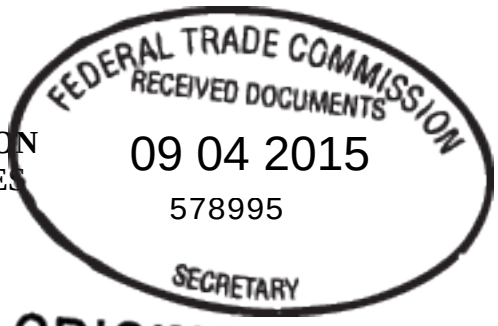
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES



ORIGINAL

In the Matter of	)	**PUBLIC**
LabMD, Inc. a corporation, Respondent.	)	Docket No. 9357

RESPONDENT LABMD, INC.'S
POST-TRIAL REPLY BRIEF

Daniel Z. Epstein
Patrick Massari
Cause of Action
1919 Pennsylvania Avenue, NW
Suite 650
Washington, DC 20006

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004

Counsel for Respondent

Dated: September 4, 2015

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTION

STATUTES

REGULATIONS

OTHER AUTHORITIES

GLOSSARY OF TERMS

Administrative Law Judge	ALJ
Administrative Procedure Act	APA
Complaint Counsel's Admissions	CCA
Complaint Counsel Post-Trial Brief	CCPTB
Complaint Counsel Proposed	CCPCL
Conclusions of Law	
Complaint Counsel Proposed Findings of Fact	CCPFF
Federal Trade Commission	FTC or Commission
Federal Trade Commission Act	FTC Act
Health Insurance Portability and Accountability Act of 1996	HIPAA
Health Information Technology for Economic and Clinical Health Act	HITECH
LabMD, Inc.	LabMD
Peer to Peer	P2P
Respondent Post-Trial Brief	RPTB
Respondent Proposed Conclusion of Law	RPCL
Respondent Proposed Findings of Fact	RPFF
Respondent's Reply to Complaint Counsel's Post-Trial Brief	RR-CCPTB
Respondent's Reply to Complaint Counsel's Proposed Conclusion of Law	RR-CCPCL
Respondent's Reply to Complaint Counsel's Proposed Findings of Fact	RR-CCPFOF
Section 5	15 U.S.C. §45
Sacramento Police Department	SPD
The Department of Health and Human Services	HHS
Tiversa, Inc.	Tiversa
United States House of Representatives Committee on Oversight and Government Reform	OGR

INTRODUCTION

The Commission, secure in its powerful administrative process advantages, has overreached, causing substantial injury to LabMD, and to the doctors and patients that it served. *See Burlington Truck Lines v. United States*, 371 U.S. 156, 167 (1962) (White, J.) ("[U]nless we make the requirements for administrative action strict and demanding, *expertise*, the strength of modern government, can become a monster which rules with no practical limits on its discretion.") (quoting *New York v. United States*, 342 U.S. 882, 884 (dissenting opinion); *see also FCC v. RCA Commc'ns, Inc.*, 346 U.S. 86, 90 (1953) ("Congress did not purport to transfer its legislative power to the unbounded discretion of the regulatory body."). FTC's collusion with Tiversa proves, as Justice Douglas warned long ago, that "[t]he temptation of many men of goodwill [in government] is to cut corners, take short-cuts, and reach the desired end regardless of the means." *Hannah v. Larche*, 363 U.S. 420, 494 (1960) (Douglas, J., dissenting).

Judgment for LabMD is proper on the significant constitutional and statutory questions, many of first impression, raised in this case. Also, FTC's case against LabMD is admittedly, directly, and entirely derivative of the Commission's unlawful collusion with Tiversa in criminal violations of HIPAA, justifying the exclusion of all Complaint Counsel's evidence. (Sheer, Tr. 31 ("It is likely that we would not know about the defects in LabMD's security practices had we not known that LimeWire was out on the—that—rather, that the 1718 File was on the P2P network.")). Nevertheless, this Court need not rule for LabMD on the law, nor even exclude the fruits of FTC's unlawful deal with Tiversa, to enter judgment in its favor. On the evidence, Complaint Counsel has failed to prove its case.

ARGUMENT

The Commission, without evidence of actual or certainly impending injury to a single consumer,[1] and without making even one allegation that medical data security laws and regulations had been violated, unleashed the unequaled might and power of the Federal government against LabMD, an innovative small company providing cancer detection services. Declaring, years after the fact, that LabMD's HIPAA-compliant data security practices were "unreasonable" and "unlawful" under Section 5, FTC destroyed LabMD without consideration for the doctors and patients it served or for whether the Commission's action would do more harm than good.

FTC uses administrative process as punishment.[2] Its "administrative process advantages" coerce firms into consent orders that are, in turn, used to extract other settlements. *See* CCPCL

[1] On March 30, 2006, FTC told Congress that it received "roughly 15 to 20 thousand contacts *per week* from the toll-free identity theft hotline,…or through our website or mail, from victims and from consumers who want to avoid becoming victims." *See* Deborah Platt Majoras, Chairman, "Prepared Statement of The Federal Trade Commission Before the Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies of the Committee on Appropriations United States House of Representatives" at 5 (March 30, 2006)(emphasis added) *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-subcommittee-science-departments-state-justice-and/p040101commissiontestimonyconcerningappropriationshouseofrepresentatives03302006.pdf However, FTC did not receive one complaint about, and could not find even one victim attributable to, LabMD, the 1718 File, or the Day Sheets.

[2] Once the Commission votes out a complaint, the merits case is functionally over.

> The key to understanding the threat of Section 5 is the interaction between its lack of boundaries and the FTC's administrative process advantages. What do I mean by administrative process advantages? Consider … FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. *In other words, in 100 percent of cases where the ALJ ruled in favor of the*

¶¶ 17-20. FTC's targets "typically prefer to settle Section 5 claims rather than go through lengthy and costly administrative litigation in which they are both shooting at a moving target and may have the chips stacked against them." *See* Joshua Wright, "The FTC at 100: Where Do We Go From Here?" at 3 (Dec. 3, 2013) *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-joshua-d.wright-ftc-100-where-do-we-go-here/131203wheredowegostatement.pdf.[3] LabMD chose not to give in, and FTC put it out of business. (Daugherty, Tr. 1027-34).

Complaint Counsel offers no evidence that LabMD's data security is "unreasonable" now, or has been at any point since July 2010. It offers no evidence that LabMD's pre-July 2010 data security practices are likely to reoccur or to cause any consumers substantial injury. All of FTC's claims of current and future risk, including the testimony of all its experts, are based on the perjured claim that the 1718 File was available on peer-to-peer networks in November 2013. (RX 525 (Kaufman, Dep. at 62 ("Well, certainly as of November 2013 the 1,718 file was still available on peer-to-peer networks.")).[4]

> *FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed.*

Wright, "Recalibrating Section 5: A Response to the CPI Symposium" at 4 (Nov. 2013) (emphasis added) (noted omitted), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf (last accessed Sept. 2, 2015).

[3] As Malcolm M. Feeley pointed out in his classic study of the Court of Common Pleas in New Haven, Connecticut, *The Process Is The Punishment: Handling Cases In A Lower Criminal Court* (2d ed, 1992), the experience of being arrested, incarcerated, and processed through pre-trial process is the primary form of punishment, rendering the ultimate adjudication and sentencing essentially irrelevant. Merely becoming engaged in the system generates significant direct and indirect costs for those caught up in it. Joshua Wright's scholarship confirms Feeley's observations apply with equal force regarding FTC.

[4] Richard Wallace, the Tiversa insider and whistle-blower, testified that CX 0019 was created to demonstrate "spread" at the specific direction of Robert Boback, Tiversa's CEO, after a meeting

Nevertheless, Complaint Counsel demands draconian, twenty-year injunctive "fencing-in" relief, *see, e.g.*, CCPCL ¶¶ 80-89, because LabMD first dared to dispute the Commission's allegations and then dared to argue that Tiversa—for its criminal violations of HIPAA, perjury, obstruction, and deceptive business practices—should be in the dock instead. *See* CCPCL ¶ 76.[5] However, even if Complaint Counsel has proven that LabMD's data security practices fail Section 5, it has not carried its burden and proven that injunctive "fencing-in" relief is proper.

I. THE COMMISSION FAILS ON THE THRESHOLD CONSTITUTIONAL AND JURISDICTIONAL ISSUES.

This case presents at least three threshold constitutional issues, apart from fair notice and the Commission's administrative process advantage, for this Court to resolve: the effect of the Appointments Clause on this proceeding; the effect of *Department of Transportation v. Association of American Railroads*, 135 S. Ct. 1225 (2015), on the Proposed Order; and the effect of FTC's collusion with Tiversa on Complaint Counsel's proofs. As set forth below, the

---

with FTC staff in Washington, D.C. (Wallace, Tr. 1368-1370). Kaufman's testimony confirms FTC viewed the "spread" of the 1718 File to be critically important, which makes sense given that Complaint Counsel had no other evidence of actual or certainly impending injury to any consumer. (RX 525 (Kaufman, Dep. at 62)); (Sheer, Tr. 15-16, 31). In other words, without spread, FTC could not meet the "likely to cause" test under Section 5(n) and its case would thus implode.

[5] Complaint Counsel states:

> LabMD's failure to take responsibility for its lax data security and refusal to acknowledge its data security issues demonstrate the need for injunctive relief. *Compare,e.g.,* LabMD's Motion to Admit RX-543 – RX-548 at 6 (asserting that Complaint Counsel should have investigated Tiversa rather than LabMD in connection with the release of the 1718 File), *with* JX0001-A (Joint Stips. of Law and Fact) at 4 (stipulating that LimeWire was installed on the billing manager's computer and that 900 files, including the 1718 File, were designated for sharing).

CCPCL at ¶ 76.

Appointments Clause requires dismissal, *Railroads* renders the Proposed Order unlawful, and FTC's collusion with Tiversa justifies exclusion of *all* Complaint Counsel's evidence.

This case also presents a threshold jurisdictional issue: whether Complaint Counsel has proven this matter is in the "public interest." *FTC v. Klesner*, 280 U.S. 19, 28 (1929). As set forth below, it has failed to do so.

A. The Appointments Clause.

Under the Appointments Clause of Article II of the Constitution, federal "inferior officers" must be appointed by the President alone, the courts, or the "Heads of Departments," as Congress provides. U.S. Const., Art. II, § 2, cl. 2. Because of the "significance of [their] duties and discretion," *Freytag v. Comm'r of Internal Revenue*, 501 U.S. 868, 881 (1991), Administrative Law Judges ("ALJs") serving within the Federal Trade Commission (to which they are "inferior") are "officers" within the meaning of the Appointments Clause. Yet, they are appointed *not* by the FTC's "Head[] of Department" (*i.e.*, the Commissioners collectively) but instead by members of the Office of Personnel Management. Accordingly, their appointment violates the Constitution, and thus the "powers conferred" on them cannot be exercised. *Buckley v. Valeo*, 424 U.S. 1, 143 (1976); *see Hill v. SEC*, No. 15-1801, 2015 WL 4307088, at *16-19 (N.D. Ga. June 8, 2015) (holding that Securities and Exchange Commission ALJs are "officers" whose selection violated the Appointments Clause); *Timbervest LLC v. SEC*, No. 15-2106, at 17-27 (N.D. Ga. Aug. 4, 2015), ECF No. 25 (same); *Duka v. SEC*, No. 13-357, 2015 WL 4940083, at *2-3 (S.D.N.Y. Aug. 12, 2015) (same).

1. Because FTC ALJs exercise significant authority, they are "Officers" within the meaning of the Appointments Clause.

The Appointments Clause specifies the permissible means of appointing "Officers of the United States." U.S. Const., Art. II, § 2, cl. 2. There are two classes of officers. "The primary class"—that of "principal" officers—"requires a nomination by the President and confirmation by the Senate." *United States v. Germaine*, 99 U.S. 508, 509–10 (1879). As for other "such inferior Officers," "the Congress may by Law vest [their] Appointment . . . , as they think proper, in the President alone, in the Courts of Law, or in the Heads of Departments." U.S. Const., Art. II, § 2, cl. 2.

The Appointments Clause applies only to "Officers of the United States." That term, the Supreme Court has emphasized, has "substantive meaning." *Buckley,* 424 U.S. at 126. Under the test set forth in *Buckley*, those "exercising significant authority pursuant to the laws of the United States" are "officers" subject to the Clause, whereas "lesser functionaries subordinate to officers of the United States" are mere "employees," to whom the Clause does not apply. *Id.* at 126 & n.162.

It is well-established that judges in Article I courts satisfy *Buckley*'s "significant authority" test.[6] *See Free Enter. Fund v. Pub. Co. Accounting Oversight Bd.*, 561 U.S. 477, 540 (2010) (Breyer, J., dissenting) (noting that, under settled precedent, "judges in Article I courts" are "officers"). In *Freytag,* the Supreme Court resolved a challenge to the appointment of a non–Article III "special trial judge" designated by the Chief Judge of the United States Tax Court to hear certain tax cases. The Court held that the judge was an "officer," since (1) his position was "established by law," (2) "the duties, salary, and means of appointment for that office" were "specified by statute," and (3) the judge "perform[ed] more than ministerial tasks" and "exercise[d] significant discretion," having been empowered to "take testimony, conduct trials, rule on the admissibility of evidence, and . . . enforce compliance with discovery orders." 501 U.S. at 881-82. It made no difference whether the judge had carried out, or even had been capable of carrying out, those "important functions" in *that* particular case. So long as the judge

[6]Article I courts are tribunals whose judges "do not have any constitutionally guaranteed lifetime tenure and protection from salary diminution" and are "not governed by the case or controversy limitation of Article III." The term "include[s] . . . legislative courts and administrative agencies that adjudicate 'public rights.'" John E. Nowak & Ronald D. Rotunda, *Constitutional Law* 22–23 (4th ed, 1991).

"is an inferior officer for purposes" of some cases, then "he is an inferior officer" in all cases. *Id.* at 882.

FTC ALJs are plainly officers under *Freytag*.[7] *See Landry v. FDIC*, 204 F.3d 1125, 1134 (D.C. Cir. 2000) (concluding that ALJs meet the three criteria). Here, as in *Freytag*, the Article I judge holds an office "established by law." *See* 5 U.S.C. § 556(b)(3) (establishing ALJs). Here, as in *Freytag*, the judge's "duties, salary, and means of appointment" are "specified by statute." *See id.* §§ 556, 557(b) (duties); *id.* § 5372 (salary); *id.* § 3105 (means of appointment). And most importantly, here, as in *Freytag*, the judge exercises "significant discretion" and discharges "important functions," such as the power "to take testimony, conduct trials, rule on admissibility of evidence, and . . . enforce compliance with discovery orders." *Freytag*, 501 U.S. at 881-82.[8]

The Supreme Court has explained that "[t]here can be little doubt that the role of the . . . administrative law judge . . . is functionally comparable to that of a judge." *Butz v. Economou*, 438 U.S. 478, 513 (1978) (internal quotation marks and citation omitted). Authorized by statute to preside over hearings in rulemaking and adjudicative proceedings, 5 U.S.C. § 556(a), ALJs may "administer oaths," "issue subpoenas," "rule on offers of proof and receive relevant

[7] Specifically, like the special trial judge in *Freytag*, FTC ALJs are *inferior* officers, because their "work is directed and supervised at some level" by one or more principal officers—namely, the FTC Commissioners. *Edmond v. United States*, 520 U.S. 651, 663 (1997).

[8] The conclusion that FTC ALJs are inferior officers is also supported by a recent opinion of the Department of Justice's Office of Legal Counsel ("OLC"). *See* Officers of the United States Within the Meaning of the Appointments Clause, 31 Op. O.L.C. 73 (2007). The opinion explains that the term "Officers of the United States" generally has been read to cover "many particular officers who had authority but little if any discretion in administering the laws; these included officers such as registers of the land offices, masters and mates of revenue cutters, inspectors of customs, deputy collectors of customs, deputy postmasters, and district court clerks." *Id.* at 95. In particular, the opinion states that the Appointments Clause governs the appointment of personnel with "authority to act in the first instance, whether or not that act may be subject to direction or review by superior officers." *Id.* As explained in text, FTC ALJs fit that description.

evidence," "take depositions or have depositions taken," "regulate the course of the hearing," "require" a party to attend a conference, "dispose of procedural requests," and "make or recommend decisions," among other actions. *Id.* § 556(c). Although his or her decisions are generally subject to *de novo* review by the Commission, an "ALJ has wide discretion in discovery matters, and his or her determinations should be reversed only for a clear abuse of discretion." *In re Boise Cascade Corp.*, No. 9133, 1982 FTC LEXIS 17, at *2 (F.T.C. Oct. 15, 1982). For example, an ALJ ruling on a discovery request will not be disturbed by the FTC "in the absence of unusual circumstances." *In re Marlo Furniture Co.*, 73 F.T.C. 1250, 1251 (1968).

Commission rules vest ALJs with still more authority. ALJs perform the agency's "statutory fact-finding functions" and "serve as presiding officers under section 18(a)(1)(B) of the Federal Trade Commission Act," the provision authorizing rulemaking to define prohibited "unfair or deceptive acts or practices." 16 C.F.R. § 0.14. More generally, the Commission vests ALJs with "all powers necessary" to conduct fair hearings, to avoid delay, and "to maintain order." *Id.* § 3.42(c). That includes the power to "compel admissions" *sua sponte*, "certify questions to the Commission," "reject written submissions that fail to comply with" rules, "deny in camera status without prejudice until a party complies with all relevant rules," impose discovery sanctions, consolidate for joint trial issues raised by factually related but separate complaints, and bifurcate trials of separate claims. *Id.* §§ 3.38(b), 3.41(b), 3.42(c). ALJs may also "suspend or bar" attorneys for inappropriate conduct. *Id.* 3.42(d). And "[a]ny party who refuses or fails to comply with a lawfully issued order or direction of an [ALJ] may be considered to be in contempt of the Commission." *Id.* § 3.42(h).

This is not the job description of a "lesser functionary" or "mere employee." Rather, these are responsibilities "essentially like those of a federal magistrate assigned to conduct a

hearing and to submit proposed findings and recommendations to a district judge." *Landry*, 204 F.3d at 1143 (Randolph, J., concurring in part and concurring in the judgment). When a party objects to a magistrate's proposed findings and conclusions, the district judge—like the Commission—must conduct *de novo* review. *See* 28 U.S.C. § 636(b)(1)(C). Nevertheless, "it has long been settled that federal magistrates are 'inferior Officers' under Article II, which is why they are appointed by 'Courts of Law' under 28 U.S.C. § 631." *Landry*, 204 F.3d at 1143 (Randolph, J., concurring in part and concurring in the judgment) (citing *Rice v. Ames*, 180 U.S. 371, 378 (1901); *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 352-54 (1931); *Pacemaker Diagnostic Clinic v. Instromedix*, 725 F.2d 537, 545 (9th Cir. 1984) (en banc) (Kennedy, J.)).[9]

That ALJs easily clear *Buckley*'s "significant authority" threshold is especially unsurprising in light of the many less significant federal positions that the Supreme Court has held to be offices. That list includes a district-court clerk, *In re Hennen*, 38 U.S. 230, 258 (1839); "thousands of clerks in the Departments of the Treasury, Interior and the othe[r]" departments, *Germaine*, 99 U.S. at 511; postmasters first class, *Myers v. United States*, 272 U.S. 52, 106 (1926); an election supervisor, *Ex parte Siebold*, 100 U.S. 371, 397-98 (1880); an

[9] Indeed, just as with magistrates, vesting ALJs with "significant discretion" and "important functions" is necessary "to safeguard [their] decisional independence." *Mahoney v. Donovan*, 721 F.3d 633, 635 (D.C. Cir. 2013); 5 C.F.R. § 930.201(3) ("An agency employing [ALJs] . . . has . . . [t]he responsibility to ensure the independence of the [ALJ]."). If FTC ALJs were merely "lesser functionaries" playing the part of the Commission's cat's-paw in agency proceedings, their decisions would lose all semblance of impartiality, and would "pose such a risk of actual bias or prejudgment that" due process would be offended. *Caperton v. A.T. Massey Coal Co.*, 556 U.S. 868, 884 (2009); *see id.* at 870 ("Just as no man is allowed to be a judge in his own cause, similar fears of bias can arise when . . . [an entity] chooses the judge in [its] own cause.").

"assistant-surgeon" and a "cadet-engineer" appointed by the Secretary of the Navy, *United States v. Moore*, 95 U.S. 760, 762 (1878); *United States v. Perkins*, 116 U.S. 483, 484 (1886); and the general counsel of the Department of Transportation, *Edmond*, 520 U.S. at 666. *See also id.* at 661 (compiling a similar list); *Free Enter. Fund*, 561 U.S. at 540 (2010) (Breyer, J., dissenting) (same). No wonder eight Justices of the Supreme Court—including five now sitting—have concluded that ALJs are indeed officers.[10]

Although a divided panel of the D.C. Circuit has held that ALJs serving in the Federal Deposit Insurance Corporation are "not inferior officers," *Landry*, 204 F.3d at 1134, the majority opinion in that case erred in several fundamental respects. First, the majority opinion simply misread *Freytag*. *See Hill*, 2015 WL 4307088 at *18 (pointing this out); Kent Barnett, *Resolving the ALJ Quandary*, 66 Vand. L. Rev. 797, 813 (2013) (Judge Randolph's separate opinion "had the better argument"). As the panel majority understood *Freytag*, the judge in that case was an officer *only because* he had been given the "power of final decision in certain classes of cases," *id.* at 1133-34. Not so. By the time the Court in *Freytag* even took up the final-decision point, it *had already concluded* that the judge was an officer *solely* because of the "significance of [his] duties and discretion" in all cases. 501 U.S. at 881; *see Hill*, 2015 WL 4307088 at *18 ("[*Freytag*] had already determined the STJs were inferior officers before it analyzed the final order authority issue.").

[10] *See Freytag*, 501 U.S. at 910 (Scalia, J., concurring in part and concurring in judgment, joined by O'Connor, Kennedy, and Souter, JJ.) (ALJs "are all *executive* officers"); *id.* at 919 (ALJs are "inferior officers"); *Free Enter. Fund*, 561 U.S. at 542 (Breyer, J., dissenting, joined by Stevens, Ginsburg, and Sotomayor, JJ.) ("As Justice Scalia has observed, administrative law judges are all executive officers.") (internal quotation marks and citation omitted). *But see id.*, 561 U.S. at 507 n.10 (opinion of the Court) (observing that "[w]hether administrative law judges are necessarily 'Officers of the United States' is disputed").

In any event, *Landry*'s nearsighted proposition that ALJs hold only "purely recommendatory powers" misses the mark for several reasons. 204 F.3d at 1132. First, by focusing only on an ultimate decision, *Landry* demeans the many other, frequently utilized powers that ALJs exercise as presiding judges. To compel an admission, require a party's attendance at a conference, or suspend an attorney, for example, is not to make a *suggestion*; it is to exercise *authority*.

Relatedly, *Landry* ignores that, "in managing the prehearing process," ALJs carry out "actions which are generally unreviewable and thus final as a practical matter," such as "control[ing] scheduling, subpoenas, document production, and depositions." Jerome Nelson, *Administrative Law Judges' Removal "Only for Cause": Is That Administrative Procedure Act Protection Now Unconstitutional?*, 63 Admin. L. Rev. 401, 415-16 (2011) (former ALJ). It also overlooks that many interlocutory orders issued by ALJs are also effectively unreviewable by the Commission. *See* 16 C.F.R. § 3.23 (in general, except for orders falling in three narrow categories that are appealable as of right, interlocutory orders are immediately appealable to the Commission only with the ALJ's permission). In any event, even as to final decisions, the Commission does not always have the last word. Because ALJs' "initial decisions become the *agency* decisions unless appealed to or reviewed by the agency," ALJs "are thus the final deciders in many instances." Nelson, 63 Admin. L. Rev. at 415 (citing 5 U.S.C. § 557(b)).

More fundamentally, *Landry* improperly uses the test for whether an official is an "*inferior* officer" for whether he or she is an "officer" at all (as opposed to a mere employee). That ALJ's cannot render *final* decisions in some contexts simply demonstrates that they are "directed and supervised" by the Commissioners. *See Edmond*, 520 U.S. at 663. But that is the

test for determining whether an "officer" is "inferior" (or "principal"); it thus cannot be the test for whether the person is an officer (or an employee).

Judge Randolph made this point: "[t]he fact that an ALJ cannot render a final decision and is subject to the ultimate supervision of the FDIC shows only that the ALJ shares the common characteristic of an 'inferior Officer,'" since "'inferior officers' are officers whose work is directed and supervised at some level by others who were appointed by Presidential nomination with the advice and consent of the Senate." *Landry*, 204 F.3d at 1142 (quoting *Edmond*, 520 U.S. at 663). *Edmond* illustrates the point. The question there was whether judges on the Coast Guard Court of Criminal Appeals, an intermediate appellate court, were inferior or principal officers. According to the Court, "[w]hat is significant is that the judges . . . have no power to render a final decision on behalf of the United States unless permitted to do so by other Executive officers." 520 U.S. at 665. By *Landry*'s logic, that would mean that the judges were not *officers* in the first place. But, by the Supreme Court's logic, it proved that the judges were *officers* who were *inferior*. Just so with FTC ALJs, whose decisions are also generally subject to principal-officer review.

For these reasons, because FTC ALJs exercise significant authority, they are "officers" within the meaning of the Appointments Clause.[11]

[11]As a consequence of ALJs' status as "officers," the "dual for-cause" removal protection afforded to them by statute is an unconstitutional "multilevel protection." *Free Enter. Fund*, 561 U.S. at 484, 502; *see* 5 U.S.C. § 7521(a) (removal action "may be taken" by FTC against an ALJ "for good cause established and determined by the Merit Systems Protection Board ['MSPB']"); *Id.* § 1202(d) (MSPB members removable for cause); 15 U.S.C. § 41 (FTC Commissioners removable for cause). As *Free Enterprise Fund* clearly holds, the executive power is infringed when "the President [is] restricted in his ability to remove a principal officer, who is in turn restricted in his ability to remove an inferior officer, even though that inferior officer" is an executive officer. 561 U.S. at 483-84.

2. Because the FTC Commissioners do not collectively appoint FTC ALJs pursuant to statute, they are not selected by the "Head of Department" in accordance with the Appointments Clause.

Because FTC ALJs are inferior officers, Congress may vest their appointment in the President, in the courts, or, as relevant here, "in the Heads of Department." U.S. Const., Art. II, § 2, cl. 2. A "Department" is "a freestanding component of the Executive Branch, not subordinate to or contained within any other such component." *Free Enter. Fund,* 561 U.S. at 511. "[A] multimember body," such as a Commission, is itself the department's "Head" if the department's powers "are generally vested in the Commissioners jointly, not the Chairman alone." *Id.* at 512. Applying these definitions in *Free Enterprise Fund*, the Supreme Court held that the Securities and Exchange Commission is a "Department," and that the "Commission as a whole" was its "Head." *Id.* at 510-13. Similarly, FTC is a "Department" and, because its powers are lodged in the full Commission, *see, e.g.*, 15 U.S.C. §§ 41, 45, 47, the Commission as a whole is its "Head." Consequently, the ALJ's in FTC are improperly appointed because they are not appointed by the full Commission—*i.e.*, the "Head" of that "Department."

The full Commission does not appoint FTC ALJs. Instead, the ALJs "are appointed under the authority and subject to the prior approval of [OPM]." 16 C.F.R. § 0.14. *See* 5 C.F.R. § 903.204 (all ALJs must be "approv[ed]" or declared "eligible[ ]" by OPM); *Friedman v. Devine*, 565 F. Supp. 200, 202 (D.D.C. 1982), *aff'd*, 711 F.2d 420 (D.C. Cir. 1983) ("Congress has committed broad authority to OPM to determine the qualifications for the position of ALJ, 5 U.S.C. § 1305, and the regulations empower OPM to rate candidates based upon criteria developed by OPM. 5 C.F.R. § 930.103."); *id.* at 203 ("OPM must be free to define and revise criteria to govern eligibility for ALJ service."); *see also* 5 U.S.C. § 3344 ("An agency . . . which occasionally or temporarily is insufficiently staffed with administrative law judges . . . may use administrative law judges selected by the Office of Personnel Management from and with the

consent of other agencies.").[12] Accordingly, the Government has recently conceded that its independent-agency ALJs are *not* appointed by department heads. *Hill*, 2015 WL 4307088 at *3 (accepting concession that "SEC ALJs are not appointed by the President, the Courts, or the [SEC] Commissioners. Instead, they are hired by the SEC's Office of Administrative Law Judges, with input from the Chief Administrative Law Judge, human resource functions, and the Office of Personnel Management") (internal quotation marks and citation omitted); Def.'s Opp. to Emergency Mot. to Supp. Br. at 2-3, *Hill v. SEC*, at 19 ("The SEC concedes that Plaintiff's ALJ . . . was not appointed by the President, a department head, or the Judiciary.") (internal citations omitted); *cf. In re Timbervest, LLC et al.*, SEC Release No. 4096, 2015 WL 3398239, at *1 (May 27, 2015) (ordering SEC Division of Enforcement to submit an affidavit setting forth the exact manner in which two particular ALJs were "selected and appointed").[13]

[12] Over the years, the FTC has made efforts to resist OPM's control over the ALJ appointment process. *See, e.g.*, Barnett, 66 Vand. L. Rev. at 805 n.40; *Advancing the Judicial Independence and Efficiency of the Administrative Judiciary A Report to the President-Elect of the United States November 2008 Federal Administrative Law Judges Conference*, 29 J. Nat'l Ass'n Admin. L. Judiciary 93, 96–97 (2009) ("During the past year . . . the Federal Trade Commission [has] sought to introduce legislation that would have permitted them to circumvent the ALJ selection process and appoint favored employees within their own agencies.").

[13] In the APA, Congress provided that "[e]ach agency shall appoint as many [ALJs] as are necessary" for rulemaking and adjudicative proceedings. 5 U.S.C. § 3105. This does not and has not authorized the full Commission to appoint ALJs. As the Government has recently noted, "agency" in § 3105 does not connote "head of department"—*i.e.*, in the case of the FTC, the full Commission. Rather, § 3105 authorizes agencies simply to hire ALJs in the same manner as they hire other employees. The Government therefore concedes that, if ALJs are officers, their means of appointment is unconstitutional. *See* Deft's Opp. to Emergency Mot. to Supp. Br. at 2-3, *Hill v. SEC*, No. 15-cv-1801 (N.D. Ga. May 29, 2015), ECF No. 15 ("[C]onsistent with ALJ James E. Grimes's status as an agency employee and not a constitutional officer, he was not appointed by the SEC Commissioners. Indeed, the SEC[ ] . . . [has] discussed . . . the statutory provision that provides that it is the agency, *not the head of the Department*, that appoints ALJs.") (emphasis added); *id.* at 25 ("Congress specified in the APA that it is the 'agency'—not the President, the department head, or the Judiciary—that appoints ALJs. [*S*]*ee* 5 U.S.C. § 3105.") (some internal citations omitted).

For these reasons, because FTC ALJs are not appointed by a department head pursuant to an act of Congress their selection violates the Appointments Clause.

B. The Proposed Order Is Unlawful.

Section II of the Proposed Order provides:

> **IT IS FURTHER ORDERED** that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:
>
> A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
>
> B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
>
> C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and
>
> D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

The Proposed Order is unlawful. First, Article I of the Constitution establishes that all authority in FTC or other agencies is inherent to statutory grants. Section 5 does not authorize FTC to "deputize" private third parties, and therefore this is *ultra vires.*

Second, the Proposed Order authorizes the "qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession" to develop and apply the metrics and standards of data security and to apply them. These metrics and standards have a coercive effect on LabMD. That is regulatory power, and therefore unlawful. *Railroads*, 135 S. Ct. at 1236 (Alito, J. concurring); *Bennett v. Spear*, 520 U. S. 154, 169 (1997).

The Proposed Order also raises Appointments Clause, separation of powers, and due process concerns. *Railroads* at 1233, 1235-39 (Alito, J., concurring). For example, Article II officers with regulatory authority must swear an oath to uphold the Constitution. The "third-party professional" who will choose and apply regulatory requirements (because FTC has not done so under 15 U.S.C. § 57a) does not. "[I]t raises '[d]ifficult and fundamental questions' about 'the delegation of Executive power' when Congress authorizes citizen suits." *Id.* at 1237 (Alito, J., concurring) (quoting *Friends of the Earth, Inc.* v. *Laidlaw Envtl. Services (TOC), Inc.*, 528 U. S. 167, 197 (2000) (Kennedy, J., concurring)). "A citizen suit to enforce existing law, however, is nothing compared to delegated power to create new law. 'By any measure, handing off regulatory power to a private entity is 'legislative delegation in its most obnoxious form.'" *Id.* at 1237-8 (Alito, J. concurring) (quoting *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936)).

That the third party's reports will be sent to FTC is of no legal moment. FTC has no medical (or other) data security standards or technical competency to judge what is or is not compliant. Instead, it relies entirely on outside "experts." In this case, for example, FTC relied on Dr. Hill, who in turn applied her own standards to determine that LabMD's data security was "unreasonable." (Hill, Tr. 230-31, 235-36) (Dr. Hill only became aware of the defense in depth strategy circa mid-2009); (RX 524 (Hill, Dep. at 59-60, 65-66, 71-74 (Ex. 1 at p. 19 ¶ 52) (as

Dep. Ex. RX-1), 86, 91-92)); (CX 0740 (Hill, Rep. at 4-8, 20 ¶ 55, 22-23 ¶ 61(b) (bullet 2), 24-25 ¶ 65, 26-28 ¶ 68(c), ¶ 69)).

FTC could, perhaps even should, adopt industry data security standards as the regulatory "metrics and standards" for Section 5. But to do this, it must exercise its 15 U.S.C. § 57a authority, not regulate through adjudication. *See* 40 CFR §§ 312.10, 11 (EPA "All Appropriate Inquiries" rule defining "environmental professional" and incorporating ASTM standards as basis for determining regulatory compliance). FTC may proceed by adjudication only in cases where it is enforcing discrete violations of existing laws and where the effective scope of the impact of the case will be relatively small, and by § 57a procedures if it seeks to change the law and establish rules of widespread application. *Ford Motor Co. v. FTC*, 673 F.2d 1008, 1010-11 (9th Cir. 1981).[14]

C. The Tiversa Taint.

The legal consequences of Tiversa's unlawful conduct, and of FTC's collusion, are of central importance to this case.

Complaint Counsel began the trial by saying:

> MR. SHEER: An insurance billing file that was designated for sharing from the billing manager's computer was found at IP addresses in Arizona, San Diego, Costa Rica, and London. The file, which we call the 1718 File, contained information about more than 9300 consumers.

[14] The third party requirement in the Proposed Notice Order, combined with FTC's lack of clear standards, creates serious due process problems by blurring FTC's accountability from a public framework for principled decision-making and clear boundaries for discretion. *See Envtl. Def. Fund, Inc. v. Ruckelshaus*, 439 F.2d 584, 598 (D.C. Cir. 1971). Judicial review after the fact can only correct the most egregious abuses, *id.*, and does nothing to prevent administrative process from becoming a burdensome punishment. *See supra* at note 1. The Proposed Notice Order all but guarantees arbitrary and discriminatory enforcement—what one "expert" might deem compliant another could deem a violation, and without clear standards from the regulator, how is LabMD to know what is right?

> JUDGE CHAPPELL: Excuse me. You say this information was found in these various places. How was it found?
>
> MR. SHEER: It was found by a third party who was searching the P2P networks.
>
> JUDGE CHAPPELL: And what was their motivation to be searching?
>
> MR. SHEER: The motivation of the search is that the third party is in the business of trying to protect the information of its clients, and it does so by searching P2P networks, looking for information about the clients. In doing that, it came across these files.

(Sheer, Tr. 16). *But see* (Wallace, Tr. 1344, 1368-70).

It then admitted:

> MR. SHEER: It is likely that we would not know about the defects in LabMD's security practices had we not known that LimeWire was out on the–that–rather, that the 1718 File was on the P2P network.

(Sheer, Tr. 31). *But see* (Wallace, Tr. 1367-68). *See also* RPFF ¶ 55 ("Boback and Tiversa directed Wallace to intentionally create the illusion that companies' PII and/or PHI was widely available on P2P networks.") (citing (Wallace, Tr. 1367-68)).

Now, Complaint Counsel says only the following about the "third party" (Tiversa) and the claim, repeated and relied upon by all of its experts, that the 1718 File was "found at IP addresses in Arizona, San Diego, Costa Rica, and London":

> Rather than demonstrate the reasonableness of its data security practices, LabMD has attempted to make this litigation only about the exposure of the 1718 File, claiming that it was "stolen" when in fact, as LabMD's witness Mr. Wallace testified in response to LabMD's questioning it was freely available from a LabMD computer to anyone, anywhere using LimeWire . . . LabMD has zeroed in on this exposure with an obsession rivaling Inspector Javert, spinning a web of conspiracy theories dripping with innuendo and unsupported allegations.

CCPTB at 4.[15]

[15] Complaint Counsel's characterization of LabMD as "Inspector Javert" for refusing quiet acquiescence to FTC's overreach and complicity in Tiversa's criminal HIPAA violations reflects a dangerous arrogance. Most recently, Chinese and Russian hackers stole the personal

Complaint Counsel's blithe assertion that LabMD must "demonstrate the reasonableness of its data security practices" neatly captures FTC's generally applicable "verdict first, trial afterward" approach to Section 5. *See, e.g.*, Wright, "Time for the FTC to Define the Scope of its Unfair Methods of Competition Authority" at 7 (Feb. 26, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/626811/150226bh_section_5_symposium.pdf.

Also, *contra* Complaint Counsel, LabMD did not make the 1718 File "freely available" to anyone (LimeWire was running ***only because*** a rogue employee violated company policy, RPFF ¶¶ 82-124) and Wallace gave no such testimony. In fact the word "freely" does not appear in the transcript of Wallace's testimony. (Wallace, Tr. 1361-1444). A file is "shared" on LimeWire only in response to a specific request. RPFF ¶¶ 52-57; (Fisk, Tr. 1153, 1156). Only because Boback directed Wallace to expertly search for information that could be "monetized,"

---

information of 22 million Americans (including intelligence assets) from the Office of Personnel Management and taxpayer information of over 300,000 Americans from the Internal Revenue Service. *See* Morgan Chalfant, *IRS Admits Breach May Have Compromised Over 300,000 Taxpayer Accounts*, Wash. Free Beacon (Aug. 17, 2015), http://freebeacon.com/national-security/irs-admits-breach-may-have-compromised-over-300000-taxpayer-accounts. The HHS Office of Inspector General reports "reveal pervasive and persistent deficiencies across HHS and its operating divisions' information security programs" including FDA and CMS, that have led to "five HHS operating divisions [being] breached using unsophisticated means within the last three years." *See* Majority Staff Report, "Information Security at the Department of Health and Human Services" (Aug. 5, 2015), http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Analysis/20150806HHSinformationsecurityreport.pdf. FTC could not prove that a single LabMD patient, from January 2005 to the present, suffered identity theft, medical identity theft, credit card fraud, or any other harm due to LabMD's allegedly unreasonable data security, yet it turned on the company. It would be anomalous and unjust for the Commission to hold a small cancer laboratory with objectively better data security performance than major federal agencies to violate Section 5.

was Tiversa able to take 1718 File because *the 1718 File was never exposed on the Internet*. Instead, it had to be physically removed from a LabMD computer. (Wallace, Tr. 1372).[16]

Finally, Tiversa's take of the 1718 File without LabMD's consent for the purpose of monetizing the information was theft by any common definition of the word. *See, e.g., Gonzales v. Duenas-Alvarez*, 549 U.S. 183, 189 (2007) ("generic definition of theft" is the "taking of property or an exercise of control over property without consent with the criminal intent to deprive the owner of rights and benefits of ownership, even if such deprivation is less than total or permanent") (citations omitted); *Hernandez-Mancilla v. INS*, 246 F.3d 1002, 1006-07 (7th Cir. 2001) (theft means "taking of property without consent") (citations omitted).

Here are the facts:

At all times relevant, the federal HIPAA provision protecting patient privacy and medical data security, 42 U.S.C. § 1320d-6(a), provided:

> A person who knowingly and in violation of this part . . . (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section.

On February 17, 2009, this was amended by the following:

[16] The claim that the 1718 File was "freely available" is one of many egregious claims by the government in this litigation. If the 1718 File was "freely available," then presumably Tiversa's patented technology would have found it when it searched for Dartmouth in January 2008; and/or LabMD would have found it, when it searched in May and June 2008. Another, related egregious claim, is that LabMD's data security put 750,000 patients were at risk. *See* (Sheer, Tr. 11); CCPTB at 80; CCPCL ¶¶ 30, 113. Only the 1718 File, a document created in June 2007 and stored, in violation of company policy, on an employee's computer with LimeWire, also in violation of company policy, was stolen. Tiversa could not have stolen any other patient information through LimeWire because none was available. In fact, between January 2005 and the present, none of LabMD's "750,000" patients on its "computer networks" have suffered any harm because there has not been a data breach. *Compare FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 U.S. App. LEXIS 14839 (3d Cir. Aug. 24, 2015), *with Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487 (7th Cir. July 20, 2015).

> For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d–9(b)(3) of this title) and the individual obtained or disclosed such information without authorization.
>
> At all times relevant, HIPAA's punishment provision, 42 U.S.C. § 1320d-6(b), provided:
>
> A person described in subsection (a) of this section shall—(1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.
>
> At all times relevant, the State of Georgia's computer crime law, Ga. Code Ann. § 16-9-

93, provided:

> (a) Computer theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession; (2) Obtaining property by any deceitful means or artful practice; shall be guilty of the crime of computer theft . . .
>
> (b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network . . . shall be guilty of the crime of computer trespass.
>
> (c) Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy. . . .
>
> (h) Criminal Penalties. (1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

On February 25, 2008, Wallace, expert in his craft,[17] as directed by Boback and on behalf of Tiversa, was seeking information for Tiversa and Boback to monetize. (Wallace, Tr. 1344).

On February 25, 2008, contrary to company policy, Rosalind Woodson, LabMD's billing manager, was running LimeWire on the desk top computer assigned to her. (CX 0001 at 7); (CX 0002 at 7); (CX 0704 (Boyle, Dep. at 57-64)); (CX 0730 (Simmons, Dep. at 10-11, 14-15, 99-100)). Wallace testified that on that date he was searching P2P networks for one of Tiversa's health insurance company clients and was able to download the 1718 file. (Wallace, Tr. 1372). Wallace testified that he downloaded the 1718 file from LabMD IP address 60.190.82.42. (Wallace, Tr. 1394).

Tiversa and Boback lacked authorization to obtain or disclose individually identifiable health information (including the 1718 File) via LimeWire or any other means. Since at least 1996, obtaining or disclosing such information without patient authorization was a felony. 42 U.S.C. § 1320d-6(a)(2)(prohibiting "obtaining"), (3) (prohibiting "disclosing"). Also, by taking the 1718 File off a LabMD hard drive without permission from the company, Tiversa and Boback committed criminal "computer theft," "computer trespass," and "computer invasion of privacy" under Georgia law. *See* Ga. Code Ann. § 16-9-93(a)-(c). Nevertheless, without patient or LabMD authorization or knowledge, Boback and Tiversa first took and then tried to monetize the 1718 File. .

Tiversa was a research partner to Dartmouth College, which was conducting research relating to data security in the health care industry. Tiversa aided Dartmouth's research by obtaining business-related records, including records containing sensitive patient information

[17] *See* (Wallace, Tr. 1337-40, 1372); (CX0 872 (Gormely, Dep. at 83); (RX 0541 (Boback, Dep. at 63-64, 100)).

belonging to health care providers, found on P2P networks and provided this information to Dartmouth College for its "Data Hemorrhages" article. (Johnson, Tr. 753-755); (CX 872 (Gormely, Dep. at 55-57)). In January 2008, Tiversa, using its technology, conducted searches on P2P networks using Dartmouth's search terms. (CX 382 at 000010). Although LabMD's 1718 file is included and discussed in Dartmouth's "Data Hemorrhages" article, there is no proof that Dartmouth obtained LabMD's 1718 File using its search terms combined with Tiversa's technology. (Johnson, Tr. 772-80); (CX 872 (Gormley, Dep. at 98-102)).

In April, 2008, months after Tiversa, using its technology, had concluded conducting its searches using Dartmouth's search terms, (RX 371); (CX 382 at 000010); (CX 872 (Gormley, Dep. at 69-71)), Johnson requested that Gormley provide him with more recently found information that would help "spice up" and "boost the impact" of his "Data Hemorrhages" article. (RX 483); (Johnson, Tr. 772-74). Neither Johnson nor Gormley deny that LabMD's 1718 file was provided to Dartmouth because of Johnson's request for "spice" to "boost the impact" of his report.

Without the knowledge or authorization of any patients or of LabMD, Tiversa and Gormley disclosed the 1718 File and all of its individually identifiable health information to Johnson. *See* (RX 483); (Johnson, Tr. 772-74, 779-80); (CX 0872 (Gormley, Dep. at 103)). Tiversa and Gormley violated 42 U.S.C. § 1320d-6(a)(2) by disclosing, and Johnson and Dartmouth violated 42 U.S.C. § 1320d-6(a)(3) by obtaining, the 1718 File.

Sometime in or around August 2009, FTC and Tiversa conspired and agreed to carry out an illegal scheme: The unlawful disclosure of the 1718 File (individually identifiable health information), wrongfully obtained by Tiversa for its own commercial advantage, to a front company called the "Privacy Institute," and then further disclosure of this information by the

front to FTC in response to a "prepackaged" civil investigative demand. (Wallace, Tr. 1353); (RX 541 (Boback, Dep. at 38-41)); (Wallace, Tr. 1362-65); (CX 0703 (Boback, Dep. at 142)); (RX 541 (Boback, Dep. at 37-38)); (RX 525 (Kaufman, Dep. at 20)). Without prior written authorization from each listed patient, Tiversa could not lawfully "disclose" the 1718 File to the Privacy Institute, and the Privacy Institute could not lawfully "obtain" it from Tiversa. *See* 42 U.S.C. § 1320d-6(a)(2), (3). Furthermore, the Privacy Institute was not a HIPAA "covered entity," so it could not lawfully disclose the 1718 File to FTC in response to the civil investigative demand without prior patient authorization, whether FTC and Tiversa agreed to the arrangement or not. *See* 42 U.S.C. § 1320d-6(a)(2), (3) (prohibiting unauthorized receipt or disclosure of individually identifiable health information); 42 CFR § 164.512(f)(1) (creating a regulatory "safe harbor" only for a "covered entity" to disclose individually identifiable health information subject to 42 U.S.C. § 1320d-6(a) pursuant to a lawful civil investigative demand).

During discovery, FTC told LabMD the following:

> Complaint Counsel . . . objects to Respondent's characterization that the "1,718 File" was "obtained" from LabMD. The evidence in this administrative proceeding does not support this characterization. For purposes of this response, Complaint Counsel understands the term "1,718 File" to mean the 1,718 page file owned by LabMD that Tiversa Holding Corp. found at four different IP addresses. . . . Complaint Counsel admits that: (1) as part of Complaint Counsel's Part II investigation of LabMD, it issued a CID to the Privacy Institute and received the 1,718 file, which has been produced at FTC-PRI-000001 – FTC-PRI-001719; and (2) as part of this administrative proceeding, it issued a subpoena duces tecum to Tiversa Holding Corp. and received four 1,718 files downloaded from four different IP addresses.

Complaint Counsel's Amended Response to LabMD's First Set of Requests for Admission (Numbers 1-20), No. 20 (Apr. 1, 2014) ("CCA").

It is not clear when FTC knew CX 0019 (the sole documentary evidence of "spread"), and Boback's testimony that the 1718 File had not been downloaded from a LabMD computer, were fabricated and false, respectively. *Compare* (Wallace, Tr. 1368-70); (Wallace, Tr. 1386-

88); (RX 541 (Boback, Dep. at 142-43)); (RX 541 (Boback, Dep. at 36-42)); (RX541 (Boback Dep. at 67)); (RX 525 (Kaufman, Dep. at 62)); (Van Druff, Tr. 1227). FTC never checked, using its "twenty-first century law enforcement tools" to verify Tiversa's claims. *See, e.g.*, (RX 525 (Kaufman, Dep. at 62)). Instead, Boback and CX0019 were the star witness and evidentiary centerpiece of Complaint Counsel's case, respectively, (Sheer, Tr. 16), and the opinions of Dr. Hill, Kam, and Van Dyke were each substantially based on this perjury and fabrication. (Wallace, Tr. 1367-70); (CX 740 (Hill, Rep. at 17)); (CX 0742 (Kam, Rep. at 19)); (Kam, Tr. 531-32, 542-46); (RX 523 (Van Dyke, Dep. at 106-07)).

What is clear, however, is that FTC knew from the start that:

- It was a felony for Tiversa to have "obtained" individually identifiable health information from LabMD and others in violation of 42 U.S.C. § 1320d-6(a)(2);
- It was a felony for Eric Johnson and Dartmouth to have "obtained" individually identifiable health information from Tiversa in violation of 42 U.S.C. § 1320d-6(a)(2), and that it was a felony for Tiversa to have disclosed this information in violation of 42 U.S.C. § 1320d-6(a)(3);
- That LabMD was a covered entity (as defined in the HIPAA privacy regulation described in 42 U.S.C. § 1320d–9 (b)(3)); and that
- FTC was encouraging and facilitating the felony violation of 42 U.S.C. §§ 1320d-6(a)(2), (3) through its Tiversa/Privacy Institute deal.

But FTC, disregarding the law, patient privacy, and the rights and interests of health care providers victimized by Tiversa, went (at best) willfully blind.

Complaint Counsel may not use evidence obtained illegally or wrongfully or any of the fruits thereof. *Knoll Assocs. v. FTC*, 397 F.2d 530, 537 (7th Cir. 1968); *see also Atl. Richfield*

Co. v. FTC, 546 F.2d 646, 651 (5th Cir. 1977). This is particularly true where it has abdicated its duty to investigate or corroborate third-party evidence. *United States v. Brown*, 500 F.3d 48, 56 (1st Cir. 2007) (authorities must at least "act with due diligence to reduce the risk of a mendacious or misguided informant"); *FTC v. Page*, 378 F. Supp. 1052, 1056 (N.D. Ga. 1974) (deterrence of governmental lawlessness served by application of the exclusionary rule regardless of the criminal or administrative nature of the proceedings); *see also Oliva-Ramos v. Att'y Gen. of the United States*, 694 F.3d 259, 272 (3rd Cir. 2012); *Donovan v. Sarasota Concrete Co*., 693 F.2d 1061 (11th Cir. 1982) (OSHA citation hearing); *In re Big Ridge, Inc*., 36 FMSHRC 1677, 1738-39, 2014 FMSHRC LEXIS 465 (F.M.S.H.R.C. June 19, 2014) (excluding tainted evidence); Richard M. Re, *The Due Process Exclusionary Rule*, 127 Harv. L. Rev. 1885 (2014) (exclusionary rule is truly a due process rule).

All of Complaint Counsel's evidence was direct "fruit" of the 1718 File and the felonious Tiversa/Privacy Institute government deal. (Sheer, Tr. 31). Consequently, CX 0307, the 1718 File, and all derivative evidence—that is, Complaint Counsel's entire case—should be excluded. *Knoll Assocs.*, 397 F.2d at 537.

The government's conduct is particularly egregious because FTC knew Tiversa to be a paradigmatic government "crony company" engaged in a pernicious form of "public competition" and rent-seeking, not merely an ordinary witness, informant, or whistle-blower. (CX 0679, Ex. 5 (Dissenting Statement of Comm'r J. Thomas Rosch, FTC File No. 1023099 (June 21, 2012))). Tiversa's business model depended on FTC targeting not hackers and cyber-thieves, but rather the unsuspecting doctors and laboratories who were their victims. For example, Wallace testified that Boback decided upon and approved all of the companies on CX 0307 to maximize Tiversa's profits in acquiring new customers. He hoped that when these

companies received letters from FTC they would call seeking Tiversa's services. (Wallace, Tr. 1362-63). In fact, Wallace testified that many companies appeared on CX 0307 because they refused to do business with Tiversa:

> Q. When a company refused to do business with Tiversa, did Boback have a certain reaction to that? . . .
>
> A. Usually it would be something to the effect of they – you know, they – I've heard this said many, many times, that, you know, **you think you have a problem now, you just wait.**

(Wallace, Tr. 1364-65) (emphasis added).

Wallace was instructed by Boback to "use any means necessary to let [companies on the list] know that an [FTC] enforcement action is coming down the line and they need to hire us or face the music, so to speak." (Wallace, Tr. 1363). Boback further instructed Wallace to scrub the list of all past clients: "The list was scrubbed of all clients in the past and future clients that we felt that there might be, you know. The prospect of doing business with them. Their information was removed." (Wallace, Tr. 1362-63).

This case proves Justice Alito's concern, that FTC can be "captured by entities over which it has jurisdiction," to be well-founded. *See N.C. State Bd. of Dental Exam'rs v. FTC*, 135 S. Ct. 1101, 1123 (2015) (Alito, J., dissenting).[18] The evidence is FTC did not maintain an

[18] The evidence is FTC and Tiversa began collaborating in 2007. (Wallace, Tr. at 1362). This collaboration was mutually beneficial. FTC used Tiversa to make it appear that Commission staff could obtain data security "wins." (Press Release, Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Fed. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015). And, as Wallace testified, Tiversa solicited clients accordingly. *See* (Wallace, Tr. 1362-1363). Throughout this proceeding, Complaint Counsel and FTC credulously relied on Boback, its star witness, and was exceedingly protective of Tiversa. *See* (Kaufman, Dep. at 62) ("I am basing that solely on the testimony of Mr. Boback"); RPFF ¶¶ 330 (Dr. Hill relies on Boback and Tiversa), 408-18, 431, 440-43 (Kam and Van Dyke rely on Boback/Tiversa); Order Denying Compl. Counsel's Mot. for Leave to Issue Subpoenas for Rebuttal Evidence (July 24,

appropriate "arm's-length" relationship with Tiversa. (Wallace, Tr. 1349-63); (RX 541 (Boback, Dep. at 38-41)); (RX 525, (Kaufman, Dep. at 62 ("as of November, 2013, the 1,718 file was still available on peer-to-peer networks . . . I'm basing that solely upon the testimony of Mr. Boback")). FTC also knew that it lacked legal authority to do the felonious Tiversa/Privacy Institute deal. But FTC decided it was above the law, and, apparently by some secret and unilateral decree, that Tiversa was too.

The primary function of the exclusionary sanction is to deter unlawful government conduct. *United States v. Janis,* 428 U.S. 433, 446 (1974). FTC's deal with Tiversa and the Privacy Institute resulted in felonious violations of 42 U.S.C. § 1320d-6 and was patently unlawful.[19] Therefore, exclusion is appropriate. *Accord Burdeau v. McDowell,* 256 U.S. 465, 476 (1921) (government could lawfully rely on stolen evidence only because it played no part in wrongfully obtaining same).[20]

2014); Compl. Counsel's Opp. to Mot. to Strike Tiversa's Notice of Info. at 1 (Nov. 14, 2014) ("the information contained within the Notice of Information is relevant to the determination of whether Mr. Wallace's testimony and a grant of immunity are in the public interest").

[19] This assumes, of course, that Complaint Counsel was blind-sided by the fact that CX0019 was a fake. However, there is ample evidence to suggest that Complaint Counsel may not have been utterly surprised. *Compare* CX0307 (showing origin of the 1718 File as Atlanta, Ga.), *with* CX0019. It is also hard to believe that for all of their contacts with Tiversa, FTC staff never asked where the 1718 File had come from prior to September 2013. Regardless, the felonious Tiversa/Privacy Institute deal is enough to exclude.

[20] Complaint Counsel has improperly relied on *Budreau* in the past. *See* Compl. Counsel's Opp. to Motion for Sanctions at 7 (Aug. 25, 2014). To begin with, *Budreau* is distinguishable because, through its complicity in the Privacy Institute scheme, FTC did play a direct part in violating HIPAA and wrongfully obtaining evidence. Once FTC learned Tiversa had obtained individually identifiable health information, the right and lawful thing to do would have been to inform HHS or the United States Attorney for the Northern District of Georgia of the need for action. Also, as the *Knoll* court suggested, 397 F.2d at 537, Justice Brandeis's dissent more accurately characterizes the current state of the law:

D. Jurisdiction Is Lacking.

Complaint Counsel has failed to establish jurisdiction.

First, FTC has wrongfully failed to demonstrate "ascertainable certainty" regarding the standards the Commission applies to distinguish between lawful and unlawful data security under Section 5. *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) ("the due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'") (citation omitted); *FTC v. Wyndham*, No. 14-3514, 2015 U.S. App. LEXIS 14839, *39-41 (3d Cir. Aug. 24, 2015). Without this, jurisdiction over LabMD is unlawful.

Second, *FTC v. Klesner*, 280 U.S. 19, 28 (1929), requires the Commission to prove this action is in the "public interest." *See also Am. Airlines, Inc. v. N. Am. Airlines, Inc.*, 351 U.S. 79, 83 (1956) ("[T]his Court has held that, under § 5, the Federal Trade Commission may not employ its powers to vindicate private rights and that whether or not the facts, on complaint or as developed, show the public interest to be sufficiently 'specific and substantial' to authorize a

---

> Plaintiff's private papers were stolen. The thief, to further his own ends, delivered them to the law officer of the United States. He, knowing them to have been stolen, retains them for use against the plaintiff. Should the court permit him to do so?
>
> That the court would restore the papers to plaintiff if they were still in the thief's possession is not questioned. That it has power to control the disposition of these stolen papers, although they have passed into the possession of the law officer, is also not questioned. . . . At the foundation of our civil liberty lies the principle which denies to government officials an exceptional position before the law and which subjects them to the same rules of conduct that are commands to the citizen. And in the development of our liberty insistence upon procedural regularity has been a large factor. Respect for law will not be advanced by resort, in its enforcement, to means which shock the common man's sense of decency and fair play.

Budreau, 256 U.S. at 476-77 (Brandeis, J., dissenting).

proceeding by the Commission is a question subject to judicial review.").[21] Absent evidence of unfairness under Section 5(a), and then any actual or certainly impending substantial injury under Section 5(n), Complaint Counsel has failed to prove a "specific and substantial" public interest in this proceeding. Rather, FTC's collusion with Tiversa suggests that the Commission's power has been employed primarily to vindicate a private right. *See* (Wallace, Tr. 1346-70, 1386-88); (CX 0703 (Boback, Dep. at 142)); (RX 541 (Boback, Dep. at 37-41)); (RX 525 (Kaufman, Dep. at 20)).

II. THE BRIEFING ORDER.

Section III(2) of the Order on Post-Trial Briefs directs Complaint Counsel to include a "discussion of the legal standards that apply to determining whether Respondent's data security practices as alleged in the Complaint are unreasonable" and findings of fact that "consider, address, and/or refer to data security requirements and practices during the relevant time period

---

[21] Complaint Counsel relies on *Klesner*, a pre-Section 5(n) case. CCPCL ¶ 31. However, it offers the government no comfort. In *Klesner*, the Supreme Court held that while the Federal Trade Commission exercises under Section 5 the functions of both prosecutor and judge, "the scope of its authority is strictly limited." 280 U.S. at 27. Among other things, a complaint may be filed only "if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public." *Id.* at 28. With respect to public interest, the Court ruled:

> [T]he mere fact that it is to the interest of the community that private rights shall be respected is not enough to support a finding of public interest. To justify filing a complaint the public interest must be specific and substantial. Often it is so, because the unfair method employed threatens the existence of present or potential competition. Sometimes, because the unfair method is being employed under circumstances which involve flagrant oppression of the weak by the strong. Sometimes, because, although the aggregate of the loss entailed may be so serious and widespread as to make the matter one of public consequence, no private suit would be brought to stop the unfair conduct, since the loss to each of the individuals affected is too small to warrant it.

Id. Complaint Counsel has not proven risk to competition, "flagrant oppression of the weak by the strong," or that "no private suit would be brought to stop the unfair conduct." In fact, class action and other cases arising from real data breach cases are filed frequently. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 24 (D.D.C. 2014) (citing cases)). Therefore, jurisdiction is lacking.

in this case." Complaint Counsel's pleadings exceed three hundred pages, but do not specify the prevailing data security standards applicable to LabMD's business during any given year (*e.g.*, 2005, 2007, or 2012), nor do they describe how LabMD's specific data security acts or practices violated them.

Section III(3) of the Order directs Complaint Counsel to "fully and clearly articulate . . . Complaint Counsel's theory of 'substantial injury' in this case, including without limitation: (1) the specific nature of the substantial injury or injuries asserted; (2) whether such asserted substantial injuries constitute present or future injuries; and, (3) as applicable, an assessment of the risk and/or likelihood of the asserted substantial injuries." Complaint Counsel has failed to do this.

After six years of inquisition, discovery, and trial, Complaint Counsel offers not a single consumer victim and no evidence of monetary loss, fraud, identity theft, harm, or injury to anyone. It presented no proof of present substantial injury to consumers, only unsubstantiated speculation of past and future injury. FTC's assessments of the risk and/or likelihood of future injury are nothing more than unfounded assumptions and guesses made by expert witnesses, of dubious provenance, who relied on Boback and CX 0019. (RX 525 (Kaufman, Dep. at 59, 67) ("likelihood" of harm dependent on expert testimony)); RPFF ¶¶ 330 (Dr. Hill relies on CX0019 and the claim of Robert Boback and Tiversa that the 1718 File was found in four (4) places: (CX 0740 (Hill, Rep. at 17 ¶ 46)) ("A list of the materials that I considered in reaching my opinions is attached to this report as Appendix B" including (CX 0019 (Tiversa: List of 4 IP Addresses where Insurance Aging File found)); (CX 0742 (Kam, Rep. at 19)); (Kam, Tr. 531-32, 542-46); (RX 523 (Van Dyke, Dep. at 106-07)))). In fact, the only evidence of injury, substantial or

otherwise, is to LabMD, its former employees, and the doctors and patients who relied on the company for fast, accurate, and cost-efficient cancer diagnostics.

A. Complaint Counsel Has Failed To Clearly Articulate Its Case.

LabMD is entitled to a clear articulation of the facts and law Complaint Counsel intends to use against it. *See* 5 U.S.C. § 554(b)(3); *Morgan v. United States*, 304 U.S. 1, 18-19 (1938) ("The right to a hearing embraces not only the right to present evidence but also a reasonable opportunity to know the claims of the opposing party and to meet them"); *Hatch v. Fed. Energy Regulatory Comm'n*, 654 F.2d 825, 835 (D.C. Cir. 1981).

Without knowing the legal standards Complaint Counsel believes applied at precise points between January 2005 and the present, and without a clear articulation of the government's "substantial injury" theory, LabMD cannot effectively defend itself and is thus deprived of due process. *Larche*, 363 U.S. at 442 ("When governmental agencies adjudicate or make binding determinations which directly affect the legal rights of individuals, it is imperative that those agencies use the procedures which have traditionally been associated with the judicial process."); *see also Wyndham*, 2015 U.S. App. LEXIS 14839 at *32-36 (distinguishing between "fair notice" in an Article III court and before an agency and noting the agency's heightened duty to provide regulated parties "fair warning of the conduct it prohibits or requires") (citations omitted).[22]

B. Section III(2): Complaint Counsel's Legal Standards.

[22] No common law court would entertain allegations of unlawful or tortious conduct over the span of a decade, as Complaint Counsel does here, without requiring the plaintiff to clearly articulate the legal standards that applied, the specific time that those standards applied, and the defendant's specific conduct that violated those standards. At a minimum, should Complaint Counsel finally articulate clear legal standards and a substantial injury theory on reply, LabMD should be given an opportunity to file a surreply to address same.

Complaint Counsel seems to nest what it considers controlling legal standards in Section 1.3 of its Proposed Conclusions of Law, but these are deficient.

1. Unlawful definition Section 5 "unfairness."

Complaint Counsel does not properly or consistently define the legal test for Section 5 "unfairness."

CCPCL ¶ 12 states that "[a]n unfair practice is defined as one that 'causes or is likely to cause substantial injury which is not reasonably avoidable by consumers . . . and not outweighed by countervailing benefits to consumers or to competition.'" CCPCL ¶ 14 states, somewhat differently, that "[t]he codification of unfairness established a cost-benefit analysis to evaluate whether practices are unfair." CCPCL ¶ 29 states, again somewhat differently, that "[a] practice is unfair if it causes or is likely to cause 'a small amount of harm to a large number of people, or if it raises a significant risk of concrete harm.'"

Complaint Counsel's Complaint and Post-Trial Brief ("CCPTB") state, again somewhat differently, that the test under Section 5 for unfairness is whether a given act or practice "caused or is likely to cause substantial injury to consumers." *See* Compl. ¶ 22; CCPTB at 65. Complaint Counsel also states, again somewhat differently, "that a practice, much less a sweeping set of practices as seen in this case, is likely to cause harm (sic) satisfies the unfairness analysis." CCPTB at 64. Finally, Complaint Counsel also states, yet again somewhat differently, that "unreasonable" data security practices are by definition "unfair" under Section 5. CCPCL ¶¶ 9, 10.

None of this is correct.

Section 5 is titled "Unfair methods of competition unlawful; prevention by Commission." This overriding statutory purpose provides the controlling interpretative context – competition

and protection of the markets must be the touchstone. *Yates v. United States*, 135 S. Ct. 1074, 1081-83, 1090 (2015).

Section 5(a) and Section 5(n) control here, and the Court should apply and construe them consistently, giving effect to both. *Mkt. Co. v. Hoffman*, 101 U.S. 112, 115-16 (1879) ("'[A] statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.' . . . [E]very part of a statute must be construed in connection with the whole, so as to make all the parts harmonize, if possible, and give meaning to each.") (citations omitted). The operative terms in these sections, including "unfairness," "causes," "likely," and "substantial injury," are undefined and so a common meaning construction is proper. *FDIC v. Meyer*, 510 U.S. 471, 477 (1994). These terms define the outer limits of the Commission's authority, and statutory construction must account for "the specific context in which that language is used, and the broader context of the statute as a whole." *Yates*, 135 S. Ct. at 1081-83.[23]

First, Section 5(a) provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a). This means, as a predicate matter, that Complaint Counsel must prove by a preponderance of the evidence that the data security acts and practices identified in the Complaint as "unfair" are marked by injustice, partiality, or deception. *LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1200 (11th Cir. 2010) (citation omitted); *see also* S.

[23] Consequently, the "unfair" act or practice must have a generalized impact on consumers or competition because the lawful exercise of FTC's unfairness authority must be grounded in the "protection of free and fair competition in the Nation's marketplaces." *See United States v. Am. Bldg. Maint. Indus.*, 422 U.S. 271, 277 (1975); 15 U.S.C. § 45; *Yates v. United States*, 135 S. Ct. 1074, 1081-83, 91 (2015) (citations omitted); *In re Int'l Harvester Co.*, 1984 FTC LEXIS 2, at *248 (F.T.C. Dec. 21, 1984) ("conduct must be harmful in its net effects" because economic issues are the FTC Act's "proper concern").

Rep. No. 74-1705, at 2 (1936) ("[T]he Commission should have jurisdiction to restrain unfair or deceptive acts and practices which deceive and defraud the public generally."); *id.* at 3 ("Under the proposed amendment, the Commission would have jurisdiction to stop the exploitation or deception of the public"); *accord Wyndham*, 2015 U.S. App. LEXIS 14839 at *17-19, *54 (noting dictionary definition of "unfairness" and that the "three requirements in § 45(n) may be necessary rather than sufficient conditions of an unfair practice.").[24]

Second, assuming an act or practice is "unfair," then, and only then, is a Section 5(n) analysis appropriate to determine unlawfulness. Section 5(n) provides:

---

[24]According to the Third Circuit:

> Wyndham argues . . . that the three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions of an unfair practice and that the plain meaning of the word "unfair" imposes independent requirements that are not met here. Arguably, § 45(n) may not identify all of the requirements for an unfairness claim. (While the provision forbids the FTC from declaring an act unfair "unless" the act satisfies the three specified requirements, it does not answer whether these are the only requirements for a finding of unfairness.). . . . Wyndham argues that a practice is only "unfair" if it is "not equitable" or is "marked by injustice, partiality, or deception." Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.
>
> We recognize this analysis of unfairness encompasses some facts relevant to the FTC's deceptive practices claim. But facts relevant to unfairness and deception claims frequently overlap. We cannot completely disentangle the two theories here. The FTC argued in the District Court that consumers could not reasonably avoid injury by booking with another hotel chain *because Wyndham had published a misleading privacy policy that overstated its cybersecurity.*

Wyndham, 2015 U.S. App. LEXIS 14839 at *15-17 (citations omitted) (emphasis added). Notably, FTC has not accused LabMD of any sort of unlawful deception here. *Compare* Compl. ¶10, *and* CCA at No. 4 (no claim of deception in Complaint), *with Wyndham*, 2015 U.S. App. LEXIS 14839 at *17 ("A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise . . . and retains the profits of their business.").

> The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

Not every "unfair" act or practice is "unlawful." Only an "unfair" act or practice under Section 5(a) that is (1) proven to "cause" now, or to be "likely to cause" in the future (2) "substantial injury" to consumers, (3) which is not "reasonably avoidable" by consumers themselves, and (4) is not outweighed by countervailing benefits to consumers or to competition, can be so declared. The Commission may not rely on undifferentiated allegations of "public harm" in an unfairness case. Instead, it must demonstrate present or a likelihood of future "substantial injury" to consumers.[25] *Cf. Wyndham,* 2015 U.S. App. LEXIS 14839 at *7-10 (on three occasions in 2008 and 2009 hackers accessed Wyndham's network and the property management systems of Wyndham-branded hotels obtaining payment card information from over 619,000 consumers, which resulted in at least $10.6 million in fraud loss and "time and money resolving fraudulent charges and mitigating subsequent harm") (citations omitted).

Section 5(n) imposes a very heavy burden on Complaint Counsel, and on the Commission, to declare an "unfair" act or practice "unlawful." This was intentional—15 U.S.C. § 45(n) was enacted to cabin, not expand, the Commission's unfairness authority. *See* S. Comm. Rep. 103-130, FTC Act of 1993 (Aug. 24, 1993) (stating that "[t]his section amends section 5 of the FTC Act to limit unlawful 'unfair acts or practices' to only those which cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers

[25] Commission leadership was confused about the applicable standard. *See* (RX525 (Kaufman, Dep. at 80-82). This confusion is reflected in Complaint Counsel's pleadings.

themselves and not outweighed by countervailing benefits to consumers or competition" and that "substantial injury" is "not intended to encompass merely trivial or speculative harm"); 140 Cong. Rec. H6162 (daily ed. July 25, 1994) (statement of Rep. Moorehead) ("Taken as a whole, these new criteria defining the unfairness standard should provide a strong bulwark against potential abuses of the unfairness standard by an overzealous FTC--a phenomenon we last observed in the late 1970's"). It should be construed accordingly.

Complaint Counsel does not define what "cause," or "likely to cause," or "substantial injury" mean as a matter of law and then apply those definitions to the facts of this case, as this Court asked it to do. Instead, it does violence to Section 5(n)'s plain language, severs it from statutory context and Congressional intent, and effectively expands FTC's power by conferring on the Commission an unbounded discretion to declare any act or practice unlawful through the mechanism of an opaque, standard-less "cost/benefit analysis."[26] For example, Section 5 does not define or equate "unfairness" with "unreasonableness" as Complaint Counsel claims. Congress never used the word in this way, not in Section 5(a) and not in Section 5(n). "Reasonableness" only appears in Section 5(n) with respect to the substantial injury analysis, when Congress required a determination whether a given injury was "not reasonably avoidable by consumers themselves" for determining substantiality.

Given the plain language of Section 5(a) and (n), the controlling legal test in this case can only be whether a challenged data security act or practice is "unfair" under the plain meaning of the word, and if so, whether the unfair act or practice may be declared unlawful because it

[26] Given that Complaint Counsel introduced no competent evidence suggesting the Commission ever undertook a "cost/benefit analysis" in this case (standard-less or otherwise), it failed to comply with Section 5(n). Therefore, any order against LabMD that is issued under Section 5 will violate due process, be arbitrary and capricious, and violate the APA.

causes, or is likely to cause, substantial consumer injury that is not outweighed by countervailing benefit. Judgments on "reasonableness" made by experts paid for by the government years after the fact do not substitute for statutorily-mandated proof.

2. Unlawful failure to apply HIPAA "covered entity" medical industry standards, exercise § 57 rulemaking authority and provide fair notice.

On August 29, 2013, FTC filed a Complaint and Notice Order against LabMD alleging that it "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security" without citing specific data security regulations, requirements or standards LabMD had violated. *See* Compl. ¶10.

On September 25, 2013, when Complaint Counsel was asked by this Court whether "the Commission issued guidelines for companies" or "is there something out there for a company to look to," it admitted that "[t]here is nothing out there for a company to look to." Tr. of Initial Pretrial Conference at 9, *In re LabMD, Inc.*, No. 9357 (F.T.C. Sept. 25, 2013).

Complaint Counsel was later asked by this Court if "there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?," and Complaint Counsel answered "No." Tr. of Initial Pretrial Conference at 10, 20-22. *But see* (Sheer, Tr. at 18-19).

On April 1, 2014, Complaint Counsel admitted that FTC's "Guides for Business" relating to data security, including the "Peer-to-Peer File Sharing: A Guide for Business" and "Protecting Personal Information: A Guide to Business," are not legally binding upon any U.S. company, and that the SANS Institute does not have lawful authority to create enforceable data security standards. CCA at Nos. 11, 13.

On April 14, 2014, more than six years after Tiversa stole the 1718 File, and more than four years after FTC began its inquisition of LabMD, the Commission's designee, Daniel

Kaufman, testified to the legal standards that governed LabMD's medical data security acts and practices during the relevant time. Here, for the first time, FTC officially advised LabMD that it was being held responsible, retroactively, for compliance with FTC's "educational materials," "industry guidance pieces," the "Guides for Business," complaints, consent orders, NIST and SANS Institute publications, financial industry regulations, and even speeches and Congressional testimony, as if these things *were* legally binding data security standards. (RX 532 (Kaufman, Dep. at 163-71, 208-09, 211-13)); *see also* CCPCL ¶¶ 127-30 (citing rules promulgated under the Graham-Leach Bliley Act, FTC "Guide for Business" and "other sources" such as NIST, SANS and US CERT without specifying specific and binding requirements).

On May 19, 2014, the Commission disavowed Complaint Counsel's statements and admissions contradicting Kaufman. According to the Commission, "[j]ust because Complaint Counsel has made particular statements or taken certain positions does not necessarily mean the Commission has adopted those positions. . . . [T]he Commission is not bound by characterizations employed by Complaint Counsel[.]" *See* Comm'n Order Denying Resp't LabMD's Mot. for Summ. Decision at 8 (F.T.C. May 19, 2014).

On May 20, 2014, Complaint Counsel said as follows:

> JUDGE CHAPPELL: This defense in depth you're talking about, is this a law, regulation or guideline that's out there for everybody to see?
>
> MR. SHEER: This is the practice that information security professionals use and have used for many, many years. It is available in many forms, including in standards that have been produced by the government, the National Institute of Science and Technology, as well as many other private organizations that supply information to –
>
> JUDGE CHAPPELL: I'm talking about government only. My question goes to the government only.
>
> MR. SHEER: Yes.
>
> JUDGE CHAPPELL: Law, regulation or guideline published by the government.

> MR. SHEER: There are guidelines that have been published, for example, having to do with the security of health information that have these same basic concepts built into them. They're not always called defense in depth, but there are a series of standard steps, which we're going to talk about, that will illustrate what "defense in depth" means.
>
> JUDGE CHAPPELL: These guidelines have been published. Can you cite me to them right now?
>
> MR. SHEER: I can point you to the -- I can point you to pieces of it right now. I can point you to the HIPAA security rule which has -- which lays out in some detail what defense in depth requires.
>
> JUDGE CHAPPELL: Did you say HIPAA?
>
> MR. SHEER: I did.

(Sheer, Tr. at 18-19).

The day before, however, the Commission reaffirmed its position that "FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations" and that "this case has nothing to do with HIPAA." *See* Comm'n Order Denying Resp't LabMD's Mot. for Summ. Decision at 5.

Given its own confusion (when Complaint Counsel began this case it did not know the Commission even had data security standards, other than 15 U.S.C. § 45(a), much less where they could be found), FTC cannot reasonably or even plausibly contend LabMD had constitutionally-sufficient notice of FTC's standards and/or should have known where to go to find them, beginning in January 2005, and every year thereafter. *See* (Daugherty, Tr. 1028 ("the FTC hovering over the company all those years. . . . We were diagnosing cancer and trying to run a medical facility, and we can't get an answer about what we're supposed to do [regarding data security]. And we're being treated like we don't care or we're–and what we're getting is brushstrokes of consent decrees and we're getting, you know, read–read this information, and there's no straight answer.")); *see also* (RX 492 (Daugherty, Dep. at 141-42 ("We started

shopping for–we were, we were very concerned by lack of Government specifics and rules and standards, so we always tried and felt we always did comply with all regulations, but it, there was no specific standards, so we–I decided to shoot for as high as we could go. We had a hard time getting companies to, that were in a marketplace as a small business that we were or a small medical business for software solutions.”))).

In fact, Complaint Counsel has offered no evidence that LabMD could reasonably have been expected to know in 2005, or 2008, or 2012, that it was expected to consult FTC commissioners’ “speeches,” “business education materials,” “Congressional testimony,” “consent decrees” or “blogs” to determine compliance obligations. (RX 532 (Kaufman, Dep. at 188-92); *accord Wyndham*, 2015 U.S. App. LEXIS 14839 at *50-51 n.23 (“We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted.”) As Dr. Hill testified:

> Q. (By Mr. Sherman) You’ve also indicated time and again that guidelines should be in writing; correct?
>
> A. (By Dr. Hill) Yes.
>
> Q. And you’ve stated that the reason that it’s so important for these to be in writing is because it creates awareness amongst not only IT professionals but also the employees who are expected to comply; correct?
>
> A. Yes.
>
> Q. That it creates continuity in terms of the enforcement and knowledge of those policies as turnover may occur; correct?
>
> A. Yes.
>
> Q. So, Professor Hill, do you think that it’s important or just as important for an enforcement agency to put its data security expectations in writing for the very same reasons?
>
> A. Excuse me. Did you say enforcement agency?

Q. Yes. Such as the FTC, the government.

A. I think–yes.

(Hill Tr. 301-02). Consequently, FTC abused its discretion by proceeding through agency adjudication rather than through its 15 U.S.C. § 57a authority to prescribe interpretative rules and general policy statements. *Accord Ford Motor Co.*, 673 F.2d at 1008; *NLRB v. Bell Aerospace Co.*, 416 U.S. 267 (1974).

In any event, due process requires FTC to test LabMD's data security acts and practices against the medical industry standards then in effect for HIPAA "covered entities" of its size and nature during the period between January 2005 and either July 2010, (the outer bound of Dr. Hill's opinion) or the present, as appropriate. *S&H Riggers & Erectors Inc. v. OSHRC*, 659 F.2d 1273, 1283 (5th Cir. 1981); *Fabi Construc. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1083 (D.C. Cir. 2007); *Ensign-Bickford Co. v. OSHRC*, 717 F.2d 1419, 1422 (D.C. Cir. 1983) (industry standards for the pyrotechnic industry applied); *accord FTC v. Accusearch, Inc.*, No. 06-105, 2007 U.S. Dist. LEXIS 74905, at *18 (D. Wyo. Sept. 28, 2007) ("Defendants were and are in the business of information brokering and can reasonably be expected to know what information is legally available" to their business). The applicable standards, their sources, and the relevant time during which they applied, must be specified.[27] However, the evidence in this case is that FTC did not do so.

LabMD, and all other HIPAA "covered entities," must comply with 42 U.S.C. § 1320d-2 and the HIPAA Security Rule, 68 Fed. Reg. 8334 (Feb. 20, 2003) (the "Security Rule"). The

[27] The Commission's decision denying LabMD's Motion to Dismiss on fair notice grounds was issued before discovery commenced in this case, on January 16, 2014. *See* Comm'n Order Denying Resp't LabMD's Mot. to Dismiss at 1 (Jan. 16, 2014) (the "MTD Order"). In other words, this Order was aimed at a facial challenge, not the as-applied challenge that is raised now. Consequently, this Court may rule on the matter.

Security Rule sets medical data security standards and specifies thirteen mandatory specifications for implementing those standards based on (1) the expertise of Federal security experts and generally accepted medical industry practices, (2) the recommendations of the National Research Council, and (3) the Strategic National Implementation Process developed under the auspices of the Workgroup for Electronic Data Interchange, an organization named in HIPAA to consult with HHS. 68 Fed. Reg. at 8336-37. HHS specified no less than ten specific "guiding principles" it used for standard selection, including improving efficiency and effectiveness of the health care system, consistency and uniformity with other HIPAA standards, and simplicity, precision and clarity. *Id.* at 8371-72. In Appendix A to Subpart C of Part 164, HHS even provided a "Matrix" for reference purposes. *Id.* at 8380.

Complaint Counsel claims LabMD failed to implement "reasonable security" in that it (1) failed to develop, implement or maintain a written security program; (2) did not use readily available measures to identify risks, including measures to detect and prevent unauthorized access; (3) did not prevent employees from "accessing" (sic) personal information not needed to perform their jobs; (4) did not adequately train employees; (5) did not establish and implement password policies; (6) did not update operating systems; and (7) "did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks." CCPTB at 14-15. However, this bill of particulars is devoid of references to medical industry data security standards and contains no temporal boundaries or specifications whatsoever.

Instead of tying its claims to actual practices and actual standards in effect during a specific period during the relevant time, Complaint Counsel says applicable legal standards are to be found in a Commission "statement" (CCPCL ¶ 15), in unspecified and undated

recommendations from NIST, SANS and other unnamed "information technology training institutes" (CCPCL ¶17), and in FTC "complaints and consent decrees" (CCPCL ¶¶ 18-20). *See generally* (RX 532 (Kaufman, Dep. at 173-76, 211-13) (describing sources of materials that "businesses can look at to get a better sense of how the Commission evaluates what is reasonable data security")). To declare LabMD in violation of Section 5, Complaint Counsel uses these "standards" to create "requirements" apparently based solely on Dr. Hill's say-so. *See* CCPTB at 23-27, 30, 31, 41, 47-49, 51-56 (citations omitted); *see also* (RX 525 (Kaufman, Dep. at 67 (deferring to Dr. Hill regarding likelihood of harm continuing through the present))). For example, Kaufman testified:

> A. (By Mr. Kaufman) In this case, the Bureau has alleged that LabMD should have had a comprehensive information security program in place.
>
> Q. (By Mr. Sherman) Is the Bureau's definition of a comprehensive information security program the same as the definition . . . as set out in Dr. Raquel Hill's expert witness report?
>
> A. I am not aware of a specific definition we have used for comprehensive information security program, but I can certainly look at her definition and see if it seems consistent with my general understanding.

(RX 532 (Kaufman, Dep. at 168).

This is unfair, unreasonable, and unlawful. First, "public statements" and "educational materials" are not constitutionally adequate standards. *See Am. Bus. Ass'n. v. United States*, 627 F.2d 525, 529 (D.C. Cir. 1980); *Wilderness Soc'y v. Norton*, 434 F.3d 584, 595-96 (D.C. Cir. 2006). Complaints and consent decrees are not sufficient either. 15 U.S.C. § 45(m)(2); *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008) ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp. v. Abrams*, 897 F.2d 34, 36 (2d Cir. 1990) ("[u]nlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement"); *Trans Union Corp. v. FTC*, 245 F.3d 809, *on denial of reh'g,*

267 F.3d 1138 (D.C. Cir. 2001); *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976); Jan Rybnicek & Joshua Wright, *Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Formal Agency Guidelines*, 21 Geo. Mason L. Rev. 1287, 1305(2014) ("[T]he Commission does not treat its settlements as precedent, meaning that past decisions do not necessarily indicate how the agency will apply Section 5 in the future."). "[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'" *Fox Television*, 132 S. Ct. at 2317. (citation omitted).

Second, FTC may not seek to enforce statements of general policy and interpretations of general applicability unless they are first published in the Federal Register. 5 U.S.C. § 552(a)(1)(D); 15 U.S.C. § 57(a); *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 754 (D.C. Cir. 2001); *Am. Bus. Ass'n*., 627 F.2d at 529; *Wilderness Soc'y*, 434 F.3d at 595-96. 15 U.S.C. § 57a(a)(1) authorizes the Commission to prescribe "interpretive rules and general statements of policy" with respect to unfair acts or practices in or affecting commerce (within the meaning of 15 U.S.C. § 45(a)), and "rules" which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce. While the Commission promulgates general statements of policy at 16 C.F.R. Part 14, there are none for medical data security. While the Commission promulgates guides for business at 16 CFR Part 251, there are none for medical data security. And, while the Commission promulgates trade rules for business at 16 CFR Part 455, there are none for medical data security. The "standards" testified to by Kaufman, and cited by Complaint Counsel, cannot by definition be interpretative rules or general statements of policy, and binding on LabMD, because the Commission did not issue them in compliance with either the APA or 15 U.S.C. § 57.

Third, Complaint Counsel previously averred that FTC does not have objective data security standards for the medical industry and HIPAA "covered entities." *See* (RX 0526) (none of the documents available on the Internet on the FTC's 'Bureau of Consumer Protection Business Center's' self-described 'Legal Resources' website, including but not limited to consent orders and FTC 'Guides for Business,' establish specific data-security practices that any U.S. company must adopt to comply with 15 U.S.C. § 45(a),(n)). Due process requires that lawful Section 5 data security "standards" applied to LabMD must be both relevant to the medical field and of a type and nature that restrict the Commission's discretion and constrain government authority, and provide sufficiently specific limits on FTC's enforcement discretion "'to meet constitutional standards for definiteness and clarity.'" *City of Chicago v. Morales,* 527 U.S. 41, 63-64 (1999) (citation omitted); *see also Ensign-Bickford Co.*, 717 F.2d at 1422.

The Commission may not lawfully require LabMD (or other HIPAA "covered entities") to monitor FTC's website and sift through the footnotes of Congressional testimony, Spanish language flyers, consent orders with title companies, drug stores or big box retailers, or rules relating to financial institutions, prospecting for that golden nugget of data security that FTC, in its sole discretion and years after the fact, might deem relevant. *See, e.g.*, (Daugherty, Tr. 1028 ("there's no straight answer")); (RX 492 (Daugherty, Dep. at 142 ("there was [*sic*] no specific standards . . .")). But this is the heart of Complaint Counsel's case. *See* CCPCL ¶¶ 18-20. Instead, LabMD was entitled to *ex ante* ascertainable certainty of FTC's expectations. *See Wyndham*, 2015 U.S. App. LEXIS 14839 at *40 ("[A]t oral argument we asked Wyndham whether the cases cited in its brief that apply the 'ascertainable certainty' standard—*all of which involve a court reviewing an agency adjudication* . . . .") (emphasis added) (citing *Fox Television*, 132 S. Ct. at 2307 (vacating an FCC adjudication for lack of fair notice of an agency

interpretation)); *PMD Produce Brokerage Corp. v. Dep't of Agric.*, 234 F.3d 48 (D.C. Cir. 2000) (vacating the dismissal of an administrative appeal issued by a Judicial Officer in the Department of Agriculture because the agency's Rules of Practice failed to give fair notice of the deadline for filing an appeal); *Gen. Elec. Co.*, 53 F.3d 1324 (vacating an EPA adjudication for lack of fair notice of the agency's interpretation of a regulation).

Finally, the Third Circuit's opinion in *Wyndham* strongly suggests that FTC's case against LabMD fails to satisfy constitutional notice requirements on an "as-applied" basis. This case is not entirely on point: It involves judicial construction of § 45, not an agency adjudication, and unlike the defendant there, LabMD *has* argued that its cybersecurity practices between January 2005 and July 2010 survive a reasonable interpretation of the cost-benefit analysis required by § 45(n). *Compare Wyndham*, 2015 U.S. App. LEXIS 14839 at *46, *and infra* at § I(C)(2) (discussing injury), *with* RPFF ¶¶ 279-88, 493-94, 500.

However, *Wyndham* is instructive because the grounds for the Third Circuit's ruling that Wyndham had fair notice are not present here.

> Wyndham's as-applied challenge falls well short given the allegations in the FTC's complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, did not use *any* encryption for certain customer files, and did not require some users to change their default or factory-setting passwords *at all*. . . . Wyndham's as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis. That said, we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis.

2015 U.S. App. LEXIS 14839 at *47-48 (citations omitted). Here, by contrast, LabMD was regulated at all times by HIPAA and had firewalls, IP address restrictions, HIPAA-appropriate encryption and a host of other data security policies in place. *See, e.g.*, RPFF ¶¶ 124, 126, 132,

137, 159, 167, 175, 246, 271, 279-86, 333, 336, 356, 368, 493-94; (Daugherty, Dep. at 135-46). FTC, without citing any standards that would have provided LabMD prior or contemporaneous notice of what Section 5 permitted or prohibited, said for the first time in August 2013 that LabMD's January 2005, to July 2010, data security practices were unlawfully weak.

Also, unlike Wyndham, LabMD did not have multiple and actual data breaches of its patient (customer) information. The Complaint cites two "security incidents" (not breaches) one involving the 1718 File, stolen by Tiversa in February 2008, and the paper Day Sheets. Compl. ¶¶ 17-21. None of LabMD's patients suffered identity theft or other harm proving, according to Complaint Counsel, that LabMD never had a data breach. (Kam, Tr. 532 (in *every* data breach in his professional experience a victim has come forward with an injury)). Fairly read, *Wyndham* stands for the proposition that FTC denied LabMD fair notice.

3. Unlawful risk of conflict with HIPAA.

FTC may proceed under Section 5 if an allegedly unfair practice violates some other law that it lacks authority to enforce. MTD Order at 13 (citations omitted). FTC perhaps could have alleged that LabMD violated HIPAA, and used that violation as grounds for an unfairness claim, though it chose not to do so. *See* MTD at 12. However, FTC may not proceed against LabMD under Section 5 if there is a risk that doing so will result in conflicting guidance, requirements or standards of conduct with 42 U.S.C. § 1320d-2 and the Security Rule. *See Credit Suisse Secs. LLC v. Billing*, 551 U.S. 264, 272-73 (2007); MTD Order at 12-13.

The Commission ruled that it does not enforce HIPAA and does not seek to do so. MTD Order at 12. It also ruled that there was no risk of conflicting guidance, requirements or standards. *Id.* at 13. However, Complaint Counsel's pleadings contain facts from trial and discovery that were not before the Commission when it ruled that there was no risk of conflict between HIPAA and the FTC Act, that demonstrate there is indeed a serious risk (in fact, a

certainty) of conflicting guidance, requirements or standards of conduct if FTC applies Section 5 in this case. Because these facts were not before the Commission when it issued the MTD, this Court is not bound by that ruling.

Also, in its May 19, 2014 ruling on LabMD's Motion for Summary Decision, the Commission ruled:

> [T]he facts LabMD alleges about HIPAA could be "material" . . . only if LabMD were correct that, as a matter of law, the Commission could not hold LabMD liable under Section 5 if its data security practices complied with HIPAA standards. But that legal argument is now foreclosed. We held in the Order denying LabMD's Motion to Dismiss that HIPAA does not "trump" Section 5 and that LabMD therefore "cannot plausibly assert that, because it complies with [HIPAA] it is free to violate" requirements imposed independently by Section 5 of the FTC Act.

Comm'n Order Denying Resp't LabMD, Inc.'s Mot. for Summ. Decision at 5 (citations omitted). However, the issue before this Court is not whether compliance with HIPAA is a "free pass" to violate Section 5; rather, it is whether Section 5 requirements created through the testimony in this case pose a risk of conflict with previously promulgated HIPAA regulations. *See Billing*, 571 U.S. at 272-73. The Commission has not decided this issue, and so this Court may resolve the matter.

FTC created a new regulatory regime using Dr. Hill, who had no medical industry experience, and applied it retroactively to find LabMD deficient, creating a clear risk of conflict with HIPAA. For example, Dr. Hill rejected scalability for a one-size-fits-all approach. *Compare* RPFF ¶¶ 330-340 (citations omitted); 42 U.S.C. § 1320d-2(d) (The Secretary shall adopt security standards that take into account "(i) the technical capabilities of record systems used to maintain health information; (ii) the costs of security measures; . . . and (v) the needs and capabilities of small health care providers[.]"); 68 Fed. Reg. at 8359 ("one of the security standard's basic premises . . . is scalability"). The Security Rule does not require "defense in

depth," as Dr. Hill does. RPFF ¶ 348; (Hill, Tr. 235-36).[28] Also, the mandatory and generally applicable standards cited by Complaint Counsel are not flexible and "technology neutral" as HIPAA requires.[29]

What Dr. Hill demands is facially more prescriptive than HIPAA and/or inconsistent with HHS regulations and guidance, including encryption at rest (an addressable requirement of 42 CFR § 164.312(a)(1)), encryption in transit (an addressable requirement of 42 CFR § 164.312(e)(1)), intrusion detection (not addressed specifically by the Security Rule), virus protection (an addressable requirement of 42 CFR § 164.308(a)(5) (ii)(B)), firewalls (not addressed specifically by the Security Rule), penetration testing (not addressed by the Security Rule), and file integrity monitoring (not addressed specifically by the Security Rule). There is

---

[28] Hill and FTC cite to the SANS Institute as a source of authoritative data security guidance. *See, e.g.*, CCPCL ¶ 130. This is what SANS has to say about "defense in depth":

> Businesses and Information Technology Security Professionals have spent a tremendous amount of time, money and resources to deploy a Defense in Depth approach to Information Technology Security. Yet successful attacks against RSA, HB Gary, Booz, Allen & Hamilton, the United States Military, and many others are examples of how Defense in Depth, as practiced, is unsustainable . . . ."

See Prescott Small, SANS Institute, "Defense in Depth: An Impractical Strategy for a Cyber World" at 1 (Nov. 14, 2011) *available at* http://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896.

[29] *Compare* CCPTB at 25 (mandating "automated scanning tools"), 26-27 (mandating "penetration tests"), 31 (mandating more than "antivirus programs, firewall logs and manual computer inspections"), 36 (mandating firewall technology), 46 (mandating two-factor authentication), 50-51 (mandating software technology), 56-57 (mandating hardware firewalls located at the network perimeter) *and* CCPCL ¶¶ 127 (citing "Safeguards Rule" not HIPAA), 130 (citing "NIST, SANS and US CERT" not HIPAA), 133 (mandating "biennial assessments and reports for twenty years from a 'qualified'….third party professional" contrary to HIPAA), 146-150 (mandating notice HIPAA does not require, including notice to insurance companies), *with* 68 Fed. Reg. at 8337 (The Security Rule does not "describe mandatory measures"), 8371 (describing guiding principles for data standard selection including consistency with other HIPAA standards, and avoidance of cost and burden), 8376-81 (setting standards) *and* 45 CFR §§ 164.400-414 (the HIPAA breach notification rule, providing detailed instructions and criteria for notification that differ from FTC's proposed relief).

no evidence that the controls demanded by Dr. Hill, such as encryption at rest, are generally adopted across the industry.

Also, FTC charges LabMD with keeping too much patient information, contrary to the practices of "IT professionals." CCPTB at 41 (citations omitted). This claim nicely illustrates the absurdity of the government's case. Medical record retention is extensively regulated. For example, AMA Code of Medical Ethics Op. No. 7.05 - Retention of Medical Records provides:

> Medical considerations are the primary basis for deciding how long to retain medical records. For example, operative notes and chemotherapy records should always be part of the patient's chart. In deciding whether to keep certain parts of the record, an appropriate criterion is whether a physician would want the information if he or she were seeing the patient for the first time[.]

Available at http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion705.page. Under Georgia law, "[a] provider [such as LabMD] having custody and control of any evaluation, diagnosis, prognosis, laboratory report, or biopsy slide in a patient's record shall retain such item for a period of not less than ten years from the date such item was created." Ga. Code Ann. § 31-33-2. Medicare requires record retention for at least five years. *See* 42 C.F.R.§ 482.24(b). Without reference to these specific standards, and then cross-checking each patient record to the standard, FTC could not, by any lawful measure, possibly conclude LabMD kept too much patient data for too long.

Additionally, Congress limited FTC's authority over breach notification to vendors of personal health records and their third party service providers in § 13407 of HITECH while LabMD and other HIPAA covered entities are subject to the HIPAA breach notification rule, 45 CFR §§ 164.400-414. Perversely, Complaint Counsel aims to end-run Congress by using the Notice Order to expand FTC's breach notification authority and swallow HIPAA whole. *See* CCPCL at 146-152.

In finding the more specific securities laws impliedly precluded application of the more general antitrust laws, the Supreme Court identified three factors: (1) the securities law "gave the SEC direct regulatory power over exchange rules and practices with respect to the fixing of reasonable rates of commission"; (2) the SEC had actively regulated; and (3) without antitrust immunity, "the exchanges and their members" could be subject to "conflicting standards." *Billing*, 551 U.S. at 272-73 (citation omitted). HIPAA gave HHS direct regulatory power over medical data security, HHS has actively regulated, and the evidence is that FTC's action in this case has placed LabMD at risk of "conflicting standards" in a field that is highly regulated by federal, state, and industry authorities. Consequently, FTC is precluded from the exercise of Section 5 authority against LabMD. *Id.*

C. Section III(3): Theory of "substantial injury."

Complaint Counsel was required to "fully and clearly articulate" its theory of "substantial injury" in this case, including without limitation: (1) the specific nature of the substantial injury or injuries asserted; (2) whether such substantial injuries constitute present or future injuries; and (3) as applicable, an assessment of the risk and/or likelihood of the asserted substantial injuries. Pre-Trial Briefing Order at § III(3). Complaint Counsel did not do this, again leaving LabMD and this Court to guess at FTC's case.

As a general matter, Complaint Counsel should be required to prove at least something more than an Article III "injury in fact," that is, the invasion of a legally protected interest which is concrete and particularized and actual or certainly impending, not conjectural or hypothetical. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147-48 (2013); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 24 (D.D.C. 2014); *cf. Wyndham*, 2015 U.S. App. LEXIS 14839 (FTC alleged three actual data breaches over a period of years

leading to the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss). An increased risk of injury is plainly different from certainly impending harm, and certainly impending injury is what the law demands. *See Clapper*, 133 S. Ct. at 1148. This is not a high bar. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Yet Complaint Counsel has failed to clear it. *Accord Reilly v. Ceridian Corp.*, 664 F.3d 38, 44 (3rd Cir. 2011); *see also Wyndham*, 2015 U.S. App. LEXIS 14839 at *45-48.

To be "substantial," the injury must be suffered by some significant number of consumers generally and/or be shown to implicate or affect free and fair competition. 15 U.S.C. § 45(n); *Yates*, 135 S. Ct. at 1082-83, 1085 ("[W]e rely on the principle of *noscitur a sociis*—a word is known by the company it keeps—to 'avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving unintended breadth to the Acts of Congress.'") (citation omitted); *In re Int'l Harvester Co*., No. 9147, 1984 FTC LEXIS 2, at *307-08 (F.T.C. Dec. 21, 1984) ("The Commission is not concerned with trivial or merely speculative harms" and "most Commission actions are brought to redress relatively clear-cut injuries, and those determinations are based, in large part, on objective economic analysis. As we have indicated before, the Commission believes that considerable attention should be devoted to the analysis of whether substantial net harm has occurred, not only because that is part of the unfairness test, but also because the focus on injury is the best way to ensure that the Commission acts responsibly and uses its resources wisely."); Hon. Julie Brill, Comm'r, Fed. Trade Comm'n, Responses to Sen. Kelly Ayotte (QFR), U.S. S. Comm. on Commerce, Sci. & Transp.: Privacy and Data Security: Protecting Consumers in the Modem World at 223 (June 19,

2011), *available at* http://www.governmentattic.org/13docs/FTC-QFR_2009-2014.pdf ("The Commission will not bring a case where the evidence shows no actual or likely harm to competition or consumers. As the Chairman explained in his testimony before the Senate Judiciary Committee last summer, 'Of (sic) course, in using our Section 5 authority the Commission will focus on bringing cases where there is clear harm to the competitive process and to consumers.' That is, any case the Commission brings under the broader authority of Section 5 will be based on demonstrable harm to consumers or competition."); J. Howard Beales, "The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection." (May 30, 2003), *available at* https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection (unfairness authority is "a powerful tool for the Commission" to attack practices that "cause ***widespread and significant consumer harm***") (emphasis added).

1. Specific nature of the substantial injuries asserted.

It appears Complaint Counsel asserts that the specific nature of the substantial injuries include identity theft, medical identity theft, medical identity fraud, reputational harm, embarrassment, monetary harm, new account fraud, tax fraud, time spent remediating problems, loss of privacy, plus an estimated $36,277 in out of pocket costs from fraud due to the theft of the Day Sheets. *See* CCPTB at 65-66, 72; CCPCL ¶¶ 30, 33, 36, 38. Complaint Counsel has not identified a single person who has suffered, or who is at certainly impending risk of suffering, any such injury.

2. Present or future injuries.

As the Court's Order on Post-Trial Briefing suggests, Section 5 unfairness authority extends only to present and future substantial injuries. *See* Order at § III(3)(2); 15 U.S.C. § 45(n) (Commission lacks authority to declare an unfair practice unlawful unless it proves the unfair practice "causes or is likely to cause" substantial injury); *Carr v. United States*, 560 U.S.

438, 448 (2010) (verb tense is used to ascertain a statute's temporal reach); 1 U.S.C. § 1 ("words used in the present tense include the future as well as the present"); *Heater v. FTC*, 503 F.2d 321, 324 (9th Cir. 1974) ("The broad power to define unfair acts and practices asserted as the basis for the refund order must be read in light of the contemplated non-retroactivity of a Commission decision").

Complaint Counsel does not allege any present substantial injury to any consumer, and so it seemingly claims only future injuries on the "likely to cause" prong of Section 5(n). *See* CCPCL ¶¶ 30 ("likely to cause" injury to a large number), 33 ("likely to cause" monetary harm), 36 ("likely to cause" harm in the form of time spent remediating problems), 38 ("likely to cause" health and safety risks). Yet clarity is lacking. For example, Complaint Counsel alleges "Consumers cannot reasonably avoid the substantial harm caused or likely to be caused by LabMD. . . . The unauthorized disclosures of the 1718 File and the . . . Day Sheets and checks provide ample evidence of the likelihood of this harm." CCPTB at 72. Apparently, the "harm" is in the past and the future but not the present.

Complaint Counsel also alleges that "In potentially exposing" individually identifiable health information "to unauthorized disclosure, LabMD's data security failures are likely to cause injury to a large number of consumers." CCPCL ¶ 30. This suggests no past or present injury, but an inchoate future injury based on layers of speculation, guess, and conjecture: a "potential exposure" (undefined) is "likely to cause" (also undefined) "injury" (also undefined) to an unspecified "large number of consumers," at some unknown point in the indefinite future.

Complaint Counsel also alleges the 1718 File patients "are likely to experience substantial harm by having their information used by identity thieves because the file was shared on the Gnutella network where any Gnutella user could access (sic) it." CCPTB at 69. *But see*

RPFF ¶ 472; (Shields, Tr. 915-22). The evidence is that only Tiversa, Dartmouth, and FTC (wrongfully) obtained the 1718 File, that the unauthorized LimeWire was removed from the rogue employee's workstation in May 2008, and that there are no incidents of identity theft attributable thereto. So this too seems to be a claim for an inchoate future injury, based on even more attenuated layers of speculation, guess, and conjecture: Tiversa stole the 1718 File on February 25, 2008, therefore "any Gnutella user could obtain it" and as a result all of the persons listed there are "likely to experience substantial harm by having their information used by identity thieves" in the indefinite future.

Complaint Counsel also alleges that the disclosure of the Day Sheets and the copied checks "caused or is likely to cause substantial injury to consumers." CCPTB at 71, 72 ("Consumers will incur . . . costs from fraud resulting from 164 cases of fraud . . . due to the unauthorized disclosure of the Day Sheets. Consumers will also spend an anticipated 2,497 hours resolving fraud arising from the disclosure of . . . the Day Sheets."). Facially, this seems to suggest past injury ("caused") and speculative, attenuated future injury in the indefinite future ("will incur") but no present injury.

To begin with, Complaint Counsel has not offered evidence, much less proven, that LabMD's security for the Day Sheets was "unreasonable." Without proof, the Day Sheets are probative of nothing. Furthermore, Complaint Counsel has not proven one case of fraud or that one consumer has spent one minute resolving fraud from the Day Sheets and copied checks since 2012, and its claim of future injury lacks any temporal boundary. Even so, Complaint Counsel claims the arc of the "risk" is endless.

Complaint Counsel also alleges "[t]he exposure of consumers' medical information contained on LabMD's system caused or is likely to cause substantial injury to consumers in the

form of medical identity theft, as exemplified by the exposure of the 1718 File on the Gnutella network." CCPTB at 70. This is difficult to untangle. To begin with, only the 1718 File, a June 2007 document, was stolen through LimeWire, no other patient information was or could have been stolen that way from LabMD (meaning that approximately 741,000 of the "750,000" patients FTC cites were never at risk from "exposure" on "the Gnutella network"), and LimeWire was removed in May 2008. *See* (CX 0704 (Boyle, Dep. at 57-64); (CX 0730 (Simmons, Dep. at 10-11, 14-15, 99-100)); *cf. Wyndham*, 2015 U.S. App. LEXIS 14839 at *46-47 (Wyndham failed to respond to confirmed hacks and customer injuries).

There is no evidence LabMD's patient information was ever improperly "disclosed" by LabMD. No computer breach occurred in this case. (Kam, Tr. 532) Given that there is no evidence that any LabMD patient, including those listed on the 1718 File and the Day Sheets, suffered any sort of injury, it is hard to understand how Complaint Counsel justifies its past injury claim ("caused"). Furthermore, it is plain that Complaint Counsel's future injury claim ("likely to cause") is entirely speculative and inchoate, anchored apparently on the theft of the 1718 File in February 2008 and on no other facts and without temporal bounds. *See* CCPTB at 70-71. According to Complaint Counsel's expert Kam, in *every* data breach in his professional experience a victim has come forward with an injury. (Kam, Tr. 532). However, there is not a single one (much less a large number) here.

3. Risk assessment/likelihood of the injuries.

Complaint Counsel's post-trial pleadings do not offer the Court or LabMD a legal standard for determining whether an act or practice is "likely" to cause substantial injury for purposes of Section 5(n). However, Congress did not define the term and so the common meaning controls. *Meyer*, 510 U.S. at 477. Webster's primary definition of "likely" is "having a high probability of occurring or being true: very probable (rain is likely today)." *See* "Likely",

Merriam-Webster's Dictionary, http://www.merriam-webster.com/dictionary/likely (last visited Sept. 2, 2015). The Ninth Circuit has defined "likely" to mean "probable." *See Sw. Sunsites v. FTC*, 785 F.2d 1431, 1436 (9th Cir. 1985) ("likely" means FTC must show "probable, not possible" deception). Webster's defines "probable" to mean "supported by evidence strong enough to establish presumption but not proof." *See* "Probable", Merriam-Webster's Dictionary, http://www.merriam-webster.com/dictionary/probable (last visited Sept. 2, 2015). Consequently, Complaint Counsel bears the burden of proving that it is "probable" or "highly probable" (depending on the authority applied) that LabMD's data security practices either cause or are likely to cause substantial injury to consumers. 15 U.S.C. § 45(n).

Complaint Counsel's risk assessment comes from Hill (RX 532 (Kaufman, Dep. at 203) ("The standard is Section 5 and reasonableness. Dr. Hill is the expert who will be or has provided testimony and report explaining why LabMD's practices were not reasonable.")), and its evidence of injury likelihood from Kam and Van Dyke. (RX 525 (Kaufman, Dep. at 59)).

With respect to Hill, as LabMD has argued, her undifferentiated "risk assessment" covers only the period between January 2005, and July 2010. She offered no opinion regarding post-July 2010 acts and practices and so, with respect to the period from July 2010 to the present, Complaint Counsel has no evidence LabMD's data security was unreasonable or in violation of Section 5. Furthermore, Dr. Hill fails the *Daubert* standard.[30] *See* RPTB at 19 n.5, 36-7, 51, 57 n.13, 74-79; RPCL ¶¶ 155, 164-71, 172-75, 201; RPFF ¶¶ 10, 86-9, 122, 287-88, 313-70, 377-85, 479. She did not specify how LabMD violated given data security standards at a given time (although data security practices and procedures were not static between 2005 and 2010, and LabMD was constantly changing to keep up), did not know HIPAA or apply medical industry

[30] *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993).

standards, and did not understand how LimeWire functioned. Hill also relied on fabricated evidence and perjured testimony provided by Boback and Tiversa to establish that the alleged "data security" deficiencies she identified were likely to cause harm (though of course they did not actually do so). (RX 524 (Hill. Dep.) (Apr. 18, 2014)); (CX 0740 (Hill, Rep. at 19, 59, 61); (Hill, Tr. 80-325)); RPFF ¶¶ 330. Dr. Hill relies on CX0019 and the claim of Robert Boback and Tiversa that the 1718 File was found in four (4) places. (CX 0740 (Hill, Rep. at 17 ¶ 46)) ("A list of the materials that I considered in reaching my opinions is attached to this report as Appendix B" including (CX 0019 (Tiversa: List of 4 IP Addresses where Insurance Aging File found)).

With respect to Kam and Van Dyke, as LabMD has argued, both are unreliable and both also fail *Daubert*'s admissibility test. *See* RPTB at 79-86; RPCL ¶¶ 164-71, 179-89 (Kam), 177-78 (Van Dyke); RPFF ¶¶ 386-427 (Kam), 428-68 (Van Dyke). Again, the empirical evidence disproves their speculative theories of harm. According to Kam, in *every* data breach in his professional experience a victim has come forward with an injury. (Kam, Tr. 532). Neither were asked or opined regarding LabMD's post-July 2010 data security, much less the current condition of LabMD's data security. RPFF ¶¶ 424 (Kam), 434 (Van Dyke). Finally, both testified to "likelihood" based on fabricated and perjured testimony from Boback and Tiversa. RPFF ¶¶ 408-18 (Kam), 431, 440-43 (Van Dyke).

Dr. Hill's, Kam's, and Van Dyke's opinions regarding the likelihood of harm in this case rest *entirely* on Tiversa's perjury and fabricated evidence. For example, factors two through four of Kam's "test" assume that Boback testified truthfully and that CX0019 was something other than a fabricated lie. (CX 0742 (Kam Report at 19)); (Kam, Tr. 531-32, 42-46). Even if this test survives *Daubert* on methodological grounds, (which it does not), it thus collapses under its own

weight. Similarly, Van Dyke's claim that he could calculate harm using his "data" from 2013 was based on Boback's testimony. (CX 0741(Van Dyke, Rep. at 8)); (Van Dyke, Tr. 645-46). This too cannot stand.

Kaufman, speaking for the Commission, highlights how tightly FTC joined with Tiversa, and underscores precisely how much it relied on a crooked, economically self-interested company, to justify this case:

> Q. (By Mr. Sherman) So is it the Bureau's position that in terms of unfair acts or practices, that it intends to produce evidence that . . . existed at LabMD from 2005 through, I think you said, around July of 2010? Or does the period extend to the present as alleged in the complaint?
>
> A. (By Mr. Kaufman) Well, certainly as of November 2013 the 1,718 file was still available on peer-to-peer networks.
>
> Q. Did the Bureau take any action to verify that?
>
> ***
>
> A. ***I am basing that solely upon the testimony of Mr. Boback.***

(RX 525 (Kaufman, Dep. at 61-62)) (emphasis added).

Complaint Counsel does not claim that LabMD's data security practices cause substantial harm to consumers now. None of its experts testified that LabMD's challenged pre-July 2010 data security practices, all of which ceased long ago, are "probable" or "highly probable" to cause harm in the future, *i.e.* in 2015 or beyond. Furthermore, none of Complaint Counsel's experts opined that LabMD's post-July 2010 data security practices are deficient in any way. Consequently, Complaint Counsel has failed to carry its burden.

4. Complaint Counsel's injury failures.

Even if LabMD's data security practices are deemed "unfair" under Section 5(a) for the relevant time frame, Complaint Counsel cannot prove substantial injury because it cannot prove (1) anything more than the speculative possibility of inchoate, potential future harm arising from

the "exposure" of PHI due to the 1718 File, the Day Sheets, and any other LabMD data security "insufficiency"; (2) that the alleged injuries cannot be "reasonably avoidable" as a matter of law, especially because LabMD is a HIPAA "covered entity" subject to the HIPAA breach notification rule; (3) that the potential injury to consumers is not outweighed by countervailing benefits of the allegedly unfair and unlawful data security practices; and/or (4) an impact on consumers generally or competition. 15 U.S.C. § 15(n).

a. More than speculative future injury is required.

The Commission has claimed repeatedly that "750,000" patients are likely to suffer substantial injury due to LabMD's allegedly unreasonable data security. (RX 525 (Kaufman, Dep. at 58-59)). The sole basis for this claim is Dr. Hill. *See* (RX 525 (Kaufman, Dep. at 56, 67-68, 70)). Complaint Counsel parrots this. *See, e.g.*, CCPTB at 5 ("LabMD's unreasonable security caused or is likely to cause substantial injury to over 750,000 consumers . . . ."). However, Dr. Hill did not opine that LabMD's data security failed to measure up after July 2010, or that pre-July 2010 data security acts and practices were likely to cause substantial harm to consumers in 2015 or beyond. (Given that there has been no harm at all to even a single LabMD patient, not in 2005, nor 2010, nor 2015, such a claim would require a rather significant empirical and theoretical leap.) And there is no evidence that "750,000" patients are "likely" to suffer substantial harm in the future due to any of LabMD's data security practices, whether before or after July 2010.

According to Kam, in *every* data breach, in his professional experience, a victim has come forward with an injury. (Kam, Tr. 532). Here, there is no victim, past or present. Complaint Counsel thus has nothing more than speculation, conjecture, and guesses concerning inchoate and speculative potential harm arising from allegedly deficient data security practices

that took place no later than July 2010, and on fabricated and perjured evidence from Tiversa, to establish "substantial injury." RPFF ¶¶ 380-82 (Hill), 408-18 (Kam), 431, 440-43 (Van Dyke); (CX 0742 (Kam, Rep. at 19)); (Kam, Tr. 531-32, 542-46).

Kam's testimony throws the deficiencies of Complaint Counsel's injury case into stark relief.

> Q. (BY MS. MORGAN) [. . .] Mr. Boback answered, on page 65, "I had heard that the individual at 173.16.83.112 was either detained or arrested in an Arizona Best Buy buying multiple computers. I don't know the outcome of this case. I'm not privileged to any of that information." Did I read that correctly?
>
> A. (BY MR. KAM) You did.
>
> Q. Mr. Boback says he heard the individual was detained or arrested instead of he knew; isn't that right?
>
> A. Yes.
>
> Q. He doesn't say who he heard it from?
>
> A. No.
>
> Q. He does not say who was arrested?
>
> A. No.
>
> Q. He does not say what law enforcement body carried out the arrest?
>
> A. I thought he referred to federal law enforcement in the --
>
> Q. Did he name a specific law enforcement body?
>
> A. Other than federal law enforcement, no.
>
> Q. He says he doesn't know the outcome of the case pertaining to identity theft in Arizona; right?
>
> A. Yes.
>
> Q. And you used this information as the factual underpinning for your assessment of the risk of harm; right?
>
> A. For some of it, yes.

(Kam, Tr. 545-46).

FTC's Unfairness Policy provides:

> As we have indicated before, the Commission believes that considerable attention should be devoted to the analysis of whether substantial net harm has occurred, not only because that is part of the unfairness test, but also because the focus on injury is the best way to ensure that the Commission acts responsibly and uses its resources wisely. Nonetheless, the Commission wishes to emphasize the importance of examining outside statutory policies and established judicial principles for assistance in helping the agency ascertain whether a particular form of conduct does in fact tend to harm consumers.

Int'l Harvester Co., 1984 FTC LEXIS 2 at *312-13. In line with established judicial principles, this requires much more than speculative hypothetical injury. *Accord Reilly*, 664 F.3d 38, 44; *see also Wyndham*, 2015 U.S. App. LEXIS 14839 at *45-48; *Remijas v. Neiman Marcus Grp., LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487, at *11-17 (7th Cir. Jan. 23, 2015).

In data breach cases where there is no breach and misuse, there has been no Section 5(n) injury as a matter of law. *Clapper*, 133 S. Ct. at 1148; *Reilly*, 664 F.3d at 44. *Neiman Marcus* demonstrates that Complaint Counsel has failed to prove substantial injury, not that it has established it. 2015 U.S. App. LEXIS 12487 at *11-12. According to the Court:

> Allegations of future harm can establish Article III standing if that harm is "certainly impending," but "allegations of possible future injury are not sufficient." . . . Here, the complaint alleges that everyone's personal data has already been stolen; it alleges that the 9,200 who already have incurred fraudulent charges have experienced harm. Those victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges. The complaint also alleges a concrete risk of harm for the rest.
>
> [. . .]
>
> Whereas in *Clapper*, "there was no evidence that any of respondents' communications either had been or would be monitored," in our case there is "no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken." . . . Like the *Adobe* plaintiffs, the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an "objectively reasonable likelihood" that such an injury will occur. . . .

> [However]: "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."

Id. at *8-12 (citations omitted). The Court then ruled:

> Mitigation expenses do not qualify as actual injuries where the harm is not imminent. . . . Plaintiffs "cannot manufacture standing by incurring costs in anticipation of non-imminent harm." . . ."If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." . . . *Clapper* [the source for these propositions] was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs.

Id. at *13-14 (citations omitted).

Complaint Counsel has failed to prove either that there was an actual data breach, as in *Neiman Marcus*, or that harm to a large number of consumers is certainly impending. Especially given the passage of time in this case since the "security incidents" pled in the Complaint occurred, this case is in all fours with *Clapper* – Complaint Counsel impermissibly seeks to use Section 5 to address a speculative harm based on something that did not, and, based on the evidence, cannot, happen.

b. Reasonable avoidance.

Complaint Counsel must prove the consumers potentially affected by the speculative harms alleged are not "reasonably capable" of mitigation. As the Ninth Circuit explained, an "injury" is not actionable under Section 5(n) "if consumers are aware of, and are reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact." *Davis v. HSBC Bank Nev.*, 691 F.3d 1152, 1168-69 (9th Cir. 2012) (citation omitted). *Davis* framed the issue as "not whether subsequent mitigation was convenient or costless, but whether it was 'reasonably possible.'" *Id.* (citation omitted); *see also Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007) ("lost data" cases "clearly reject the theory that a plaintiff is entitled to reimbursement for credit monitoring services or for time and money spent monitoring

his or her credit"). Here, LabMD is subject to HIPAA and so consumers will be notified in the event of a breach pursuant to 45 C.F.R. §§ 164.400-414 and are fully capable of mitigating the injury after the fact. *Davis,* 691 F.3d at 1168-69.

As a matter of law, speculation about the potential time and money consumers could spend resolving fraudulent charges cannot satisfy Section 5(n), let alone confer standing under Article III. *See id.*; *Reilly,* 664 F.3d at 46 (concluding that "alleged time and money expenditures to monitor financial information do not establish standing because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for . . . claims" at issue); *Randolph*, 486 F. Supp. 2d at 8 ("[L]ost data" cases "clearly reject the theory that a plaintiff is entitled to reimbursement for credit monitoring services or for time and money spent monitoring his or her credit."). As a matter of law, that a plaintiff has willingly incurred costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a "concrete and particularized" or "actual or imminent" injury. *In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 28-33 (listing cases).

c. Countervailing benefit.

Section 5(n) requires FTC to conduct a countervailing benefit analysis and declare unlawful only those unfair practices that fail review. 15 U.S.C. § 45(n). The analysis must include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters. *See Int'l Harvester Co.*, 1984 FTC LEXIS 2 at *307-11. In other words, FTC must conduct a proper cost-benefit analysis, and introduce it into the record (allowing LabMD to challenge and cross-

examine) before it may declare an unfair practice that causes or is likely to cause substantial injury and that is not reasonably avoidable by consumers themselves, unlawful. *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009) (noting "the requirement that an agency provide reasoned explanation for its action"); CCPCL ¶ 14 ("The codification of unfairness (sic) established a cost-benefit analysis to evaluate whether practices are [unlawful]." (citations omitted).

The Commission has long recognized that declaring an act or practice as "unfair" means a more rigorous analysis than is necessary under a deception theory. *Int'l Harvester Co.*, 1984 FTC LEXIS 2 at *270-71. The primary difference between full-blown unfairness analysis and deception analysis is that deception does not ask about offsetting benefits. Instead, it presumes that false or misleading statements either have no benefits, or that the injury they cause consumers can be avoided by a company at very low cost. It is also well established that one of the primary benefits of performing a cost-benefit analysis is to ensure that government action does more good than harm. *Id.*

In bringing this case, the Commission abdicated its duty to conduct a robust and statistically valid cost-benefit analysis. For its part, Complaint Counsel has blurred the line between unfairness and deception, claiming that LabMD could have corrected its data security "failings" at "low cost" and done something differently (although precisely what at any given point in time is never specified). *See* CCPCL ¶¶ 15, 19, 50, 113. Complaint Counsel's "low cost" claim, unsupported by any study or analysis, *see* CCPCL ¶ 50 ("Countervailing benefits are unlikely to be significant when more effective security measures could have been implemented at relatively low cost."), does not substitute for a proper countervailing benefit analysis, and it would be arbitrary and capricious to find for the Commission without one. *FTC v. Neovi, Inc.*,

598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (FTC offered expert testimony that the defendants' business model did not provide any advantage and that any benefits were small, did not have a positive impact in the marketplace, and did not benefit competition).

Specifically, a critical part of Complaint Counsel's case is that LabMD kept too much patient information on hand and so doctors had too much access.[31] However, it was the *doctors* who provided LabMD with the patient information they wanted in LabMD's database. *See* CCFF ¶¶ 81-82, 104, 113-115; (Daugherty, Tr. 1063). This produced real benefits. (Daugherty, Tr. 942 ("[T]he doctor could actually choose who read his tissue. He wasn't locked in to the hospital pathology team. Now, with all due respect to pathology -- hospital pathology teams . . . those are generalists. And if you have cancer, and the person diagnosing your cells is a pathologist, logically you would like to have someone that just reads that type of cell because practice makes perfect . . . ."), 944-45, 950-51 ("[W]hat you had at the time was offices that would have to take triplicate 8-1/2" x 11" order forms, and they'd have to have one for every lab they were going to use, and they'd have to hand-fill it out. And all this is an option for human error, a potential for human error that compromises patient quality. I mean patient diagnostic quality. Clinical quality. . . . I wanted to technologically solve this problem."), 953 ("So the

[31] Complaint Counsel argues:

> LabMD collected and maintained data which it did not need to conduct its business, even though IT practitioners during the relevant time period regularly purged unneeded data. If an organization collects more data than needed to conduct its business, it increases the scope of potential harm if the organization's network is compromised. LabMD had no policy for deleting data which it no longer needed and has not destroyed any patient information it has received from consumers since the company's inception. In addition, LabMD collected and has maintained indefinitely Personal Information regarding approximately 100,000 consumers for whom it never performed testing and, therefore, whose information it had no business need to collect or maintain.

CCPTB at 41 (citations omitted).

overall plan was to streamline the process from the moment the receptionist in the urologist's office enters the patient information to the moment, you know, the tissue arrives, goes to the lab, the doctor, the pathologist at LabMD, renders a diagnosis, and that result then is immediately available. That removed so many potential human errors that would slow down or compromise the medical result and the clinical process."); 955-64); (Daugherty, Tr. 962 ("[I]n our marketplace, typically approximately 85 percent of all the specimens were allowed to come to LabMD. But that 15 percent that weren't allowed to come to LabMD, by removing all the pitfalls of having to manage that was a huge time savings and a huge removal of bureaucracy from physicians' offices . . . [T]he amount of errors just fell through the floor.")).

As Mr. Daugherty testified:

> JUDGE CHAPPELL: Hold on a second. Why would LabMD have information on a consumer for whom it never performed any services?
>
> THE WITNESS: Because, as I said this morning, [doctors] can't read into the future, so depending on their software and the system, they send–the doctor doesn't know who he's going to order anything on. He doesn't know until he does and he sees the patient, so they push everything in, depending on the system, the morning of or the night before, especially back in those days when it was–every office had different software. I mean, every office had different software . . . . [I]t's this benefit of not having to wait, to not having to have patient–penmanship mistakes or diagnosis errors or data entry errors, so all this was done ahead of time to eliminate all the pitfalls of handwriting.
>
> [. . .]
>
> JUDGE CHAPPELL: Bottom line –
>
> THE WITNESS: . . . [W]hen they started using LabMD, they would do an entire database dump. And then we would have an update. . . . We are their laboratory. We are their covered entity. We are practicing medicine with them. We're not like McDonald's. And so . . . they sent [patient information] over . . . to expedite operations and to have a more efficient, safer system.

(Daugherty, Tr. 1063-65).

Assuming, *arguendo*, FTC's medical data security competency,[32] to prevail Complaint Counsel still must demonstrate that the allegedly unlawful conduct by LabMD results in net consumer injury. 15 U.S.C. § 45(n); *Int'l Harvester Co.*, 1984 FTC LEXIS 2 at *307-18. Here, this means a demonstration that the decisions of the doctors who provided LabMD with patient information are less than optimal because the benefits of improved cancer diagnosis do not outweigh the hypothetical risk of identity theft due to LabMD's alleged data security failures. No such demonstration was made.

Complaint Counsel alone has the burden of proof that FTC has reasonably evaluated and concluded that the risk of harm is large compared to any offsetting benefits.[33] LabMD has nothing to prove or rebut. Declarative statements (*e.g.*, "low cost"), without a meaningful cost-

---

[32] This is a rather gross assumption. For example, Kaufman testified:

> Q. (MR. SHERMAN) If there were a breach notification under HITECH, would that be something that the Bureau would enforce?
>
> A. (MR. KAUFMAN) I'm sorry, what is HITECH?
>
> Q. HITECH is a piece of legislation related to HIPAA.
>
> A. I would have to see the legislation.
>
> [. . .]
>
> A. I know there is proposed legislation out there that would put us or give us that authority but I am not aware of which legislation.

(RX 525 (Kaufman, Dep. at 52-53)). *Compare* CCPTB at 41 *with* Am. Med. Ass'n, Ethics Opinion 7-05 – Retention of Medical Records ("(1) Medical considerations are the primary basis for deciding how long to retain medical records. For example, operative notes and chemotherapy records should always be part of the patient's chart. In deciding whether to keep certain parts of the record, an appropriate criterion is whether a physician would want the information if he or she were seeing the patient for the first time."), *available at* http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion705.page; *see also* 42 C.F.R. § 482.24(b); Ga. Code Ann. § 31-33-2.

[33] *See* J. Howard Beales, III, Dir., Bureau of Consumer Prot., Fed. Trade Comm'n, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection at 9 (May 2003), *available at* http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection; *see also* Am. Bar Ass'n, Section of Antitrust Law, Consumer Protection Law Developments 57-59 (2009).

benefit analysis that would allow the Court to judge net effects, are not enough. 15 U.S.C. § 45(n); *Ctr. Fla. Enters., Inc. v. FCC*, 598 F.2d 37, 49 (D.C. Cir. 1978) (reasoned decision making required in an adjudication).

Complaint Counsel offered no study or competent cost-benefit analysis here. This omission is troublesome because FTC clearly can, and does, provide such a thing. *Neovi*, 598 F. Supp. 2d at 1116 ("[E]xpert testimony from Dr. Mann established that Defendants' business model did not provide any advantage over other payment options and that any benefits were small. Dr. Mann states that Qchex did not have a positive impact in the marketplace and did not benefit competition. . . . Defendants did not provide any legitimate evidence to the contrary."). Furthermore, the Commission's own precedent required it to do so. *Int'l Harvester Co.*, 1984 FTC LEXIS 2 at *270-71 ("[W]e cannot be confident, without a cost-benefit analysis, that a Commission action would do more good than harm . . . [and] a cost-benefit analysis is required only under an unfairness and not under a deception approach.").

The testimony was that LabMD's data security software, hardware, and IT practices were purposefully designed to integrate disparate external systems and to meet doctors' needs. (Daugherty, Tr. 959-62, 970-71, 982, 1036, 1063). Complaint Counsel, however, did not produce any evidence showing that it considered the practicalities of the operation at all. Thus, because FTC has not carried out a proper cost-benefit analysis, the net effects of LabMD's challenged data security practices cannot be assessed or challenged, and Complaint Counsel has failed to carry its burden of proof under Section 5(n).

d. Consumers generally/competitive effect.

Section 5 must be construed in accordance with its primary purpose of protecting free and fair competition. *Am. Bldg. Maint. Indus.*, 422 U.S. at 277; *see also Int'l Harvester Co.*, 1984

FTC LEXIS 2 at *311 n.24 ("[T]he inquiry should begin, at least, by asking 'whether the acts or practices at issue inhibit the functioning of the competitive market and whether consumers are harmed thereby.'" (citation omitted)).[34] This means Complaint Counsel should be required to evaluate and then prove that LabMD's data security had some generalized impact on markets or consumers generally, to meet the test of Section 5(n). *See* Beales, *supra* note 33 ("[U]nfairness [has] a more prominent role as a powerful tool for the Commission to . . . attack a wider range of practices that may not involve deception but nonetheless cause widespread and significant consumer harm.").

Of course, Complaint Counsel has not offered evidence proving LabMD's allegedly deficient data security practices inhibit the market's functioning and/or cause widespread and significant consumer harm, as required by Section 5(n), again leaving LabMD with nothing to prove or rebut. But this case shows just how far FTC has strayed from its statutory mission. FTC's refusal to exercise its 15 U.S.C. § 57a authority; its claims that standards are to be found buried in Commission complaints, consent orders, and speeches; and the action against LabMD, jointly and severally demonstrate that the Commission's application of Section 5 to data security is destructive to small businesses and likely anti-competitive in application, if not design.[35]

---

[34] *See* 15 U.S.C. §§ 45(a), (n); *Yates*, 135 S. Ct. at 1082-83, 85 ("[W]e rely on the principle of *noscitur a sociis*—a word is known by the company it keeps—to 'avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving unintended breadth to the Acts of Congress.'"); S. Rep. No. 75-221, at 2 ("[W]here it is not a question of a purely private controversy, and where the acts and practices are unfair or deceptive to the public generally, they should be stopped regardless of their effect upon competitors. This is the sole purpose and effect of the chief amendment of section 5.").

[35] *See* CCPCL ¶¶ 17-20; (RX 532 (Kaufman, Dep. at 191-92)); (Hill, Tr. 292 ("For both -- for small organizations and for large organizations, the [seven principles] guidelines are consistent.")). Thus, FTC favors big business and burdens small firms, discouraging innovation and job creation and lessening competition.

III. LabMD PREVAILS ON THE RECORD.

This Court need not find for LabMD on a single one of the legal issues discussed above to rule in its favor, because Complaint Counsel fails on the evidence.

A. Analytics.

Complaint Counsel submitted 1799 proposed findings of fact. An analytical review suggests just how thin FTC's case truly is.

- Approximately 500 of Complaint Counsel's 1799 proposed findings of fact are the expert opinions or conclusions of Hill, Kam, Van Dyke, and Shields. However, Complaint Counsel offers these opinions or conclusions without accounting for the exclusion of Boback and the 1718 File. *See, e.g.*, (Kam, Tr. 545-56). Also, expert conclusions and opinions cannot be used to establish facts. In *In re Realcomp II, Ltd.*, No. 9320, 2009 FTC LEXIS 250 (F.T.C. Oct. 30, 2009), the ALJ, in his initial decision, adopted summaries of experts' opinions and analyses as findings of fact. *Id.* at *9 n.4. Upon review of the case by the Commission, the Commission opined that "[w]e adopt those findings to the extent that they simply summarize such testimony or analysis, but without any implication that we endorse such opinions or analyses." *Id.* An example of the proposed finding of fact in *Realcomp II* is as follows: "'Realcomp's antitrust

---

> When regulations are complex to discover or interpret, there are likely to be benefits to specialization, which large firms can more easily exploit. . . . Large firms have staff specialists with the time and competence to do this while small businesses often do not. . . . [S]mall businesses prefer that regulations be phrased in concrete and not generic terms so that, once the discovery cost is incurred, it is clear exactly what the company must do.

See Andrew Hale, *et al.*, Mercatus Ctr., George Mason Univ., Working Paper: *Regulatory Overload: A Behavioral Analysis of Regulatory Compliance* 7 (Nov. 2011), *available at* http://mercatus.org/sites/default/files/publication/Reg_Overload_HaleBorysAdams_WP1147_0.pdf (citations omitted); *see also* (Daugherty, Tr. 951-52 (discussing competitive challenges facing small businesses in the cancer diagnostic space)).

Some agencies believe that small businesses and objective regulatory standards together impede efficient federal regulation and are using the instrumentalities of regulatory power accordingly. *See, e.g.* Dep't of Labor, Wage & Hour Div., Admin.'s Interpretation No. 2015-1, *The Application of the Fair Labor Standards Act's "Suffer or Permit" Standard in the Identification of Employees Who Are Misclassified as Independent Contractors* 4 (July 15, 2015) ("The factors should be considered in totality . . . not . . . as a checklist, but rather the outcome must be determined by a qualitative rather than a quantitative analysis."), *available at* http://www.dol.gov/whd/workers/Misclassification/AI-2015_1.pdf. However, Section 5(n) obligates FTC to protect competition and markets, not maximize federal authority and control over private businesses.

economic expert, Dr. Eisenstadt testified that Realcomp's Policies' effect on the non-ERTS share in Realcomp was at most a 1% decrease in the percentage of non-ERTS listings.'" *Id.* The Commission said "[w]e accept this as an accurate factual summary of what Dr. Eisenstadt said, but we do not necessarily endorse the conclusion he expressed." *Id.* Here, Complaint Counsel does not limit its proposed findings by qualifying them as what Complaint Counsel's experts concluded, opined, or testified. Instead, Complaint Counsel attempts to have this Court accept the conclusions made by its experts as fact. The findings of fact that parrot expert conclusion and opinion, and that reflect Boback's testimony and CX0019, should be disregarded and given no probative value.

- Approximately forty-five (45) proposed findings of fact rely exclusively on the investigational hearing testimony of Curt Kaloustian, who was not cross-examined. Complaint Counsel did this knowing that such testimony would not be given weight. *See* Final Prehearing Conference, *In re LabMD, Inc.*, No. 9357, 9-10 (F.T.C. May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "[Investigational hearing depositions] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").
- Approximately fifty-six (56) proposed findings of fact draw inferences from the ProviDyn Reports. The fact that a statement was contained in the ProviDyn report, however, is only probative of the fact that this statement was contained in the ProviDyn report. ProviDyn was trying to sell LabMD services, not enforce regulations. And there was no testimony that ProviDyn's methods or assessment were commonly used, accurate, or applicable. Complaint Counsel simply liked what the report said. Therefore, this report should be accorded little weight as to truth or accuracy.
- Approximately ninety-five (95) proposed findings of fact fail to cite to specific references to the evidentiary record. This violates the Court's Order. *See* Order on Post-Trial Briefs, *In re LabMD Inc.*, No. 9357, 2 (F.T.C. July 16, 2015) ("All proposed findings of fact shall be supported by specific references to the evidentiary record."); *id.* at 3 ("Do not use '*Id.*' as a cite for proposed findings of fact . . . .").
- Approximately 135 proposed findings of fact mischaracterize, misquote, misstate, or are otherwise unsupported by the record.

B. FTC's Witnesses.

To prove LabMD's data security practices were unlawful, and as a substitute for victims and loss and studies and statistics, Complaint Counsel offered the testimony of three experts, one "rebuttal" expert, and less than a handful of former LabMD employees.

1. The experts.

Given Complaint Counsel's post-trial pleadings, the following points are particularly salient.

As for Dr. Hill:

- Complaint Counsel cited Hill's testimony over 250 times.
- Dr. Hill assumed harm based on Boback and CX0019. (CX 0740 (Hill, Rep. at 17)); (Hill, Tr. 88). But she did not testify that any harm was occurring or was likely to occur.
- Dr. Hill's testimony, by its own terms, only covers the time period from January 2005 through July 2010. (CX 0740 (Hill, Rep. at 3-4)). Thus, she has nothing to say about LabMD's data security beyond July 2010, or about present or future harm.
- Dr. Hill critiqued LabMD's data security using general IT principles without reference to, or apparent knowledge of, medical industry standards and practices during the relevant time period. (RX524 (Hill, Dep. at 150-51)). This critique is not based on FTC's website materials or speeches, but on unpublished, unreviewed, and unverified standards that Hill created herself. (This, alone, should mean that judgment for LabMD is appropriate on fair notice grounds.) (Hill, Tr. 230-33; 240-41). Without its expert giving any consideration to the standards of the FTC, Complaint Counsel cannot use Dr. Hill's expert opinion to establish "the legal standards that apply to determining whether Respondent's data security practices as alleged in the Complaint are unreasonable," as required by the Court's Order on Post Trial Briefs.
- Dr. Hill asserted that "defense in depth" was necessary. (Hill, Tr. 306-10). But she only became aware of "defense in depth" circa mid-2009. (Hill, Tr. 306). She did not explain how LabMD was supposed to know about this before then. In fact, Dr. Hill did not specify how LabMD came up short at any specific time.
- Dr. Hill relied on Kaloustian for key conclusions without citing a second, corroborating source. *See* (CX 0740 (Hill, Rep. at 38, 42, 47,)); (Hill, Tr. 274-276).

As for Kam:

- Complaint Counsel cited Kam's testimony over 100 times to establish that LabMD's data security is likely to cause substantial injury. But Kam has no expertise in computer data security or computer network security, (Kam, Tr. 518); neither has his personally-developed methodology been generally accepted in the fields of medical or data privacy or statistical analysis, nor has any work based

upon his methodology been peer-reviewed or published. (CX 0742 (Kam, Rep. at 17-18)); (RX 522 (Kam, Dep. at 46)).

- Kam's statistical model falls apart in the face of the empirical proof. He estimated that there would be seventy-six (76) victims of medical identity theft due to the alleged disclosure of the 1718 File, (CX 0742 (Kam, Rep. at 19)), and he noted that in *every* data breach in his professional experience a victim has come forward with an injury. (Kam, Tr. 532). Yet, not a single victim has been identified here.

- But even if this Court were to find that the evidence in Kam's model is valid, widely accepted, reliable, and peer-reviewed (which, of course, it is not), his testimony and opinion should be rejected. Kam's opinion–the critical link in Complaint Counsel's claim that it has proven LabMD's supposedly unfair data security practices cause or are likely to cause harm–is inextricably bound up in Boback and CX0019. For instance, Kam's factors two and three consider to whom the 1718 File was disclosed and that the file was acquired and viewed. Factor four considers the extent to which disclosure was mitigated. Kam relied on Boback's testimony to conclude that the 1718 File was found on four IP addresses, and was available as late as November 21, 2013 on the peer-to-peer network. (CX 0742 (Kam, Rep. at 19)). *But see* (Wallace, Tr. 1367-70). In other words, Kam's opinion bears no relationship to the true facts of this case.

As for Van Dyke:

- Complaint Counsel cites Van Dyke over ninety (90) different times to help establish that LabMD's supposedly unfair data security practices cause or are likely to cause substantial injury. Van Dyke assumed LabMD's data security was inadequate, but he is not qualified to opine on this issue. (Van Dyke, Tr. 696).

- Van Dyke never testified that inadequacies (real or manufactured) pre-July 2010 cause harm now or are likely to cause harm in the future.

- Van Dyke relied on Boback and CX0019 and thus thought that "[t]he circumstances of the unauthorized disclosure of the 'Insurance Aging Report' . . . make identity fraud **more likely**." (CX 0741 (Van Dyke, Rep. at 8) (emphasis added). Of course, the 1718 File was not found at any of these four IP addresses. (Wallace, Tr. 1383). Thus, no unauthorized disclosure occurred. Van Dyke's conclusion should actually read that "[t]he circumstances of [the lack of an unauthorized disclosure] of the 'Insurance Aging Report' . . . make identity fraud [**less]** likely."

- With respect to the Day Sheets, Van Dyke said: "[H]aving studied fraud, my work in fraud has caused me to be very careful about security, where I don't want to opine on what would be adequate security or not but rather to say, when information is exposed, in this case found in the hands of people who have

pleaded no contest to identity theft, what the likelihood of harm is." (Van Dyke, Tr. 649-50).

- Van Dyke "studied fraud" and therefore concluded that, in this case, there would be over 2,500 cases of identity fraud from the 1718 File, and over 160 cases of identity fraud from the Day Sheets. (CX 0741 (Van Dyke, Rep. at 12)); (Van Dyke, Tr. 618-19). However, there were, and are, no cases of identity fraud.

Finally, as for Shields:

- Complaint Counsel cites Shield over 100 times regarding security risks in the use of peer-to-peer networks, but Shields was merely a rebuttal witness. (Tr. 747-48).

- Shields also relied heavily on Boback. (Shields, Tr. 904-06).

- In response to questions from the Court, Shields confirmed that Tiversa was much more likely to find the 1718 File than the average user. (Shields, Tr. 920-21). Shields also confirmed how difficult it would be to find the 1718 File without using specialized search terms. (Shields, Tr. 919). In fact, he confirmed Fisk's testimony that finding the 1718 File would be exceptionally difficult. (Fisk, Tr. 1141). Shields said: "In the situation where there are two to five million users on the network, then somebody would probably have a chance of finding the file . . . particularly in some of the other scenarios that I outlined. For example, while 'PDF' might have a low probability of finding that file, the fact that there are two to five million users on the network every hour just means that if a very small percentage of them are curious enough to open random PDF files, someone might find that." (Shields, Tr. 919). Shields pointed to no facts, no statistics, and no study. Instead, he speculated that "someone *would probably* have *a chance* of finding," and "if a very small percentage of them *are curious enough* to open random PDF files, someone *might find* that." (Shields, Tr. 919) (emphasis added).

C. Fact Witnesses.

Complaint Counsel depends substantially on former LabMD employees Curt Kaloustian and Alison Simmons. This reliance is severely misplaced.[36]

[36]Complaint Counsel routinely stretches the testimony. For example, Jeff Martin, cited as the sole source for CCPFF ¶ 87, could not have known what he is cited as the authority for. According to Complaint Counsel, "For some physician-clients from at least January 2012 through February 2014, after an initial transmission to LabMD of all the client's patients' information, additional patients' information was sent to LabMD only when patients had testing performed by LabMD." Martin, however, lacked the training and knowledge to make this claim.

1. Curt Kaloustian

Complaint Counsel cites to Kaloustian testimony in total over ninety (90) times and relies exclusively on Kaloustian testimony approximately forty-five (45) times. Kaloustian worked at LabMD between October 2006 through April or May 2009. (CX0735 (Kaloustian, IHT at 7, 17)). Yet, shortly before Kaloustian testified, he had been terminated by LabMD for inadequate work performance. (RX 415 (Kaloustian Background Check/A. Simmons' Resignation, at 1) ("Terminated for failure to perform job duties")). Bob Hyer found that Kaloustian was "completely unqualified." (CX 0719 (Hyer, Dep. at 41-42).

Kaloustian was never cross-examined; LabMD was never notified about his IHT examination, *see, e.g.*, RPTB at 56-57; *see also* RPCL ¶ 133; and this Court indicated that his testimony will be accorded little weight. Final Prehearing Conference, *In re LabMD, Inc.*, No. 9357, 9-10 (F.T.C. May 15, 2014). Nevertheless, just as Complaint Counsel (and its experts) relied on Boback's, Tiversa's, and CX0019's uncorroborated claims, so too did Complaint Counsel (and its experts) rely on Kaloustian's uncorroborated claims. *See* CCPFF ¶¶ 216, 226, 266, 512, 542, 555-58, 568-69, 571-78, 590-93, 595-96, 604, 623, 628-29, 653-54, 970-71, 982, 1008, 1013, 1059, 1086-87, 1095-96; (CX 0740 (Hill, Rep. at 38, 42, 47)); (Hill, Tr. 274-76).

Notwithstanding the limitations of Kaloustian's knowledge and expertise, Complaint Counsel relies on Kaloustian to establish, for example, that LabMD did not have security requirements for the computers it provided to physician-clients, CCPFF ¶ 266; that LabMD's antivirus software did not have the capability to remediate and remove viruses, CCPFF ¶ 536; that LabMD's use of ClamWin was not enough to provide reasonable data security, CCPFF ¶¶ 571-78, 590-960; that, as of October 2006, LabMD's firewalls did not have the capability of inspecting packets and, through April 2009, it did not have any tools or practices to inspect the content of Internet traffic into and out of its network, and, between March 2004 until April 2009,

it did not monitor traffic on its network, CCPFF ¶¶ 653-54; that, between October 2006 through April 2009, every server login username was "admin" and every password was "LABMD" and that servers were all linked to the same default administrator user profile, preventing IT staff from setting up user accounts for each IT employee, CCPFF ¶¶ 970-71; and, that LabMD did not implement IP address filtering, which would prevent communication with the network by an untrusted source, until late 2008 or 2009. CCPFF ¶ 1096.

Complaint Counsel and its experts (especially Dr. Hill) used this testimony as the critical foundation and loadstone for their claims against LabMD. But IHT testimony generally, and Kaloustian's in particular, is a very slim reed on which to hang a case.

2. Alison Simmons

Complaint Counsel cites Simmons' testimony over seventy (70) times to support its claims regarding LabMD's purportedly inadequate data security. *See, e.g.* CCPFF ¶ 73 (personal information stored in unencrypted form); CCPFF ¶ 103 (consumers personal information stored on computers supplied by LabMD to physicians); CCPFF ¶ 276 (LabMD lacked control over computers placed in physicians' offices); CCPFF ¶ 477 (LabMD lacked software monitoring policy from at least 2004 through August 2009); CCPFF ¶ 600 (LabMD had no process for reviewing or verifying that AVG anti-virus was operating properly on employee computers); CCPFF ¶ 1372 (no security measures in place to detect or prevent P2P sharing from the Billing Computer); s*ee also* (CX 0740 (Hill, Rep. at 23, 27, 35, 36, 38)).

As it did with Kaloustian, Complaint Counsel overreaches with Simmons. She worked at LabMD between October 2006 and August 2009, (RX 508 (Simmons, Dep. at 10)), and was competent to testify only for that period. Her primary responsibilities at LabMD did not involve IT security but rather "responding to phone calls from physician-clients who had problems with LabMD's system, managing and troubleshooting LabMD's database, generating reports, and

maintaining computers for the company." CCPFF ¶ 373; (CX 0719 (Hyer, Dep. at 40-41). Yet, Complaint Counsel cites her, without accounting for her duties, expertise, and the temporal parameters of her work, to establish a host of purported data security inadequacies. Simmons does not help FTC's case.[37]

IV. COMPLAINT COUNSEL IS NOT ENTITLED TO FENCING-IN RELIEF.

LabMD has demonstrated there is no legal basis for fencing-in relief in RR-CCPCL ¶¶ 73-121, which are incorporated herein by reference. LabMD has also demonstrated the Proposed Order is unlawful. *See* Resp.'s Reply to Proposed Notice Order, *In re LabMD, Inc.*, No. 9357 (FTC Sept. 3, 2015), which is attached as Addendum A and *supra* at § I(B). Upon review, Complaint Counsel's remedy case is at least as thin as its Section 5(a)/(n) case.

A. The Legal Standard.

"'Fencing-in remedies are designed to prevent future unlawful conduct.'" *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006) (citation omitted). Complaint Counsel must prove "cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive." *United States v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953). The Commission is not, under any circumstances, authorized to issue punitive orders. *Heater*, 503

[37] Simmons's testimony actually refutes Complaint Counsel's arguments that LabMD lacked appropriate security and damages severely FTC's injury claims. After LabMD was notified by Tiversa that the 1718 File was "on the internet," Simmons was directed to search all computers for file sharing software. (CX 0704 (Boyle, Dep. at 57-66, 74-88)). She found it only on Roz Woodson's computer and removed it. (CX 0730 (Simmons, Dep. at 10-11, 14-15)). She testified that she searched for the 1718 File on peer-to-peer networks from her home computer two hours on the day of the call from Tiversa and then once a week for a month or longer but was never able to find it. (CX 730 (Simmons, Dep. at 17-18)). She also testified that the billing department had a firewall and billing employees were prohibited from going to non-specified web sites, except for those needed to perform their jobs. (CX 0730 (Simmons, Dep. at 16, 22-26, 38-43)). She further testified that no one was authorized to make any downloads without going through IT. (CX 0730 (Simmons, Dep. at 17)).

F.2d at 326-27 (overturning an FTC order for restitution as inconsistent with the purpose of the FTC Act, which does not authorize punitive or retroactive punishment).

Borg-Warner Corp. v. FTC, 746 F.2d 108, 110-12 (2d Cir. 1984) (holding FTC failed to bear its burden and justify relief because "speculative and conjectural" allegations were not sufficient to justify equitable relief against a terminated violation), and *Litton Indus., Inc. v. FTC*, 676 F.2d 364, 370-71 (9th Cir. 1982), should control here. As the Ninth Circuit ruled:

> Because fencing-in provisions are prophylactic, the ultimate question is the likelihood of the petitioner committing the sort of unfair practices they prohibit. Accordingly, "(a)mong the circumstances which should be considered in evaluating the relation between the order and the unlawful practice are whether the respondents acted in blatant and utter disregard of the law, and whether they had a history of engaging in unfair trade practices." . . . We also consider whether the violations involved "a technique of deception that easily could be transferred to an advertising campaign for some other product." . . . [Fencing-in orders] should be used with caution "because they alter the scheme of penalties and enforcement procedures defined by the Act."

Id. (citations omitted). There is no evidence LabMD "acted in blatant and utter disregard of the law" or had "a history of engaging in unfair trade practices." Applying "fencing in" relief in this case, therefore, would be a clear abuse of discretion and unlawful. *See Grant*, 345 U.S. at 633 ("The necessary determination is that there exists some cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive.").

To ensure that a fencing-in order bears a reasonable relationship to the unlawful practice found to exist, the Commission considers three factors. They are: (1) the deliberateness and seriousness of the present violation; (2) the respondent's past history of violations; and (3) the transferability of the unlawful practices to other products. *In re Thompson Med. Co., Inc.*, No. 9149, 1984 FTC LEXIS 6, at *414-15 (F.T.C. Nov. 23, 1984). Complaint Counsel has not proven that it is entitled to fencing-in relief under any of these factors.

B. No Proof Of "Unreasonable" Data Security Post-July 2010.

Dr. Hill confined her opinions and conclusions to "the time period from January 2005 through July 2010 (Relevant Time Period)." (CX 0740 (Hill, Rep. at 3-4). She said that "from my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period." (CX 0740 (Hill, Rep. at 4).[38]

FTC's Rule 3.33 witness, Daniel Kaufman, made it clear the Commission relied only on Hill, Boback, and Tiversa with respect to this time frame. (RX 525 (Kaufman, Dep. at 61) (Q. "Is the Bureau also taking the position that the condition of LabMD's data security was an unfair practice from 2005 January to the present?" A. "My understanding is that according to the expert report of Dr. Hill, there was insufficient evidence for her to assess the period beyond July 2010 or so.")); (RX 525 (Kaufman, Dep. at 67) (Q. "I think we're back at the same place. So is it the Bureau's contention, based on the expert witness report of Ms. Hill, that harm – that there is a reasonable likelihood of substantial injury or harm to consumers, the 750,000 that we're talking about, in that that likelihood continues to exist through the present?" **MS. VAN DRUFF**: "Objection, **calls for expert testimony.** You may respond." THE WITNESS: "And we're not talking about the 1,718 file and the data sheets?" BY MR. SHERMAN: Q. "Right." **A. "Okay. I would have to defer to Professor Hill on that issue.**") (emphasis added)); (RX 532 (Kaufman, Dep. at 203) ("The standard is Section 5 and reasonableness. Dr. Hill is the expert who will be or has provided testimony and report explaining why LabMD's practices were not reasonable.")).

[38] This is a puzzle. Dr. Hill certainly had at least as much information about LabMD's post-July 2010 operations as she did its pre-July 2010 operations, and likely more. Yet, the only post-July 2010 information she deemed worthy and reliable was the information she obtained from Boback and CX0019. The obvious inference is that she believed LabMD's post-July 2010 data security was indeed reasonable, but that she was not being paid to say so.

FTC's designee also cited Boback, whose testimony Complaint Counsel has since putatively disavowed, possibly because he is a liar and a criminal. (RX 525 (Kaufman, Dep. at 61-62) (Q. "So is it the Bureau's position that in terms of unfair acts or practices, that it intends to produce evidence that that existed at LabMD from 2005 through, I think as you said, around July of 2010? Or does the period extend to the present as alleged in the complaint?" A. "Well, certainly as of November 2013 the 1,718 file was still available on peer-to-peer networks." Q. Did the Bureau take any action to verify that?" A. "I am basing that solely upon the testimony of Mr. Boback.")).

In other words, as a matter of fact and law, Dr. Hill is the only game in town on the reasonableness of LabMD's data security for the period July 2010 to the present. Accordingly, Complaint Counsel has failed to prove that LabMD's data security was unreasonable for the period of July 2010 to the present.

C. The Proposed Order Fails.

The Proposed Order is unconstitutional. *See supra at* § I(B); *Ass'n of Am. R.R.s*, 135 S. Ct. 1225 (2015). It is also unlawful in its terms and effect because it is not sufficiently clear to be comprehensible or reasonably related to the alleged violations. *See* Resp't's Reply to Proposed Order, *In re LabMD, Inc.*, No 9357 (FTC Sept. 3, 2015). Also, imposing the Proposed Notice Order without a factual basis–that is, testimony establishing that it is reasonably related to the allegedly unlawful activity at issue and, in this particular case, not in conflict with HIPAA–is arbitrary, capricious, and contrary to law. *Fox Television*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action"); *Billing*, 551 U.S. at 275. There is simply no basis in law to require LabMD to comply with requirements, such as extensive "third party" monitoring, on the record here. *Borg-Warner Corp.*, 746 F.2d at 110-12.

D. Complaint Counsel's Failures Of Proof.

Totality of the Evidence: Complaint Counsel encourages this Court to consider "the record as a whole" in meting out punitive fencing-in relief. *See* RR-CCPCL ¶ 57 (citing *Niresk Indus. Inc. v. FTC*, 278 F.2d 337, 340 (7th Cir. 1960)). But the record "as a whole" is that none of LabMD's patients have ever suffered identity theft or any other injury because of alleged data breaches by the company, for the simple fact that there have been none; that LabMD had robust IT procedures for a small business; that it fired employees who broke its data security policy; that this case was brought, and Complaint Counsel's experts testified, in reliance on a criminal fraudster who fabricated evidence; and that Complaint Counsel cannot find anyone to testify that LabMD's post-July 2010 data security has been unreasonable. On the record as a whole, this case never should have seen the light of day. FTC staff and the Commission owe LabMD, and the federal taxpayers, an apology. *Compare Wyndham*, 2015 U.S. App. LEXIS 14839 *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487.

Past Conduct/Future Practices: Complaint Counsel relies on *FTC v. Ruberoid Co.*, 343 U.S. 470 (1952), to importune fencing-in relief. However, *Ruberoid* torpedoes FTC's case because that case requires Complaint Counsel to demonstrate a genuine connection between past violations and future conduct. *See also Int'l Harvester*, 1984 FTC LEXIS 2 at *246-47, *267-70; *Thompson Med. Co.*, 1984 FTC LEXIS 6 at *414-15. Among other things, Complaint Counsel must show–because the data practices specified in the Complaint reflect technology, software, and industry practices from before (and in some cases, many years before) 2010, and such technology, software, and industry practices have changed (sometimes radically)–"that there is a cognizable danger of a recurrent violation . . . ." *Grant*, 345 U.S. at 633.

No such connection has been shown here because none of Complaint Counsel's experts–neither Dr. Hill, nor Kam, nor Van Dyke–testified that LabMD's post-July 2010 data security practices were unreasonable. Any of them could have done so, because all of the information they needed to make this evaluation was available, but none did. Instead, all Complaint Counsel had, and all the experts relied on, was Boback, Tiversa, and CX0019. Boback, Tiversa, CX0019, however, proved to be a perjurer, a scam, and a fake, respectively. With the liars, frauds, and fake out of this case, none of Complaint Counsel's experts–not Dr. Hill, not Kam, not Van Dyke–could aver that LabMD's data security, pre- or post-July 2010, causes or is likely to cause substantial injury.

Complaint Counsel, for its own reasons, chose to litigate this case without respect for the fact that LabMD was a medical business; that LabMD's hardware and software systems need to be configured in particular ways to ensure the appropriate transmission of information; and that HIPAA's Security Rule applied to its operations beginning in 2003. But, even applying the "IT industry" standards that Dr. Hill created for this litigation, Complaint Counsel has failed to prove the connection between past violations and future conduct needed to support the requested relief.

No Public Interest or Necessity: To justify fencing-in relief, Complaint Counsel must show that it is in the public interest. Whatever else Complaint Counsel has done in this case–and FTC's thinly veiled obsession with LabMD and Mr. Daugherty suggests a dangerous form of agency mission creep–the "public interest" has not been a central concern. Complaint Counsel has failed to prove LabMD's data security was "unreasonable" under Section 5(a) and then "unlawful" under Section 5(n). There is no **actual or certainly impending injury or harm here** and no testimony (except that based on Boback, Tiversa, and CX0019) that LabMD's data

security practices, past or present, are likely to cause it in the future. The dog, so to speak, is still on the porch.

No Prior or Current Violations: Complaint Counsel admits LabMD does not have any prior Section 5 (or HIPAA or any other) violations. It has not proven any current violations. The demanded fencing-in relief cannot be supported.

No "Cognizable Danger of Recurrent Violation": There is no evidence that any of the alleged unfair and unlawful data security practices identified by Dr. Hill continued after July 2010, or that any different unfair and unlawful data security practices occurred from that date to the present. *See* (RX 525 (Kaufman, Dep. at 67)); (RX 532 (Kaufman, Dep. at 201)). There is no evidence that any alleged unfair and unlawful data security acts and practices could occur in LabMD's current state. *See* (Daugherty, Tr. 1031-34, 53). There is no evidence of something more than a mere possibility that any alleged unfair and unlawful data security practices will occur if LabMD resurrects as a going concern. Therefore, Complaint Counsel has failed to carry its burden of showing there is a "cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive." *Grant*, 345 U.S. at 633.

CONCLUSION

FTC's case against LabMD is constitutionally and statutorily infirm on multiple grounds. Also, on the evidence Complaint Counsel has failed to carry its burden of proof. Plainly, the Commission has overreached.

This action, ostensibly about data security, began in January 2010. The Commission could find no victims, or even an expert to testify that there had been "unreasonable" data security at any time since July 2010. Nevertheless, in league with a corrupt company that made

money from FTC enforcement, the government burned millions of taxpayer dollars and destroyed an innovative cancer lab, for nothing at all.

This case was prosecuted only because FTC lost sight of its obligation to wield power lawfully and prudently, of its duty to act only after carefully considering all of the facts and consequences, and of the principle that government action must do more good than harm. *See Int'l Harvester,* 1984 FTC LEXIS 2 at *271 (to be sure "a Commission action [will] do more good than harm . . . a cost-benefit analysis is required . . . under an unfairness approach[.]"). What has happened here, these past six years, confirms the maxim that "absolute discretion, like corruption, marks the beginning of the end of liberty." *New York v. United States,* 342 U.S. 882, 884 (1951) (Douglas, J., dissenting). It confirms also that "[t]he standard set for people of good will is even more useful to the venal." *Id.*

For the reasons set forth herein this case should be dismissed and judgment entered for Respondent.

/s/ Daniel Z. Epstein
Daniel Z. Epstein
Patrick Massari
Cause of Action
1919 Pennsylvania Avenue, NW Suite 650
Washington, DC 20006
Phone: (202) 499-4232
Email: daniel.epstein@causeofaction.org

/s/ *Reed D. Rubinstein*
Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW Suite 610
Washington, DC 20004
Phone: (202) 372-9100
Email: reed.rubinstein@dinsmore.com

Counsel for Respondent, LabMD, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on September 4, 2015, I caused to be filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send an electronic notification of such filing to the Office of the Secretary:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW, Rm. H-113
Washington, DC 20580

I also certify that I delivered via hand delivery and electronic mail copies 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 a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Jarad Brown, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Room CC-8232
Washington, DC 20580

Dated: September 4, 2015 /s/ Patrick J. Massari

PUBLIC

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: September 4, 2015 /s/ Patrick J. Massari

ATTACHMENT 1

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

In the Matter of	)	**PUBLIC**
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

RESPONDENT LABMD, INC.'S REPLY TO COMPLAINT COUNSEL'S PROPOSED ORDER

I. THE PROPOSED ORDER IS UNLAWFUL.

A. General Principles.

15 U.S.C. §45 ("Section 5") does not authorize the Commission to issue a Notice Order with the Complaint. Consequently, the Notice Order in this case is either a judicially reviewable final order, or it demonstrates prejudgment in violation of due process, or it is *ultra vires* act in violation of the Administrative Procedure Act ("APA").

Article I of the Constitution establishes that all authority in FTC is inherent to statutory grants. Nothing in 15 U.S.C § 45 authorizes FTC to "deputize" private third parties, and therefore the Proposed Order is unlawful.

The Proposed Order authorizes the "qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession" to develop and apply the metrics and standards of data security and to apply them. These metrics and standards have a coercive effect on LabMD. That is regulatory power, and the Proposed Order is therefore unlawful. *Dep't of Trans. v. Ass'n of Am. Railroads,* 135 S. Ct. 1225, 1236 (2015) (Alito, J. concurring); *Bennett v. Spear,* 520 U. S. 154, 169 (1997).

Especially because FTC lacks properly promulgated data security rules or guidance for medical companies otherwise subject to HIPAA, the Proposed Order also raises Appointments Clause, separation of powers, and due process concerns. *Railroads* at 1233, 1235-39 (Alito, J., concurring). For example, Article II officers with regulatory authority must swear an oath to uphold the Constitution. The "third-party professional" who will choose and apply regulatory requirements (because FTC has not done so under 15 U.S.C. § 57a) does not. "By any measure, handing off regulatory power to a private entity is 'legislative delegation in its most obnoxious form.'" *Id.* at 1238 (citations omitted)(Alito, J. concurring); *Carter v. Carter Coal Co.*, 298 U. S. 238, 311 (1936).

That the third party's reports will be sent to FTC is of no legal moment. FTC has no medical (or other) data security standards or technical competency to judge what is or is not compliant. Instead, it relies entirely on outside "experts" - - in this case, for example, FTC relied on Dr. Hill, who in turn applied her own standards to determine LabMD's data security was "unreasonable."

FTC could, perhaps even should, adopt industry data security standards as the regulatory "metrics and standards" for Section 5. But to do this, it must exercise its 15 U.S.C. § 57a authority, not regulate through adjudication. *Compare* 40 CFR §§ 312.10, 11 (EPA "All Appropriate Inquiries" rule defining "environmental professional" and incorporating ASTM standards as basis for determining regulatory compliance); FTC may proceed by adjudication only in cases where it is enforcing discrete violations of existing laws and where the effective scope of the impact of the case will be relatively small and by § 57a procedures if it seeks to change the law and establish rules of widespread application. *Ford Motor Co. v. FTC*, 673 F.2d 1008, 1010-11 (9th Cir. 1981).

The Proposed Order is not equitable but punitive and therefore unlawful. *See* CCPCL at ¶ 76; *Heater v. FTC*, 503 F.2d 321, 326 (9th Cir. 1974) (FTC may not punish past conduct only proscribe specific practices in the future). "'The act does not expressly confer any general power, of the kind possessed by a court of equity, to compel restitution, or otherwise to so mold the decree as to do substantial justice under the circumstances. Of course, no damages can be awarded, or mandatory order entered. Where, therefore… there is no occasion for repeating it, the Commission cannot give relief.'" Henderson, The Federal Trade Commission 71 (1924) (*cited in Heater*, 503 F.2d at 326).

Complaint Counsel has the heavy burden of proving by a preponderance of the evidence that "there exists some cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive." *United States v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953). "[W]hen the Commission exercises its discretion in favor of granting relief, it must have a more substantial basis for that decision than the speculative and conjectural concerns that led it to enter a cease and desist order in this case." *Borg-Warner Corp. v. FTC*, 746 F.2d 108, 110-11 (2d Cir. 1984). Furthermore, "In Commission proceedings it is 'the FTC staff's burden of showing that an injunction was warranted.' *SCM Corp. v. Federal Trade Commission*, 565 F.2nd 807, 813 (2d Cir. 1977), *appeal after remand*, 612 F.2d 707 (2d Cir.), *cert. denied*, 449 U.S. 821, 66 L. Ed. 2d 23, 101 S. Ct. 80 (1980); *TRW, Inc. v. Federal Trade Commission*, 647 F.2nd 942, 954 (9th Cir. 1981)." *Id.* at 110.

FTC must connect the Proposed Order to possible or actual effects on competition through a careful analysis of "net effects." 15 U.S.C. § 45(n); *Int'l Harvester Co.*, 104 FTC 949, 1061, 1073-74 (1984); *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 248 (1972) ("The [Commission's] opinion is barren of any attempt to rest the order on its assessment of particular

competitive practices or considerations of consumer interests independent of possible or actual effects on competition. Nor were any standards for doing so referred to or developed"). However, it has failed to do so.

On the record of this case, there is no basis in law to require LabMD to comply with requirements such as establishing a "comprehensive information security program," hiring outside professionals to conduct biannual audits for twenty years, or hiring additional personnel to monitor the security of patient data without proof by a preponderance of the evidence that such data is being maintained in violation of HIPAA and/or in violation of Section 5, or at least has been since July 2010. *See Borg-Warner Corp.*, 746 F.2d at 110-11.

B. Complaint Counsel Failed To Prove That "Fencing-in" Relief Is Appropriate.

As a matter of law, "fencing-in" relief is inappropriate. *Borg-Warner Corp.*, 746 F.2d at 110-11 (FTC failed to bear its burden and justify relief because "speculative and conjectural" allegations were not sufficient to justify equitable relief against a terminated violation) and *Litton Indus., Inc. v. FTC*, 676 F.2d 364, 370 (9th Cir. 1982), should control here. As the Ninth Circuit ruled:

> Because fencing-in provisions are prophylactic, the ultimate question is the likelihood of the petitioner committing the sort of unfair practices they prohibit. Accordingly, "(a)mong the circumstances which should be considered in evaluating the relation between the order and the unlawful practice are whether the respondents acted in blatant and utter disregard of the law, and whether they had a history of engaging in unfair trade practices." We also consider whether the violations involved "a technique of deception that easily could be transferred to an advertising campaign for some other product"….[fencing-in orders] should be used with caution "because they alter the scheme of penalties and enforcement procedures defined by the Act."

Litton Indus., 676 F.2d at 370 (citations omitted). There is no evidence LabMD "acted in blatant and utter disregard of the law" or had "a history of engaging in unfair trade practices." Applying "fencing in" relief in this case therefore would be a clear abuse of discretion and unlawful.

Also, fencing-in relief "must be sufficiently clear that it is comprehensible to the violator, and must be 'reasonably related' to a violation of [Section 5]. To ensure that a fencing-in order bears a reasonable relationship to the unlawful practice found to exist, the Commission considers three factors: (1) the deliberateness and seriousness of the present violation; (2) the respondent's past history of violations; and (3) the transferabilty of the unlawful practices to other products. *Thompson Medical Products Co., Inc.*, 104 FTC 648, 833 (1984.)It must be "reasonably calculated to prevent future violations of the sort found to have been committed." *See ITT Continental Baking Co. v. FTC*, 532 F.2d 207, 221-22 (2d Cir. 1976).

The first factor for fencing-in relief is "the deliberateness and seriousness of the present violation." Complaint Counsel has failed to prove by a preponderance of the evidence a present violation, or that LabMD knowingly violates Section 5, or that the violations are "serious." *Compare In the Matter of Daniel Chapter One*, 2009 FTC LEXIS 157, at *281-282, *with In the Matter of POM Wonderful LLC*, 2012 FTC LEXIS 18, at *97-*98 (F.T.C. Jan. 11, 2012).[39]

The second factor is "history of prior violations." *See Thompson*, 104 FTC at 833. There are none. *See* CCPCL at ¶ 116.

The third factor is "the degree of transferability of the violation to other products." *See In re Daniel Chapter One*, 2009 FTC LEXIS 157, at *280-*281. As a matter of law, Complaint Counsel has failed to prove transferability in this case. Among other things, there is no evidence

[39] Complaint Counsel has not specified, much less proven, LabMD engaged in any alleged unfair and unlawful data security acts and practices post-July, 2010. But even if the alleged unfair and unlawful data security acts and practices in the period covered in Dr. Hill's report, January, 2005, through July, 2010, are deemed "present" violations under *Thompson*, FTC has never denied that LabMD's data security complied with HIPAA. A HIPAA-compliant data security program cannot be a "serious" violation of Section 5 without creating conflict with HIPAA, a conflict that would render Section 5 a nullity. *Credit Suisse Secs. LLC v. Billing*, 551 U.S. 264, 275-76 (2007). It is hard to believe the Commission would undercut its own authority by making such an irrational finding.

in this case that the alleged unfair and unlawful data security practices that supposedly occurred between January, 2005, and July, 2010, as specified in Dr. Hill's report, could reoccur. Given the ever-changing evolution in data security technology, this omission is fatal.

Fencing-in relief is therefore both unnecessary and unlawfully punitive in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370.

C. The Proposed Order Includes A Prohibited "Obey-The-Law" Provision.

Complaint Counsel's demanded relief includes a prohibited "obey-the-law" provision. *See* Compl. at ¶ 7-8; CCPTB at Addendum A. If FTC gave LabMD notice during the relevant time (2005-2010) that Section 5 required these things, as Complaint Counsel has argued, then the proposed order is an invalid "obey-the-law" provision. *SEC v. Goble*, 682 F.3d 934, 949 (11th Cir. 2012). If FTC did not give LabMD notice during the relevant time that Section 5 required these things, then, by definition, LabMD lacked constitutional fair notice.

Also, "an injunction based upon an erroneous conclusion of law is invalid." *Hughey v. JMS Dev. Corp.*, 78 F.3d 1523, 1531 (11th Cir. 1996). Injunctions (such as the proposed Order) "may not merely require someone to 'obey the law.'" *Id.* (citations omitted). "Broad, non-specific language that merely enjoins a party to obey the law or comply with an agreement" will not suffice:

> Here, the district court's order granting permanent injunctive relief only stated: Defendant shall not discharge stormwater into the waters of the United States from its development property in Gwinnett County, Georgia, known as Rivercliff Place *if such discharge would be in violation of the Clean Water Act*. (emphasis supplied).
>
> Not only was this an "obey the law" injunction, it was also incapable of enforcement as an operative command. The court's order merely required JMS to stop discharges, but failed to specify how JMS was to do so. Discharges, though not defined by the order, occurred only when it rained, and any discharge was a violation of the order. Rain water ran into the subdivision's government-approved streets and storm sewers; then into the small stream that started on the subdivision property; on into a tributary stream; and eventually into the Yellow River. Was JMS supposed to stop the rain from falling? Was JMS to build a retention pond to slow and control discharges? Should JMS have constructed a treatment plant to comply with the requirements of the CWA?

> The injunction's failure to specifically identify the acts that JMS was required to do or refrain from doing indicates that the district court–like the CWA, the EPA, Georgia EPD, and Mr. Hughey–was incapable of fashioning an operative command capable of enforcement. As such, we must vacate this "obey the law" injunction.

Id. at 1531-32.

The Order commands LabMD to "obey the law" but leaves it to a private party – the "qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession" to specify what must be done. Thus, the Order is unlawful because of FTC's reliance on a private third party to develop and apply the "metrics and standards" of data security to LabMD. *Railroads*, 135 S. Ct. at 1233, 1236 (Alito, J. concurring); 1240-44 (Thomas, J., concurring). Or, it is unlawful because it commands only that LabMD "obey the law." *Hughey*, 78 F.3d at 1531-32; *see also, FTC v. Ruberoid Co.*, 343 U.S. 470, 492-93 (1952) (Jackson, J., dissenting) ("I cannot find that ten years of litigation have served any useful purpose whatever. No doubt it is administratively convenient to blanket an industry under a comprehensive prohibition in bulk – an undiscriminating prohibition of discrimination. But this not only fails to give the precision and concreteness of legal duties to the abstract policies of the Act, it really promulgates an inaccurate partial paraphrase of its indeterminate generalities. Instead of completing the legislation by an order which will clarify the petitioner's duty, it confounds confusion by literally ordering it to cease what the statute permits it to do.").

II. RESPONDENT'S REPLY TO SPECIFIC ORDER PROVISIONS.

A. Definitions.

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

Reply to Proposed Order Definition No. 1

LabMD has no specific reply to Proposed Order Definition No. 1.

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

Reply to Proposed Order Definition No. 2

LabMD has no specific reply to Proposed Order Definition No. 2.

3. "Affected Individual" shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before the date of service of this order, including, but not limited to, consumers listed in the Insurance File and the Sacramento Documents, but for purposes of Parts III.A and III.C of this Order excluding consumers listed in the Sacramento Documents to whom LabMD has already provided notice of the breach.

Reply to Proposed Order Definition No. 3

LabMD has no reason to believe the persons listed on the 1718 File were or reasonably could have been "accessible to unauthorized persons."

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

Reply to Proposed Order Definition No. 4

LabMD replies as follows to Proposed Order Definition No. 4.

As a matter of law, Complaint Counsel failed to prove that the insurance file or any other PHI or PII "was available to a peer-to-peer file sharing network through a peer-to-peer file sharing application installed on a computer on respondent's computer network." (Wallace, Tr. 1339-1391).

5. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first

and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.

Reply to Proposed Order Definition No. 5

LabMD has no specific reply to Proposed Order Definition No. 5.

6. "Sacramento Documents" shall mean the documents identified in Appendix A to Complaint Counsel's Complaint filed August 28, 2013.

Reply to Proposed Order Definition No. 6

LabMD has no specific reply to Proposed Order Definition No. 6.

B. Section I.

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

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

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

prevention, detection, and response to attacks, intrusions, or other systems failures;

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

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

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

Reply to Proposed Order Section I And Subparts A-E

LabMD replies as follows to Proposed Order Section I and Subparts A-E.

Section I is unlawful as (1) the Department of Health and Human Services ("HHS") is the regulatory authority mandated to supervise the activities in question; (2) ample evidence exists that HHS exercises that authority; and (3) a resulting risk arises that the Proposed Order and HIPAA'S Security Rule, *see* 45 C.F.R. Part 160 and Part 164 Subparts A and C (Security Rule), if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct. *See Credit Suisse Secs. LLC v. Billing*, 551 U.S. 264, 275-76 (2007). For instance, Section I essentially ignores the Security Rule's flexible approach by failing to take into account the costs involved in its Proposed Order. 45 C.F.R. § 164.306(b). Therefore, it is precluded "as given context and likely consequences, there is a 'clear repugnancy'" between the Proposed Order and HIPAA's Breach Notification Rule. *Billing*, 551 U.S. at 275. (citation omitted).

Section I is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370; *Jacob Siegel Co. v. Federal Trade Comm'n*, 327 U.S. 608, 613 (1946). Section 5 does not authorize FTC to "aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79.

Section I is unlawful because it is does not state why it was issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d). This command of specificity is a reflection of the seriousness of the consequences that may flow from a violation of an injunctive order. *See Pasadena City Board of Education v. Spangler*, 427 U.S. 424, 438-39 (1976).

The list of offending words and phrases, jointly and severally and/or *in toto*, includes:

- **comprehensive information security program**
- **reasonably designed** to protect
- **security, confidentiality, and integrity** of personal information
- **collected from or about consumers**
- by respondent or by any corporation, subsidiary, division, **website, or other device or affiliate owned or controlled by respondent**
- Such **program, the content and implementation of which must be fully documented in writing,** shall contain **administrative, technical, and physical safeguards**
- **appropriate** to respondent's **size and complexity**
- **the nature and scope of respondent's activities**
- the **sensitivity** of the personal information **collected from or about consumers**
- **the designation of an employee or employees to coordinate and be accountable for the information security program**
- **the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any**

safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures

- **the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures**
- **the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards**
- **the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.**

Every one of these words and phrases are too broad, vague, and without context to allow LabMD to assign any specific meaning to them such that the specific behavior that Complaint Counsel seeks to enjoin is impossible to discern.

First, FTC has never articulated any standards or guidance of any kind relating to medical data security. Second, FTC is preempted by HHS/CMS and HIPAA/HITECH in clamoring for any "future relief" as applied to LabMD, a covered entity under HIPAA. Third, the terms in Complaint Counsel's proposed order have never even been defined by FTC in this case—how is any respondent expected to adhere to imaginary guidelines and avoid putative "prohibited" courses of conduct without knowing in advance what those might be?

All of Complaint Counsel's terms in the proposed order as set forth by LabMD herein are akin to the word "discriminating" in *Payne v. Travenol Laboratories*, which "like the word 'monopolizing' in *Schine Chain Theatres, Inc. v. United States*, 334 U.S. 110, 125-26, (1948), is too general." *Payne v. Travenol Laboratories, Inc.*, 565 F.2d 895, 898 (5th Cir. 1978); *see also Meyer v. Brown & Root Constr. Co.*, 661 F.2d 369, 373 (5th Cir. 1981) (citing *Int'l*

Longshoremen's Assoc. v. Philadelphia Marine Trade Assoc., 389 U.S. 64, 76 (1967)). "Such 'obey the law' injunctions cannot be sustained. *See, e.g., NLRB v. Express Publishing Co*., 312 U.S. 426, 435-36, 61 S. Ct. 693, 85 L. Ed. 930 (1941); *Russell C. House Transfer & Storage Co. v. United States*, 189 F.2d 349, 351 (5th Cir. 1951)." *Id.*; *see also SEC v. Smyth*, 420 F.3d 1225, 1233 n.14 (11th Cir. 2005); *Burton v. City of Belle Glade*, 178 F.3d 1175, 1200 (11th Cir. 1999); *Florida Ass'n of Rehab. Facilities, Inc. v. Fla. Dep't of Health and Rehabilitative Servs.*, 225 F.3d 1208, 1222-23 (11th Cir. 2000). As the Supreme Court held in *Schine*, "[t]he public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined." 334 U.S. at 125-26.

Accordingly, Complaint Counsel's demanded relief should be denied for the following: Section I and Subparts A-E; Section II and Subparts A-D; Section III and Subparts A-C; Section IV and Subparts A-B; Section V; Section VI; Section VII; and, Section VIII and Subparts A-C.

C. Section II.

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

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

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

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

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

Reply to Proposed Order Section II And Subparts A-D

LabMD replies as follows to Proposed Order Section II and Subparts A-D.

Section II requires LabMD to retain a "third-party professional" to develop and apply "the metrics and standards" of data security. These metrics and standards will have a coercive effect on LabMD, which is regulatory power. FTC's Order is therefore an unlawful violation of Article I, and the Appointments Clause, separation of powers, and due process. *See Railroads*, 135 S. Ct. at 1225, 1231-36 (2015).

Section II is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*,

676 F.2d at 370; *Jacob Siegel Co.*, 327 U.S. at 613 (1946). Section 5 does not authorize FTC to "aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79.

Section II is unlawful because it is does not state why it was issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d); *Pasadena City Board of Education*, 427 U.S. at 438-39; *Payne*, 565 F.2d at 897. As the Supreme Court held in *Schine*, "The public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined." 334 U.S. at 125-26.

Problematic provisions include:

- in connection with **its compliance with Part I of this order**
- respondent shall obtain **initial and biennial assessments and reports ("Assessments")**
- **qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession**
- **Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute**
- **a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580**
- **Each Assessment shall: set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period**
- **explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers**

- **explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order**
- **certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period**
- **Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared**
- **All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment**
- **Any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No.1023099**

In all other respects, in reply to Complaint Counsel's proposed order Section II and Subparts A-D, as a matter of fact and law, LabMD asserts and adopts as if fully set forth herein its reply to Section I and Subparts A-E, *supra.*

D. Section III.

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

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

1. a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.), and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

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

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

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

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

Reply to Proposed Order Section III And Subparts A-C

LabMD replies as follows to Proposed Order Section III and Subparts A-C.

Section III is unlawful as (1) HHS is the regulatory authority mandated to supervise the activities in question; (2) ample evidence exists that HHS exercises that authority; and (3) a resulting risk arises that the Proposed Order and HIPAA'S Breach Notification Rule, *see* 45 CFR §§ 164.400-414, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct. *See Billing*, 551 U.S. at 275-76. Therefore, it is precluded "as given context and likely consequences, there is a 'clear repugnancy'" between the Proposed Order and HIPAA's Breach Notification Rule. *Billing*, 551 U.S. at 275. (citation omitted).

Section III is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370; *Jacob Siegel Co.*, 327 U.S. at 613. Section 5 does not authorize FTC to

"aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79.

Section III is unlawful because it is does not state why it was issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d); *Pasadena City Board of Education*, 427 U.S. at 438-39; *Payne*, 565 F.2d at 897. As the Supreme Court held in *Schine*, "[t]he public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined." 334 U.S. at 125-26.

Problematic provisions include:

- Respondent shall provide **notice** to **Affected Individuals** and **their health insurance companies** within 60 days of service of this order unless an **appropriate notice** has **already been provided.**
- Respondent shall send the **notice** to **each Affected Individual** by first class mail, only after obtaining **acknowledgment from the Commission or its staff that the form and substance of the notice satisfies the provisions of the order.** The **notice must be easy to understand and must include:**
- **a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.), and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures**
- **advice on how Affected Individuals can protect themselves from identity theft or related harms. Respondent may refer Affected Individuals to the Commission's identity theft website (www.ftc.gov/idtheft), advise them to contact their health care providers or insurance companies if bills don't arrive on time or contain irregularities, or to obtain a free copy of their credit report from www.annualcreditreport.com and monitor it and their accounts for suspicious activity, or take such other steps as respondent deems appropriate**
- **Respondent shall send a copy of the notice to each Affected Individual's health insurance company** by first class mail

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

In all other respects, in reply to Complaint Counsel's proposed order Section III and Subparts A-C, as a matter of fact and law, LabMD asserts and adopts as if fully set forth herein its reply to Section I and Subparts A-E, *supra.*

E. Section IV.

> **IT IS FURTHER ORDERED** that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:
>
> A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, notice letters required by Part III of this order and documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
>
> B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

Reply to Proposed Order Section IV And Subparts A-B

LabMD replies as follows to Proposed Order Section IV and Subparts A-B.

Section IV is unlawful as (1) HHS is the regulatory authority mandated to supervise the activities in question; (2) ample evidence exists that HHS exercises that authority; and (3) a resulting risk arises that the Proposed Order and HIPAA'S Security and Breach Notification Rules, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct. *See Billing*, 551 U.S. at 275-76. Therefore, it is precluded "as given context and likely consequences, there is a 'clear repugnancy'" between the Proposed Order and HIPAA's

Security and Breach Notification Rules. *Billing*, 551 U.S. at 275 (citation omitted) (*Compare* 45 CFR Part 160 (establishing HHS principles of cooperation with HIPPA entities to help achieve compliance) and Part 164 Subparts A and C (Security Rule) (focusing on a flexible approach to data security); 45 C.F.R. § 164.316(b) (retain general compliance documentation for six years and make available to persons needing to implement procedures) (45 C.F.R. §§ 164.400-414 (Breach Notification Rule) (no requirement for onerous breach-related multi-year reporting to agency)).

Section IV is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370; *Jacob Siegel Co.*, 327 U.S. at 613. Section 5 does not authorize FTC to "aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79.

Section IV is unlawful because it is does not state why it was issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d); *Pasadena City Board of Education*, 427 U.S. at 438-39; *Payne*, 565 F.2d at 897. As the Supreme Court held in *Schine*, "The public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined."
334 U.S. at 125-26.

Problematic provisions include:

- **for a period of five (5) years,** a print or electronic copy of **each document relating to compliance**

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

In all other respects, in reply to Complaint Counsel's proposed order Section IV and Subparts A-B, as a matter of fact and law, LabMD asserts and adopts as if fully set forth herein its reply to Section I and Subparts A-E, *supra.*

F. Section V.

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

Reply to Proposed Order Section V

LabMD replies as follows to Proposed Order Section V.

Section V is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370; *Jacob Siegel Co.*, 327 U.S. at 613. Section 5 does not authorize FTC to "aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in

retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79.

Section V is unlawful because it is does not state why it was issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d); *Pasadena City Board of Education*, 427 U.S. at 438-39; *Payne*, 565 F.2d at 897. As the Supreme Court held in *Schine*, "The public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined." 334 U.S. at 125-26.

Problematic provisions include:

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

In all other respects, in reply to Complaint Counsel's proposed order Section V, as a matter of fact and law, LabMD asserts and adopts as if fully set forth herein its reply to Section I and Subparts A-E, *supra.*

G. Section VI.

> **IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which

> respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

Reply to Proposed Order Section VI

LabMD replies as follows to Proposed Order Section VI.

Section VI is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370; *Jacob Siegel Co.*, 327 U.S. at 613. Section 5 does not authorize FTC to "aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79.

Section VI is unlawful because it is does not state why it issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d); *Pasadena City Board of Education*, 427 U.S. at 438-39; *Payne*, 565 F.2d at 897. As the Supreme Court held in *Schine*, "The public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined."

334 U.S. at 125-26.

Problematic provisions include (in bold):

- **Respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address**.

In all other respects, in reply to Complaint Counsel's proposed order Section VI, as a matter of fact and law, LabMD asserts and adopts as if fully set forth herein its reply to Section I and Subparts A-E, *supra.*

H. Section VII.

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

Reply to Proposed Order Section VII

LabMD replies as follows to Proposed Order Section VII.

Section VII is unlawful as (1) HHS is the regulatory authority mandated to supervise the activities in question; (2) ample evidence exists that HHS exercises that authority; and (3) a resulting risk arises that the Proposed Order and HIPAA'S Security and Breach Notification Rules, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct. *See Billing*, 551 U.S. at 275-76. Therefore, it is precluded "as given context and likely consequences, there is a 'clear repugnancy'" between the Proposed Order and HIPAA's

Security and Breach Notification Rules. *See Billing*, 551 U.S. at 275. (citation omitted) (*Compare* 45 CFR Part 160 and Part 164 Subparts A and C (Security Rule) (focusing on a flexible approach to data security); 45 CFR §§ 164.400-414 (Breach Notification Rule) (requiring notification, but not compliance reporting, to HHS secretary only)).

Section VII is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370; *Jacob Siegel Co.*, 327 U.S. at 613. Section 5 does not authorize FTC to "aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79.

Section VII is unlawful because it is does not state why it was issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d); *Pasadena City Board of Education*, 427 U.S. at 438-39; *Payne*, 565 F.2d at 897. As the Supreme Court held in *Schine*, "The public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined." 334 U.S. at 125-26.

Problematic provisions include (in bold):

- Respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, **setting forth in detail the manner and form of their compliance with this order.** Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit **additional true and accurate written reports.**

In all other respects, in reply to Complaint Counsel's proposed order Section VII, as a matter of fact and law, LabMD asserts and adopts as if fully set forth herein its reply to Section I and Subparts A-E, *supra.*

I. Section VIII.

> This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:
>
> A. any Part in this order that terminates in less than twenty (20) years;
>
> B. this order's application to any respondent that is not named as a defendant in such complaint; and
>
> C. this order if such complaint is filed after the order has terminated pursuant to this Part.
>
> Provided, further, that if such complaint is dismissed or a federal court rules that each respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Reply to Proposed Order Section VIII

LabMD replies as follows to Proposed Order Section VIII.

Section VIII is unlawful as (1) HHS is the regulatory authority mandated to supervise the activities in question; (2) ample evidence exists that HHS exercises that authority; and (3) a resulting risk arises that the Proposed Order and HIPAA'S Security and Breach Notification Rules, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct. *See Billing*, 551 U.S. at 275-76. Therefore, it is precluded "as given context and likely consequences, there is a 'clear repugnancy'" between the Proposed Order and HIPAA's

Security and Breach Notification Rules. *Billing*, 551 U.S. at 275. (citation omitted) (*Compare* 45 CFR Part 160 and Part 164 Subparts A and C (Security Rule) (focusing on a flexible approach to data security); 45 CFR §§ 164.400-414 (Breach Notification Rule) (establishing standards for corrective action and notification to the public and to HHS)).

Section VIII is unlawful because it is not reasonably related to the specific "unlawful practices" found to exist in this case. *Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus., Inc.*, 676 F.2d at 370; *Jacob Siegel Co.*, 327 U.S. at 613. Section 5 does not authorize FTC to "aggregate" practices and declare them unfair and then unlawful. 15 U.S.C. §§ 45(a), (n). As previously argued, there is no basis for FTC to demand this sanction and it is offered only in retaliation and to punish LabMD and Mr. Daugherty for their refusal to accede to FTC's demands. *See* CCPCL at ¶ 79. The twenty-year duration, for a business without any prior violations and that has never been alleged to have violated applicable HIPAA regulations, is particularly offensive.

Section VIII is unlawful because it is does not state why it was issued, state its terms specifically, and describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required. *See* Fed.R.Civ.P. 65(d); *Pasadena City Board of Education*, 427 U.S. at 438-39; *Payne*, 565 F.2d at 897. As the Supreme Court held in *Schine*, "The public interest requires that a more specific decree be entered on this phase of the case. The precise practices found to have violated the act should be specifically enjoined." 334 U.S. at 125-26.

Problematic provisions include (in bold):

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

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

In all other respects, in reply to Complaint Counsel's proposed order Section VIII, as a matter of fact and law, LabMD asserts and adopts as if fully set forth herein its reply to Section I and Subparts A-E, *supra.*

III. RESPONDENT'S PROPOSED ORDER.

Based on controlling law and the record in this case, this is the only Order that is appropriately issued:

> **IT IS ORDERED** that *In the Matter of LabMD, Inc.*, Docket No. 9357, is dismissed with prejudice; and
>
> **IT IS FURTHER ORDERED** that judgment for Respondent shall be entered.

But even if, contrary to the controlling law and the record in this case, this Court or the Commission were to find that LabMD presently violates Section 5's unfairness provision, then this is the only Order that could be lawfully issued:

> **IT IS ORDERED** that the respondent shall, no later than ninety (90) days after the date of service of this order, establish and implement, and thereafter maintain reasonable data security based on prevailing medical industry standards for companies of its nature, size and location, to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent.

Notice of Electronic Service

I hereby certify that on September 04, 2015, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s Reply Brief to Complaint Counsel's Post-Trial Brief , with:

D. Michael Chappell
Chief Administrative Law Judge
600 Pennsylvania Ave., NW
Suite 110
Washington, DC, 20580

Donald Clark
600 Pennsylvania Ave., NW
Suite 172
Washington, DC, 20580

I hereby certify that on September 04, 2015, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s Reply Brief to Complaint Counsel's Post-Trial Brief , upon:

John Krebs
Attorney
Federal Trade Commission
jkrebs@ftc.gov
Complaint

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Jarad Brown
Attorney
Federal Trade Commission
jbrown4@ftc.gov
Complaint

Kent Huntington
Counsel
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Sunni Harris
Esq.
Dinsmore & Shohl LLP
sunni.harris@dinsmore.com
Respondent

Daniel Epstein
Cause of Action
daniel.epstein@causeofaction.org
Respondent

Patrick Massari
Counsel
Cause of Action
patrick.massari@causeofaction.org
Respondent

Alain Sheer
Federal Trade Commission
asheer@ftc.gov
Complaint

Laura Riposo VanDruff
Federal Trade Commission
lvandruff@ftc.gov
Complaint

Megan Cox
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Federal Trade Commission
rmehm@ftc.gov
Complaint

Erica Marshall
Counsel
Cause of Action
erica.marshall@causeofaction.org
Respondent

Patrick Massari
Attorney