 5 was last amended in 1994; HIPAA was enacted in 1996. *See* MTD Order at 4-5, 11 n.17. Assuming the Section 5 "unfairness" otherwise extended to data-security, application of the *Credit Suisse* factors shows a "plain repugnancy" between the FTC's Section 5 "unfairness" data-security regime and HHS's enforcement of HIPAA/HITECH. *Credit Suisse Securities v. Billings*, 551 U.S. 265, 272, 275-76 (2007); MSD at 19-22; *see also* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2, *307 n.15 (1984)("Of course, if matters involving health and safety are within the primary jurisdiction of some other agency, Commission action might not be appropriate.").

HIPAA (1996), HHS's HIPAA Privacy Rule (2000), and HHS's HIPAA Security Rule (2003) all predate the FTC's "expansion" of Section 5 "unfairness" to data-security, as Swindle admitted that as of September 22, 2004, no "unfairness" cases had been brought. Swindle Testimony at 7; *cf.* MTD Order at 8 (dating "origin" to "late 1990s" but only citing post-2006

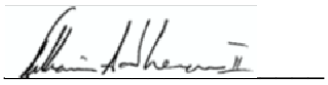
[6] "[T]he Commission cannot enforce HIPAA and does not seek to do so…. The Commission does not enforce HIPAA or HITECH…." MTD Order at 12 & n.19.

documents). Since HIPAA was enacted in 1996, Congress could (and would) not have thought it necessary to explicitly state the FTC has no authority.[7] *Cf.* MTD Order at 12. Even if Section 5 "unfairness" otherwise conferred data-security jurisdiction, the FTC may not impose PHI data-security standards over and above HIPAA. *FTC v. A. P. W. Paper Co.*, 328 U.S. 193, 198-204 (1946).

CONCLUSION

For these reasons, LabMD's Motion should be GRANTED.

Respectfully submitted,



Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141

/s/ Michael D. Pepson
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.

[7] The recent vintage of the FTC's claimed Section 5 "unfairness" data-security authority is precisely why the HIPAA Privacy Rule's Implied Repeal Analysis omits mention of Section 5 but specifically discusses the FTC's data-security authority under a different, targeted statute. 65 Fed. Reg. at 82,481-82,485. HIPAA was necessary, in part, *because* the FTC has never had Section 5 "unfairness" authority over PHI. *Cf. id.* at 82,464 (HHS's HIPAA rule "establishes, for the first time, a set of…fair information practices").

CERTIFICATE OF SERVICE

I hereby certify that on May 12, 2014, 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 caused to be hand-delivered twelve paper copies of the foregoing document to the following address: Document Processing Section, RFO Receiving Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610, Washington, D.C. 20024.

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: May 12, 2014 By:/s/ Michael D. Pepson

2962021v2

EXHIBIT 1

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

LabMD, INC.	)	
	)	
Plaintiff,	)	CIVIL ACTION FILE
	)	NO. 1:14-CV-810-WSD
v.	)	
	)	ATLANTA, GEORGIA
FEDERAL TRADE COMMISSION	)	
	)	
Defendant.	)	
	)	

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

Wednesday, May 7, 2014

APPEARANCES OF COUNSEL:

For the Plaintiff: KILPATRICK TOWNSEND & STOCKTON LLP
(By: Ronald L. Raider
William D. Meyer)
Burleigh Lavisky Singleton)

DINSMORE & SHOHL LLP
(By: Reed D. Rubinstein)

For the Defendant: U.S. DEPARTMENT OF JUSTICE
(By: Lauren Fascett
Perham Gorji
Joel Marcus)

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

And I believe he is still effectively expressing his speech, and, therefore, there is a legitimate reason.

THE COURT: Are you telling me as an officer of the court that after a critical blog post, that somebody at the FTC, in order to make sure that he was -- that he was not impeded in his First Amendment rights, decided the next day to 75 times make sure that the same post was up there and, therefore, it could come in and make an argument like you have just made, that the purpose of that access was to make sure that he was unimpeded in the exercise of his First Amendment rights?

MR. GORJI: Your Honor --

THE COURT: Is that what you are saying?

MR. GORJI: Your Honor, that is not the sole explanation.

THE COURT: Is that what -- is that one of your explanations?

MR. GORJI: I believe that is a legitimate reason for --

THE COURT: And is that why the -- is that why you are representing to me that the FTC accessed his blog, was to make sure that his First Amendment rights were not being impeded?

MR. GORJI: No, I'm not making that representation, Your Honor, that that is the sole reason.

THE COURT: So you are backing from what you just told me?

MR. GORJI: No, no, Your Honor. I believe that one legitimate basis for --

THE COURT: Was that a legitimate basis on behalf of your client, the FTC, the reason why they accessed the blog post 75 times the day after the post was made?

MR. GORJI: Your Honor, I would have to get FTC to provide an explanation as to why they accessed it. I can --

THE COURT: You just told me twice that's one of the reasons they accessed it. Is that one of the reasons why they accessed it?

MR. GORJI: Well, Your Honor, I know that's one of the reasons why I accessed it, for example, during the course of this litigation.

THE COURT: Did you access it on September 17th or September 18th?

MR. GORJI: No, Your Honor.

THE COURT: How many times have you accessed it?

MR. GORJI: Maybe a handful, Your Honor. But -- and that was my motivation.

But I can also surmise, Your Honor, that a government agency might think that there is possibility of statements related to the conduct -- to the conduct that FTC is trying to regulate on his postings and looking for that

reason.

Now, whether or not that is the actual motivation here, Your Honor, I can't attest to that. I can ask FTC to provide you with their explanation.

THE COURT: This is taking an interesting and troubling turn which I never expected, for an admission by an FTC lawyer that they monitor blogs routinely of companies for whatever purposes, and you don't even know the purposes except for this purpose, that the only purpose that you have expressed, which I find incredible, is that you stated on behalf of your agency that the day after this blog posting was made, that the 75 times -- assuming that's true, but even if it was seven times, that they monitored it to make sure that his First Amendment rights were not being impeded, is incredible.

MR. GORJI: Your Honor, that's not my sole explanation. My other explanation --

THE COURT: But it's one of your explanations, isn't it?

MR. GORJI: Your Honor --

THE COURT: Isn't it?

MR. GORJI: Your Honor, I think perhaps that is probably an explanation as to why I personally did it. With respect to the FTC, I don't know whether or not that motivated --

THE COURT: Was my question unclear about the accessing of the website the day after the posting? Did you not understand that?

MR. GORJI: Your Honor, your question was not unclear. I perhaps was confused, but not because of the lack of clarity of your question. I apologize to the Court.

Again, I can have the FTC provide an explanation as to why they are monitoring, and my explanation is again what I surmise, but it may not be sufficient here. And, Your Honor, if Your Honor would like, we could have FTC provide an explanation to the Court.

THE COURT: Well, let's have this rule between you and me at least. This is a hearing. I am a judicial officer, and you are an officer of the court. When I ask you a question, don't duck and cover the question. Answer the question so that I know that what you are telling me is accurate and I can rely upon it. Is that fair?

MR. GORJI: That's fair, Your Honor. I didn't intend to give the impression that I knew what the reason was. I was providing an explanation as to why I think it might be reasonable.

THE COURT: Well, that's not what you said, and the record will be clear that in answer to my two questions, that is not what you said.

MR. GORJI: Your Honor, the jurisdictional arguments are the primary arguments we do make. We do also make the 12 (b) (6) arguments, Your Honor, that do not deny your authority but that we believe the causes of action fail to state a claim.

But I would just like to put something in perspective on behalf of the government here, Your Honor, which is the history of acrimony that you perceive, this is a case that I was just very recently assigned to along with co-counsel here. Counsel who was on this case is no longer with the Department of Justice.

And so I just became aware of this transcript last week, Your Honor. And so there certainly wasn't any --

THE COURT: That's not the defendant's or my fault or my problem. That's your problem. If you want to switch lawyers, you switch lawyers.

And if you are talking about the fellow who was here on the CID, I could tell you as a result of that hearing that there was already a history of acrimony and I think on behalf of the agency the exertion of authority in a mean-spirited way.

MR. GORJI: Well, Your Honor, I can just say that --

THE COURT: And you might -- you know, I'm not saying that -- if you are just new to this case, which

MR. GORJI: Documents, papers.

THE COURT: All right. So -- and where did the police department claim that the papers -- how were the papers obtained?

By papers, you mean paper documents, that somehow they got hold of some paper documents with some patient information on it? Is that what the allegation is?

MR. GORJI: Yes, Your Honor. My understanding is they were in possession of the individuals who pled no contest to the state charges of identity theft.

THE COURT: Well, if they pled no contest, they probably cooperated. Did they tell you where they got the papers?

MR. GORJI: Your Honor, if I might inquire?

Your Honor, I don't have information as to how the documents and the information was obtained by the identity thieves.

THE COURT: Well, has anybody from the FTC gone out and interviewed the people who pled *nolo* to that to find out where it came from, to see whether or not there was indeed a security breach?

Let me tell you something, these are the most simple questions of this investigation. That you are claiming that some police department prosecuted some people for having possession of information which you are now

claiming wrongfully was not protected by LabMD, and you can't even tell me whether or not you have interviewed the people who had the data to find out where they got it to see whether or not there was a security breach or not? And yet you have implemented and instituted this investigation?

And this is your case. You are new -- I know you might be new on it, but for heaven's sakes, you are arguing to me that there is a hearing on May 20th and you don't even know.

MS. FASCETT: Your Honor, if I may just explain, just for clarity, not as an excuse. The FTC attorneys that are handling the administrative proceeding in that hearing, they I'm assuming definitely know these details. They are not present. They are not here today.

We are just -- we were just brought in from DOJ to represent this complaint in this action. So that's part of why we don't have these facts. But we represent the FTC here and we can get these facts for you.

MR. RUBINSTEIN: Your Honor, if I could?

THE COURT: I'm not --

MR. RUBINSTEIN: I --

THE COURT: Sit down.

MR. GORJI: Your Honor, my --

THE COURT: So where are those lawyers? Are they too busy to come to Atlanta today?

MS. FASCETT: Well --

THE COURT: Is that one of them sitting back there in the gallery?

MS. FASCETT: No, she's a U.S. Attorney here in Atlanta, unrelated.

THE COURT: How about this other fellow back there, is he an FTC lawyer too?

MR. MARCUS: Your Honor, we have a gentleman here from the FTC.

THE COURT: Are you involved in this investigation?

MR. MARCUS: I am personally not involved in the investigation.

THE COURT: Okay. So you are off the hook.

So far I have got four lawyers here and none of them are involved in the investigation. How about --

MR. MARCUS: We do have are a lawyer who is involved in the investigation.

THE COURT: And what's your name?

MR. SCHOSHINSKI: Good morning, Your Honor. Robert Schoshinski. I'm assistant director in the Division of Privacy and Identity Protection.

THE COURT: All right. So in this case, what investigation has been made as to the source of the documents that the police department out in California found?

MR. SCHOSHINSKI: Your Honor, the complaint counsel, so that is the FTC counsel who is litigating the complaint in the administrative action, noticed the depositions of the two individuals who pled no contest to identity theft.

One they could not serve because she was just simply not findable. The other one was in jail. We --

THE COURT: Did you try to find her?

MR. SCHOSHINSKI: Yes, we did, Your Honor. We hired several process servers. They made many attempts to try to find her but were unable to serve her.

THE COURT: And when did you first try to serve her?

MR. SCHOSHINSKI: Your Honor, I don't have the exact dates, but --

THE COURT: Well, give me an approximation.

MR. SCHOSHINSKI: Your Honor, I would say late 2013, early 2014.

THE COURT: So really late in the game, you finally decided that it made sense to go and find out with respect to one of the allegations that's the basis of your investigation that's been ongoing for months, because the CID was something I dealt with some months ago, that you finally decided -- or not you, but your lawyers finally decided that maybe it would be good to try to find the people who actually had the

information to determine where they got it?

MR. SCHOSHINSKI: Yes, Your Honor.

THE COURT: Does that strike you as odd?

MR. SCHOSHINSKI: Your Honor, it doesn't strike me as odd. It's what --

THE COURT: Does it strike you as late?

MR. SCHOSHINSKI: Your Honor, it strikes me as the normal course of the investigation.

THE COURT: Boy, that's a sad comment on your agency, that you would wait until months before a hearing and months after you instituted an investigation on a principal claim that you are asserting, that you have not even taken any effort to interview the people that you claim had the documents that underlie the charge of a security breach. That strikes me as almost being unconscionable.

And how much money -- how much activity was there before you served those subpoenas trying to get the information from LabMD with respect to a security breach that you don't even know how it occurred? How much activity?

MR. SCHOSHINSKI: Your Honor, how would you like me to estimate?

THE COURT: Let's start in months.

MR. SCHOSHINSKI: Well, Your Honor, I believe the investigation began in January of 2010.

THE COURT: Okay. So three years before you tried

to subpoena them?

MR. SCHOSHINSKI: Your Honor --

THE COURT: I'm sorry, two and a half years.

MR. SCHOSHINSKI: Your Honor, the knowledge of this incident didn't occur until after the CID enforcement hearing up here in Atlanta. That's when we were notified that this incident had occurred, in October of 2012.

THE COURT: So you found out about the -- the incident you are talking about is the California police incident?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: All right. And how soon after you found out about the incident did you try to contact the police authorities in California to find out what they knew about the source of the information?

MR. SCHOSHINSKI: Immediately.

THE COURT: And what did they tell you?

MR. SCHOSHINSKI: They told us that they did not know.

THE COURT: And then what did you do next, and how soon did you do it?

MR. SCHOSHINSKI: We shared the information with LabMD concerning the -- what we found out once we were able to confirm that it was LabMD's information, and we then attempted to find out further from the California police

department what they knew about the source of this information.

THE COURT: And what did they tell you they knew about the source?

MR. SCHOSHINSKI: They told us they were not able to get the source from the defendants in the case.

THE COURT: Did you talk to the prosecutor of the case as well?

MR. SCHOSHINSKI: I don't believe so, Your Honor.

THE COURT: And so you tried to track down one of the two defendants. Did you try to track down the second of the two defendants?

MR. SCHOSHINSKI: Yes, Your Honor. We actually obtained service on the second defendant, who was in jail. We noticed his deposition in the action, went to take his deposition, and he pleaded the Fifth Amendment and refused to answer questions.

THE COURT: So sitting here today, you have no idea where the documents came from, whether they came from LabMD or some other source? Is that a fair thing to say?

MR. SCHOSHINSKI: No. We believe they were LabMD's documents.

THE COURT: Well, they might have been LabMD's documents, but you don't know how they got into the possession of the two individuals that you tried to contact

that pled guilty to this offense?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: So you have no information to establish how those documents were obtained; is that right?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: And you are still proceeding on this claim?

MR. SCHOSHINSKI: Yes, Your Honor, because the claim is not concerning that incident alone. It's concerning --

THE COURT: All right. But are you still proceeding on that claim?

MR. SCHOSHINSKI: We are proceeding on that evidence, Your Honor.

THE COURT: And that evidence relates to other claims, because you have other documents that were found in other places?

MR. SCHOSHINSKI: That evidence relates to the potential injury suffered by consumers as a result of exposure of this information.

THE COURT: Are you serious about that last response?

MR. SCHOSHINSKI: Yes, Your Honor, I am.

THE COURT: So you don't know where the documents came from, you don't know how these people got the possession

of it, you don't know whether they originated from LabMD or some other place, but you are going to use that to show that, because they committed identity theft, that certain individuals were damaged by documents, the source of which you don't even know?

MR. SCHOSHINSKI: Yes, Your Honor.

THE COURT: Holy cow.

So what's the other incident that you are relying on?

MR. SCHOSHINSKI: The other incident is the exposure of the insurance agent file of several thousand consumers.

THE COURT: And when was that?

MR. SCHOSHINSKI: That was in 2008, Your Honor.

THE COURT: And that was through the file-sharing program?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: And how do you know that they came through the file-sharing program?

MR. SCHOSHINSKI: We know because third parties found the file on file-sharing programs.

THE COURT: Well, I accept that. How do you know that they came through the file-sharing program that was loaded on a computer at LabMD?

MR. SCHOSHINSKI: Based on the evidence we obtained

than it is in this case, and then they are arguing that, although I'm co-equal to the judge in New Jersey, that because it came to me a different way, that I can't.

I suspect that they would love to travel forward on the New Jersey decision because it favors them and that they will try to deny the opportunity for another judge to weigh in.

But I think it's a significant -- you ought to find a way, unless you are so hell bent on expanding this jurisdiction or advocating this jurisdiction, to find some way to decide this legal issue.

And I understand why you are doing what you are doing. I have been alive long enough to understand how government and their agencies work. I have been a member of an agency and I understand its impact on defendants or in this case on parties that are under investigation. I understand that too because I have done that as well.

But I think that there is a fundamental jurisdictional legal issue, and there ought to be some way of getting a more definitive ruling than what you have right now.

Because I would hope that you would think that in this current healthcare environment, that the more competition and providers there are for medical detection devices or processes like those offered by LabMD, that the

better off the consuming public is and the better off patients will be. But by your conduct, you have taken one out of the market it looks like.

And if I was an agency head, I would say there has got to be some way of being satisfied that this doesn't happen again, however it happened, and to make sure that we have as many providers as possible out there determining whether or not people do or do not have cancer.

And that that would mean a good faith, transparent, authentic discussion about what your concerns are, and trying to get those allayed by some process which would not be a twenty-year monitoring.

You know, I have defended people that had twenty-year monitoring responsibilities by an agency, big companies, and it's very, very expensive, and it's really intrusive, and in my personal opinion, having been on both sides, they generally are not necessary.

But there is never a middle ground. There should be.

But I would think that it would be in the benefit of all the parties here to say whatever happened, it can't happen again, but whatever you are doing ought to continue to be done, because it benefits the consuming public, which I think is who you are supposed to be protecting under reasonable certainties, that the consuming public would be

Congress, and we turn things down.

I think good lawyers -- and he was an agency lawyer for a long time and ran the Southern District for a long time as United States Attorney -- that that lesson has always stuck with me.

So where we are now is I have given you my insights about this. I understand there is no more evidence to be presented.

I don't need any more -- I guess you can cross-examine him if you want. All I hear him saying is that he doesn't like your expert's report and he would have done something differently and he's claimed that HIPAA is what should be, because there are specific standards there -- I think that you will admit that there are no security standards from the FTC. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes.

I too find how does any company in the United States operate when they are trying to focus on what HIPAA requires and to have some other agency parachute in and say, well, I know that's what they require, but we require something different, and some company says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did.

And if you want to conform and protect people, you

ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.

But I think that's what happens when you jump too quickly into something that you want to do, and whether that's circumstances or whether that's agency motivation, I don't know. But it seems to me that it's hard for a company that wants to -- even a company who hires people from the outside and says what do we have to do, and they say you have to do this, but I can't tell you what the FTC rules are because they have never told anybody.

Again, I think the public is served by guiding people beforehand rather than beating them after they -- after-hand. But the assistant director doesn't have the authority to do that. He reports to the deputy director, who reports to the director, who reports to the commission. So he's way down in the pecking order.

So I understand what this witness said.

I suspect that this witness will say that he never consulted with LabMD before about their security processes. He's just come in to opine on the opinions offered by Ms. Hill. Is that correct?

THE WITNESS: Correct.

THE COURT: I kind of wish he had been there before.