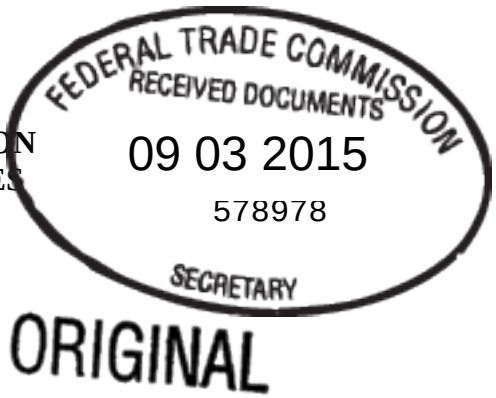

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

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

ORIGINAL

RESPONDENT LABMD, INC.'S REPLY TO COMPLAINT COUNSEL'S CONCLUSIONS OF LAW

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 3, 2015

TABLE OF CONTENTS

1. RESPONDENT LABMD, INC.'S REPLY TO COMPLAINT COUNSEL'S PROPOSED CONCLUSIONS OF LAW

1.1 Burden of Proof

1. Rule 3.43(a) states that "Counsel representing the Commission … shall have the burden of proof," except as to a factual propositions put forward by another proponent, such as affirmative defenses. 16 C.F.R. § 3.43; *see also* Administrative Procedure Act, 5 U.S.C. § 556(d); JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2).

Reply to Proposed Conclusion of Law No. 1

LabMD has no specific response to Proposed Conclusion of Law No. 1.

2. The standard of proof is preponderance of the evidence. *Daniel Chapter One*, Docket No. 9329, 2009 FTC LEXIS 157, at *134-35 (Aug. 5, 2009) (collecting cases); JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2-3).

Reply to Proposed Conclusion of Law No. 2

Complaint Counsel's Proposed Conclusion of Law No. 2 is incomplete.

Complaint Counsel's burden of proof is, at a minimum, a preponderance of the evidence. *See In re N.C. Bd. of Dental Exam'rs*, No. 9343, 2011 FTC LEXIS 137 at *11-12 (F.T.C. July 14, 2011); *In re Auto. Breakthrough Scis., Inc.*, No. 9275, 1998 FTC LEXIS 112, at *37 n.45 (F.T.C. Sept. 9, 1998) (holding that each finding must be supported by a preponderance of the evidence in the record). However, the preponderance standard is arguably inconsistent with a common meaning construction of 15 U.S.C. § 45(a). "The language of the statute itself implies the enactment of a standard of proof." *Steadman v. SEC*, 450 U.S. 91, 98 (1981). Webster's primary definition of "likely" is "having a high probability of occurring or being true: very probable (rain is likely today)." *See* Merriam-Webster's Dictionary, http://www.merriam-webster.com/dictionary/likely (last visited Sept. 3, 2015). The Ninth Circuit has defined "likely" as "probable." *See Sw. Sunsites v. FTC*, 785 F.2d 1431, 1436 (9th Cir. 1985). Therefore, Complaint Counsel should be required to prove its case by clear and convincing

evidence. *Colorado v. New Mexico*, 467 U.S. 310, 316 (1984) (holding that a "highly probable" burden requires "clear and convincing" evidence).

Requiring Complaint Counsel to prove causation and injury by clear and convincing evidence is consistent with Congressional intent. *See* S. Com. Rep. 103-130 at 13 ("The Committee believes [Section 5(n)] is necessary in order to provide the FTC, its staff, regulated business, and reviewing courts greater guidance on the meaning of unfairness and to prevent a future FTC from abandoning the principles of the December 17, 1980, and March 5, 1982, letters[.]"); Ernest Gellhorn, *Trading Stamps, S&H, and the FTC's Unfairness Doctrine*, 1983 Duke L.J. 903, 906, 942 (1983) (noting FTC's abuse of its Section 5 unfairness jurisdiction).

3. Complaint Counsel has the burden of proof to prove by a preponderance of the evidence that LabMD's practices are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 3).

Reply to Proposed Conclusion of Law No. 3

Complaint Counsel's Proposed Conclusion of Law No. 3 is misleading, confusing, and incomplete.

The Commission does not sit as or with the authority of a court of equity. Instead, it exercises only Congressionally-delegated administrative functions and not judicial powers. *FTC v. Eastman Kodak*, 274 U.S. 619, 623 (1927); *Fox v. Clinton*, 684 F.3d 67, 75-77 (2012). Section 5 therefore provides the burden of proof and standard for review. *Steadman*, 450 U.S. at 98.

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) are relevant to this case 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 therefore 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.

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. *See* 15 U.S.C. § 45(a); *Yates*, 135 S. Ct. at 1081-83, 1091; *Carr v. United States*, 560 U.S. 438, 448 (2010); *Meyer*, 510 U.S. at 477; *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 U.S. App. LEXIS 14839, at *15-17, *54-55 (3rd Cir. Mar. 3, 2015); Merriam-Webster's Dictionary, "Unfair," http://www.merriam-webster.com/dictionary/unfair (last visited Step. 3, 2015).

Second, Section 5(n) provides that "[t]he Commission lacks 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 is not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (emphasis added). 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.

As to the first element, this means Complaint Counsel must prove by a preponderance of the evidence that injury is occuring now or "likely" to occur in the future. *See* 15 U.S.C. § 15(n); 1 U.S.C. § 1; *Carr*, 560 U.S. at 448; *Gwaltney of Smithfield v. Chesapeake Bay Found.*, 484 U.S. 49, 57 (1987); *Steadman*, 450 U.S. at 98. *But see* Compl. ¶ 22 ("As set forth in Paragraphs 6 through 21, respondent's [*sic*] failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information . . . *caused, or is likely to cause*, substantial injury to consumers . . . .") (emphasis added). "Likely" should be given its ordinary meaning. Webster's primary definition of "likely" is "having a high probability of occurring or being true: very probable (rain is likely today)." *See* Merriam-Webster's Dictionary, http://www.merriam-webster.com/dictionary/likely. The Ninth Circuit has defined "likely" as "probable." *See Sw. Sunsites*, 785 F.2d at 1436.

As to the second element, Complaint Counsel must prove by a preponderance of the evidence that an "injury" is "substantial." This initially requires a showing of 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 Breach 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 harm is plainly different from certainly impending harm, and certainly impending harm 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.

Even if an unfair act or practice causes a Section 5(n) injury, the injury must also be proven "substantial" to be declared unlawful. 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.'"); *In re Int'l Harvester Co*., 104 F.T.C. 949, 1071 (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."); S. Rep. No. 75-22 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."); *United States v. Am. Bldg. Maint. Indus.*, 422 U.S. 271, 277 (1975); *Int'l Harvester Co.*, 104 F.T.C. at 1075; J. Howard Beales, Former Dir., Fed. Trade Comm'n, Speech: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, at § II (May 30, 2003) (unfairness authority is "a powerful tool for the Commission" to attack practices that "cause ***widespread and significant consumer harm***") (emphasis added), *available at* https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

As to the third element, Complaint Counsel must prove by a preponderance of the evidence that a substantial injury is not "reasonably avoidable by the consumers themselves." Even if an act or practice is "unfair" under Section 5(a), and causes or is likely to cause substantial injury, it may not be declared unlawful "if consumers are aware of, and are reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact." *Davis v. HSBC Bank Nevada*, 691 F.3d 1152, 1168-69 (9th Cir. 2012). *Davis* framed the issue as "not whether subsequent mitigation was convenient or costless, but whether it was reasonably possible." *Id.*; *see also Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007) ("[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 to the fourth element, even if an act or practice is "unfair" under Section 5(a), and causes or is likely to cause substantial injury which is not reasonably avoidable by the consumers themselves, Complaint Counsel must prove the substantial injury "is not outweighed

by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Section 5(n) requires FTC to conduct a countervailing benefit analysis, including not only the relative costs and benefits of the "unfair" act or practice 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 that would flow from government action. *Int'l Harvester Co.*, 104 F.T.C. at 1070, 1073-74. This means Complaint Counsel must prove by a preponderance of the evidence "net consumer injury," in other words, that government action does more good than harm. *See id.* at 1070, 1076; *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1115 (S.D. Cal. 2008) (FTC offered expert testimony that the defendants' business model did not provide any advantage and that any benefits were small, that it did not have a positive impact in the marketplace and did not benefit competition); 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.").

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 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.

On the evidence, Complaint Counsel has failed to carry its burden of proving that any of LabMD's data security practices are, or ever were, "unfair" under Section 5(a). It has also failed to prove that those practices, if unfair, may be declared unlawful under Section 5(n). As a result, the case against LabMD should be dismissed.

4. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 4

LabMD has no specific response to Proposed Conclusion of Law No. 4.

1.2 Jurisdiction

5. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). The act defines "commerce" as, *inter alia*, "commerce among the several States." *Id*. § 44.

Reply to Proposed Conclusion of Law No. 5

Complaint Counsel's Proposed Conclusion of Law No. 5 is incomplete and misleading.

First, Section 5(a) cannot be read in isolation from Section 5(n).

Second, the Commission's Section 5 authority must be viewed in the light of other relevant statutes, "particularly where Congress has spoken subsequently and more specifically to the topic at hand." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000). In this case, the Commission seeks to subject a Health Insurance Portability and Accountability Act ("HIPAA") "covered entity" to Section 5. However, FTC may not do so if there is a risk of conflicting guidance, requirements, or standards of conduct with the HIPAA Security Rule, 68 Fed. Reg. 8334 (Feb. 20, 2003). *See Credit Suisse Secs. (USA) LLC v. Billing*, 551 U.S. 264, 272-73 (2007).

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." *Credit Suisse*, 571 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. 45 C.F.R. § 164.302 ("A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity."); 45 C.F.R. § 160.103 (definition of a "covered entity").

As a matter of law, FTC does not have the power to declare – for the first time through adjudication – conduct that is permitted by and compliant with HHS's preexisting regulatory scheme, promulgated in accordance with an Act of Congress, unfair and unlawful under Section

5. *Accord Wyndham*, 2015 U.S. App. LEXIS 14839 at *39-41 (discussing agency's obligation to provide fair notice and "ascertainable certainty"); *Ford Motor Co. v. FTC*, 673 F.2d 1008 (9th Cir. 1981); *NLRB v. Bell Aerospace Co.*, 416 U.S. 267 (1974). Consequently, FTC is precluded from exercising Section 5 authority against LabMD.

6. Respondent has engaged in "commerce," as defined in the FTC Act. JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2. Respondent has admitted that it tested samples from numerous states, including Alabama, Mississippi, Florida, Georgia, Missouri, Louisiana, and Arizona. Ans. ¶ 5; CX0766 (LabMD's Resps. and Objs. To Reqs. For Adm.) at 3, Adm. 8-12. Furthermore, the consumers whose samples Respondent tested and from whom Respondents collects payments are "located throughout the United States." CX0766 (LabMD's Resps. and Objs. To Reqs. For Adm.) at 3, Adms. 9-12; CX0088 (*in camera*) (LabMD Copied Checks) at 1-10; CX0726 (Maxey, SUN Designee, Dep. at 17-31); CX0718 (Hudson, Dep. at 131-33); CX0722 (Knox, Dep. at 19); CX0706 (Brown, Dep. at 146-47); CX0715-A (Gilbreth, Dep. at 6); CX0713-A (Gardner, Dep. at 27-29); CX0714-A ([Fmr. LabMD Empl.], Dep. at 35-36). Respondent's practices are thus "in or affecting commerce." *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 17 (rejecting Respondent's "frivolous" argument that its conduct does not meet the definition of "commerce" based on allegation that it tested samples from consumers throughout the United States and Respondent's admission that LabMD test samples sent from six states outside of Georgia); *see also P.F. Collier & Son Corp. v. FTC*, 427 F.2d 261, 272 (6th Cir. 1970) (holding that the nationwide scopes of operations imparted the requisite interstate character).

Reply to Proposed Conclusion of Law No. 6

LabMD has no specific response to Proposed Conclusion of Law No. 6.

7. The Commission has jurisdiction over persons, partnerships, and corporations. 15 U.S.C. § 45(a)(2). A "corporation" is defined in Section 4 of the FTC Act as "any company . . . which is organized to carry on business for its own profit or that of its members[.]" 15 U.S.C. § 44. LabMD is a privately-held corporation organized under the laws of the state of Georgia. *Supra* CCFF § 4.2 (Corporate Structure) (¶¶ 54-55). The Commission has jurisdiction over LabMD, a corporation.

Reply to Proposed Conclusion of Law No. 7

The last sentence of Complaint Counsel's Proposed Conclusion of Law No. 7 is

erroneous. LabMD is indeed a Georgia corporation. However, it does not follow that the Commission has jurisdiction over it.

First, the Commission lacks jurisdiction because it has violated the Appointments Clause. U.S. Const., Art. II, § 2, cl. 2; *Freytag v. Comm'r of Internal Revenue*, 501 U.S. 868, 881 (1991); *Buckley v. Valeo*, 424 U.S. 1, 144 (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).

Second, FTC's exercise of Section 5 jurisdiction over LabMD violates due process because it has failed to provide fair notice and apply medical industry standards. *Wyndham*, 2015 U.S. App. LEXIS 14839 at *39-41 (agency must provide "ascertainable certainty"); *Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1084 (D.C. Cir. 2007); *Ensign-Bickford Co. v. OSHRC*, 717 F.2d 1419, 1422 (D.C. Cir. 1983); *S&H Riggers & Erectors Inc. v. OSHRC*, 659 F.2d 1273, 1280-83 (5th Cir. 1981) (reasonable-person standard divorced from relevant industry standards or regulations violates due process); *Diebold, Inc. v. Marshall*, 585 F.2d 1327, 1333 (6th Cir. 1978). It is arbitrary, capricious, contrary to law, and a violation of due process for Complaint Counsel to allege and/or the Commission to determine unreasonableness without specific reference to HIPAA/HITECH regulations. *See Fabi Constr. Co.*, 508 F.3d at 1084; *Ensign-Bickford Co.*, 717 F.2d at 1422; *S&H Riggers*, 659 F.2d at 1280-83.

Third, *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 proceeding by the Commission is a question subject to judicial review.") (citation omitted). Complaint Counsel has failed to introduce evidence proving 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. 146-70, 186-88); (CX 0703 (Boback, Dep. at 142)); (RX 541 (Boback, Dep. at 37-41)); (RX 525 (Kaufman, Dep. at 20)).

Fourth, LabMD is a HIPAA-covered entity. 45 C.F.R. § 160.103. HHS regulates medical data security. *See* 68 Fed. Reg. at 8334. If there is a risk of conflict between Section 5 and HIPAA, *i.e.*, that Section 5 could prohibit what HIPAA allows, as the evidence (including Dr. Hill's testimony and the proposed order) shows that it does in this case, then Section 5 must yield and FTC lacks jurisdiction. *Brown & Williamson*, 529 U.S. at 133; *Credit Suisse*, 551 U.S. at 272-73.

8. Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a)(1).

Reply to Proposed Conclusion of Law No. 8

This is a variation of Complaint Counsel's Proposed Conclusion of Law No. 5, and so LabMD repeats its response thereto.

9. The Commission's authority to take action against unfair acts or practices ("unfairness") under Section 5 of the FTC Act extends to unreasonable data security practices. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 2 ("LabMD's Motion to Dismiss . . . calls on the Commission to decide whether the FTC Act's prohibition of 'unfair . . . acts or practices' applies to a company's failure to implement reasonable and appropriate data security measures. We conclude that it does."); *FTC v. Wyndham Worldwide Corp.*, 2014 WL 1349019 at *6-9 (D.N.J. Apr. 7, 2014) (concluding that Section 5 authority extends to data security).

Reply to Proposed Conclusion of Law No. 9

Complaint Counsel's Proposed Conclusion of Law No. 9 is erroneous, misleading, and incomplete.

First, FTC's authority extends only to acts or practices that are "unfair" under Section 5(a). To declare such unfair acts or practices unlawful, FTC must prove all of the Section 5(n) elements.

Second, FTC may not exercise Section 5 authority if it creates a risk of conflict with HIPAA, as the facts show that it does in this case. *Credit Suisse*, 551 U.S. at 272-73; *compare* RPFF ¶¶ 330-34, 333 (sic) - 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). Also, the mandatory and generally applicable standards cited by Complaint Counsel are not flexible and "technology neutral," as HIPAA requires. *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 C.F.R. §§ 164.400-414 (the HIPAA breach notification rule, providing detailed instructions and criteria for notification that differ from FTC's proposed relief). The Commission ruled there was not a facial conflict between Section 5 and HIPAA. However, it did not have all of these conflicts and inconsistencies before it, nor did it address these matters, and therefore, this Court may rule on the issue.

Third, FTC must provide *ex ante* "ascertainable certainty" of the standards that it will apply to declare conduct permitted or prohibited under Section 5. *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) ("Just as in the First Amendment context, the due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Wyndham*, 2015 U.S. App. LEXIS 14839 at *39-41. "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) ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement"); *see 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, 1305-06 (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."). Also, 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" that define with specificity acts or practices that are unfair or deceptive acts or practices in or affecting commerce.

Fourth, 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." *Ensign-Bickford Co.*, 717 F.2d at 1422; *City of Chicago v. Morales,* 527 U.S. 41, 63-64 (1999).

Fifth, FTC does not have the power to declare – for the first time through adjudication – conduct that is permitted by and compliant with HHS's preexisting regulatory scheme, promulgated under HIPAA/HITECH in accordance with an act of Congress, unfair and unlawful under Section 5(a) and (n), respectively. *Accord Wyndham,* 2015 U.S. App. LEXIS 14839 at *39-41 (discussing agency's obligation to provide fair notice and "ascertainable certainty"); *Ford Motor Co.*, 673 F.2d 1008; *Bell Aerospace Co.*, 416 U.S. 267. FTC had to

judge LabMD's conduct by reference to applicable medical industry standards for businesses of LabMD's size and nature. *See Fabi Const. Co.*, 508 F.3d at 1088.

Finally, the law cited by Complaint Counsel establishes that the judicial predicate for any Section 5 data security case is at least two actual data breaches involving widespread and substantial actual consumer harm plus unreasonable data security practices. *See Wyndham*, 2015 U.S. App. LEXIS 14839 at *47 ("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."); *accord Int'l Harvester Co.*, 104 F.T.C. at 1061-62, 1064-66, 1073-74.

10. LabMD's unreasonable data security practices constitute unfair acts or practices within the scope of Section 5 of the FTC Act, 15 U.S.C. § 45.

Reply to Proposed Conclusion of Law No. 10

Complaint Counsel's Proposed Conclusion of Law No. 10 is inaccurate and misleading.

LabMD repeats and incorporates by reference its response to Proposed Conclusion of Law No. 3. Only data security practices that are "unfair" as that term is used in Section 5(a) – that is, marked by injustice, partiality, or deception – are potentially "unlawful." Then, an "unfair" act or practice may be declared "unlawful" only if FTC satisfies the Section 5(n) test. 15 U.S.C. §§ 45(a), (n); *Wyndham*, 2015 U.S. App. LEXIS 14839 at *14-19; *Yates*, 135 S. Ct. at 1081-83, 1091; *Carr*, 560 U.S. at 44; *Meyer*, 510 U.S. at 477. Notably, Section 5 uses the word "unreasonable" only with respect to avoidance of harm. *See* 15 U.S.C. § 45(n).

11. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 11

LabMD has no specific response to Proposed Conclusion of Law No. 11.

1.3 LabMD's Failure to Employ Reasonable Measures to Prevent Unauthorized Access to Personal Information Was, and Is, an Unfair Practice

12. An unfair practice is defined as one that "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." 15 U.S.C. § 45(n); JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2).

Reply to Proposed Conclusion of Law No. 12

Complaint Counsel's Proposed Conclusion of Law No. 12 is contrary to the statute.

First, LabMD repeates and incorporates by reference its response to Proposed Conclusion of Law No. 3.

Second, Section 5 does not specifically define the term "unfair." Therefore, it is given its ordinary meaning of "marked by injustice, partiality, or deception." 15 U.S.C. § 45(a); *Wyndham*, 2015 U.S. App. LEXIS 14839 at *14-19; *Yates*, 135 S. Ct. at 1081-83, 1091; *Carr*, 560 U.S. at 44; *Meyer*, 510 U.S. at 477; Merriam-Webster's Dictionary, "Unfair", http://www.merriamwebster.com/dictionary/unfair (last visited Aug. 9, 2015).

Section 5(n) provides that "[t]he Commission lacks 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 is not outweighed by countervailing benefits to consumers or to competition."

Consequently, Section 5(n) does not define unfairness, as Complaint Counsel contends. Instead, it serves to qualify and limit FTC's authority to declare "unfair" practices unlawful.

13. Congress deliberately delegated broad power to the FTC under Section 5 of the FTC Act to address unanticipated practices in a changing economy. *See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972); *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985); *see also* Comm'n Order Denying Resp't's Mot. to Dismiss at 6 (Jan. 16, 2014) (finding no evidence of "congressional intent to preserve inadequate data security practices that unreasonably injure consumers").

Reply to Proposed Conclusion of Law No. 13

Complaint Counsel's Proposed Conclusion of Law No. 13 is incomplete.

First, FTC's "power" is limited by Section 5 itself. That means it must prove Section 5(a) unfairness and then all of the Section 5(n) factors to lawfully exercise "power." The *Sperry* and *American Financial Services* cases predate 15 U.S.C. § 45(n), which was enacted to cabin, not expand, the Commission's unfairness authority, and so these cases need to be viewed and applied accordingly.

Second, FTC's "power" is also limited by its obligation to provide *ex ante* notice and ascertainable certainty of its standards, and by its duty to rationally link the facts of the case with to the exercise of such "power." *Wyndham*, 2015 U.S. App. LEXIS 14839 at *39-41; *see also* 5 U.S.C. § 552(a)(1)(D); *Fox Television*, 132 S. Ct. at 2317-18. As the Court held in *FTC v. Sperry & Hutchinson Co.*:

> [T]he Commission has not rendered an opinion which, by the route suggested, links its findings and its conclusions. The 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. . . . At the least the Commission has failed to "articulate any rational connection between the facts found and the choice made.

405 U.S. 233, 248-49 (1972).

Third, because LabMD is a HIPPA "covered entity," FTC's "power" may not create a risk of conflict with HIPAA's Security Rule. *Brown & Williamson*, 529 U.S. at 133; *Credit Suisse*, 551 U.S. at 272-73. The Commission has ruled that Section 5 does not facially create a "clear repugnace" with, or run the risk of conflict with, HIPAA. That is the law of the case. However, the Commission has not decided this question on an as-applied basis, and so this Court has the authority to decide the question.

14. The codification of unfairness established a cost-benefit analysis to evaluate whether practices are unfair. *See* 15 U.S.C. § 45(n) (requiring evaluation of the

likelihood of "substantial injury" and of "countervailing benefits"); J. Howard Beales III, Director, Bureau of Consumer Protection, Federal Trade Comm'n Remarks at the Marketing and Public Policy Conference: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003) ("[C]odification of those principles in 1994 re-established a cost/benefit analysis (injury to consumers not outweighed by countervailing benefits) as the test for unfairness.").

Reply to Proposed Conclusion of Law No. 14

LabMD has no specific response to Complaint Counsel's Proposed Conclusion of Law No. 14 except to note that the "codification of unfairness" is the plain language of Section 5(a) and Section 5(n).

15. As the Commission recently expressed it: "The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of the available tools to improve security and reduce vulnerabilities." Comm'n Statement Marking 50th Data Sec. Settlement (Jan 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

Reply to Proposed Conclusion of Law No. 15

Complaint Counsel's Proposed Conclusion of Law No. 15 is legally insufficient and should be stricken.

This "statement" was not promulgated in the Federal Register pursuant to the Commission's 15 U.S.C. § 57a authority, is not binding on LabMD, was not issued until after this case was filed, and is not a cognizable legal standard of any kind. *See* 5 U.S.C. § 552(a)(1)(D); *Fox Television*, 132 S. Ct. at 2317-18; *Am. Bus. Ass'n.*, 627 F.2d at 529; *Wilderness Soc'y*, 434 F.3d at 595-96.

16. As with the application of the reasonableness standard of care in any other circumstance, what constitutes reasonable data security practices for a company that maintains consumers' sensitive Personal Information will vary depending on the circumstances. *See FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) ("[T]he proscriptions in [Section] 5 are flexible, 'to be defined with particularity by the myriad of cases from the field of business.'") (internal

citations omitted); *Brock v. Teamsters Local Union No. 863*, 113 F.R.D. 32, 34 (D.N.J. 1986) (reasonableness under prudent man standard "tried on the individual facts of [the] case" in light of standards developed in case law); *In re Zappos.com, Inc.*, 2013 WL 4830497, at *3-4 (D. Nev. Sept. 9, 2013) (applying "reasonable and prudent person" standard in negligence case for failure to safeguard electronically held data). Reasonableness turns on the amount and sensitivity of the information the company handles (going to the magnitude of injury from unauthorized access to information) and the nature and scope of the firm's activities (going to the structure of the firm's network, how the network operates, the types of security vulnerabilities and risks it faces, and feasible protections). *Cf. FTC v Accusearch, Inc.*, 2007 WL 4356786 at *7 (D. Wyo. Sept. 28, 2007) (defendants "can reasonably be expected to know" the legal environment in which their industries operate).

Reply to Proposed Conclusion of Law No. 16

Complaint Counsel's Proposed Conclusion of Law No. 16 is erroneous as a matter of law, inaccurate, and misleading.

First, as a general matter, any "reasonableness" standard FTC might wish to impose must be in harmony with Section 5's plain language and cannot be construed in a way that violates LabMD's due process rights.

Second, if Complaint Counsel believes that "[r]easonableness turns on the amount and sensitivity of the information the company handles (going to the magnitude of injury from unauthorized access to information) and the nature and scope of the firm's activities (going to the structure of the firm's network, how the network operates, the types of security vulnerabilities and risks it faces, and feasible protections)," and that this standard applied to LabMD during the Relevant Time, then it must demonstrate Federal Register publication and/or dissemination by some other lawful means, so that LabMD and other medical companies had *ex ante* "ascertainable certainty" of this expectation and a basis for knowing that it applied to HIPAA "covered entites." *Wyndham*, 2015 U.S. App. LEXIS 14839 at *39-41; *see also* 5 U.S.C. § 552(a)(1)(D); *Fox Television*, 132 S. Ct. at 2317-18; *Am. Bus. Ass'n.*, 627 F.2d at 529;

S&H Riggers, 659 F.2d at 1285; *Ford Motor Co.*, 673 F.2d 1008; *Bell Aerospace Co.*, 416 U.S. 267. FTC had to judge LabMD's conduct by reference to applicable medical industry standards for businesses of LabMD's size and nature. *See Fabi Const. Co.*, 508 F.3d at 1088.

Third, medical data security "reasonableness" under Section 5, as a matter of law, is a matter of first impression. Section 5(n) does not define "unreasonable" data security acts or practices, nor does it even use the term. Therefore, there is no statutory basis for a "reasonableness" standard. *See Steadman*, 450 U.S. at 98. Regardless, reasonableness is not whatever requirement the Commission determines, *post facto*, to have applied as if it had been part of an existing regulation. Rather, reasonableness is an objective test that must be determined on the basis of evidence in the record, and "industry standards" are concrete and discernible standards applicable to a given company in its particular line of business. *See Fabi Constr. Co.*, 508 F.3d at 1084 (industry standards for a building construction company applied); *Ensign-Bickford Co.*, 717 F.2d at 1422 (industry standards for the pyrotechnic industry applied); *S&H Riggers*, 659 F.2d at 1280-83 (reasonable-person standard divorced from relevant industry standards or regulations violates due process); *Diebold*, 585 F.2d at 1333 ("[U]nless we embrace the untenable assumption that industry has been habitually disregarding a known legal requirement, we must conclude that the average employer has been unaware that the regulations required point of operation guarding.").

Fourth, due process requires the Commission to articulate and apply an *objective* and *industry-specific* "reasonableness" standard of care to Respondent before commencing action against it. 5 U.S.C. § 552(a)(1)(D); *see Fla. Mach. & Foundry v. OSHRC*, 693 F.2d 119, 120 (11th Cir. 1982) ("[A] standard of this generality requires only those protective measures which the employers' industry would deem appropriate . . . .") (emphasis added); *S&H Riggers*, 659

F.2d at 1285; *B&B Insulation v. OSHRC*, 583 F.2d 1364, 1370 (5th Cir. 1978) (industry-specific standard, *e.g.*, what is customary for sausage industry or roofing industry).

Fifth, if LabMD reasonably relied on experts to design and implement its information technology system, then its data security practices could not have been "unreasonable." *See R.P. Carbone Constr. Co. v. OSHRC*, 166 F.3d 815, 819-20 (6th Cir. 1998) (reasonable reliance on subcontractors who were experts relieves contractor from liability) (citation omitted). Complaint Counsel did not prove by a preponderance of the evidence that LabMD wrongfully relied on IT professionals, and so it cannot establish that LabMD acted unreasonably.

17. A company can reference the recommendations of government agencies, such as the National Institute of Standards and Technology ("NIST"), well-known private sources, such as the SANS Institute and other information technology training institutes, and manufacturers of the software and hardware the company uses for guidance on how to identify the risks and vulnerabilities they face, and select and maintain data security practices that are reasonable under their circumstances. *See* CX0740 (Hill Report) ¶¶ 60 & n.8, 74; Shields, Tr. 884-85; CX0738 (Shields Rebuttal Report) ¶ 40; *supra* CCFF § 6.2 (Comprehensive Information Security Program) (¶¶ 1121-1124). NIST, for example, has published materials on a wide variety of information security topics, including basic security practices and risk assessment methods that can be tailored to the circumstances. *See* CX0740 (Hill Report) ¶ 74 & n.25. Similarly, the SANS Institute has since 2001 annually published and updated a free, easily accessible list of the most critical security vulnerabilities confronting firms, security professionals, and law enforcement. The compilation includes reference materials, information about new vulnerabilities, security measures that companies may use to defend against attacks, and links to free security tools. *See* CX0740 (Hill Report) at 64.

Reply to Proposed Conclusion of Law No. 17

Complaint Counsel's Proposed Conclusion of Law No. 17 is erroneous as a matter of law.

First, this is factual claim, not a legal conclusion and should be stricken accordingly.

Second, internet postings of links to SANS Institute and NIST publications, and similar materials on the Commission's official website do not replace Federal Register publication. *See*

5 U.S.C. § 552(a)(1)(D) (mandating Federal Register publication); *Util. Solid Waste*, 236 F.3d at 754. Without such publication, these documents have no legal effect.

Third, due process mandates an objective, medical industry-specific "reasonableness" standard of care and not a general "IT industry" standard. *See S&H Riggers*, 659 F.2d at 1280-81, 85; *Fla. Mach. & Foundry*, 693 F.2d at 120.

Fourth, there are contradictions between NIST and SANS, on the one hand, and HIPAA, on the other hand. CX 0405, HHS' Security Series 6, entitled "Basics of Risk Analysis and Risk Management," states:

> The Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to '[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.' [. . .] **Although only federal agencies are required to follow federal guidelines like the NIST 800 series**, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, "Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, **this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations**."

(CX 0405 (HIPAA Security Series 6, at 1-2)) (emphasis added).

Hill never accounted for this language. (Hill, Tr. 235-36). Also, HIPAA is based on scalability, which FTC failed to properly consider. 42 U.S.C. § 1320d-2(d)(1)(A)(v); 45 C.F.R. §§ 164.302, 164.308(a)(1), 164.312(a)(1); HIPAA Security Series, "7 Security Standards: Implementation for the Small Provider," vol. 2, paper 7 (Dec. 10, 2007), at 1-3 ("Factors that determine what is 'reasonable' and 'appropriate' include cost, size, technical infrastructure and resources."), 12 ("The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and

other applicable resources to review and maintain their Security Rule compliance efforts."), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015).

> 18. Companies may also review FTC complaints and consent decrees. *FTC v. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019, at *15 (D.N.J. Apr. 7, 2014) (noting that consent orders provide guidance to courts and litigants); *see also* Comm'n Order Denying Resp't's Mot. to Dismiss at 14 ("Complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings."); *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 496-97 (1st Cir. 2009) (in reviewing data security claim under state unfair practices act, noting that "a substantial body of FTC complaints and consent decrees focus on" data security and provide interpretive guidance for determining unfair conduct).

Reply to Proposed Conclusion of Law No. 18

Complaint Counsel's Proposed Conclusion of Law No. 18 is erroneous as a matter of law, legally insufficient, factually erronesous, incomplete, intentionally misleading, and confusing.

The Commission is bound by the Administrative Procedure Act ("APA"), which provides a consent decree is not binding authority or a legally-cognizable "standard" of agency expectations. *Intergraph Corp. v. Intel Corp*., 253 F.3d 695, 698 (Fed. Cir. 2001) (consent orders do "not establish illegal conduct"); *Altria Grp.*, 555 U.S. at 89 n.13; Jan M. Rybnicek & Joshua D. 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, 1305-06 (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."). As the Third Circuit said:

> 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. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC's only answer was that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." We also asked whether the FTC has "informed the public that it needs to look at complaints and consent decrees for guidance," and the Commission could offer no examples.

Wyndham, 2015 U.S. App. LEXIS 14839 at *50-51 n.23 (citations omitted).

19. The FTC's consent decrees illustrate commonly-known data security issues, highlight security vulnerabilities similar to those found with respect to LabMD, and provide notice about some of the types of data security practices the FTC has identified as unreasonable. They concern fundamental security elements, including: conducting risk assessments to identify reasonably foreseeable risks; assessing the effectiveness of existing security measures and adopting additional measures in light thereof; testing and monitoring security measures for effectiveness; and adjusting the measures appropriately. For example, the complaints in a number of FTC actions allege that the respondent failed to conduct adequate risk assessments and, as a result, failed to adopt easily implemented measures to address reasonably foreseeable risks that an appropriate risk assessment would have revealed. *See, e.g.*, *BJ's Wholesale Club, Inc.*, FTC File No. 042-3160, Docket No. C-4148 (2005) (alleging unfair failure to employ reasonable security measures, including failing to conduct security investigations); *DSW, Inc.*, FTC File No. 052-3096, Docket No. C-4157 (2006) (alleging unfair failure to employ reasonable security measures, including failing to employ sufficient measures to detect unauthorized access); *Nations Title Agency, Inc.*, FTC File No. 052-3117, Docket No. C-4161 (2006) (alleging unfair failure to employ reasonable security measures, including failure to assess risks to consumer information it collected and stored and failure to implement policies and procedures in key areas); *CardSystems Solutions, Inc.*, FTC File No. 052-3148, Docket No. C-4168 (2006) (alleging unfair failure to employ reasonable security measures, including failing to adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks); *Reed Elsevier, Inc.*, FTC File No. 052-3094, Docket No. C-4226 (2008) (alleging unfair failure to employ reasonable security measures, including allegations related to insecure user credentials to access Personal Information of consumers); *TJX Cos., Inc.*, FTC File No. 072-3055, Docket No. C-4227 (2008) (alleging unfair failure to employ reasonable security measures, including allegations relating to insecure user credentials and failure to employ sufficient measures to detect and prevent unauthorized access to computer networks); *CVS Caremark Corp.*, FTC File No. 072-3119, Docket No. C-4259 (2009) (alleging unfair failure to employ reasonable security measures, including failure to train employees to treat information securely and failure to implement a reasonable process for discovering and remedying risks to Personal Information); *Dave & Buster's, Inc.*, FTC File No. 082-3153, Docket No. C-

4291 (2010) (alleging unfair failure to employ reasonable security measures, including failure to detect and prevent unauthorized access to computer networks or conduct security investigations); *Rite Aid Corp.*, FTC File No. 072-3121, Docket No. C-4308 (2010) (alleging unfair failure to employ reasonable security measures, including failure to properly train employees); *Fajilan & Assocs.*, FTC File No. 092-3089, Docket No. C-4332 (2011) (alleging unfair failure to employ reasonable security measures, including failure to develop and disseminate information security policies, perform risk assessments, address risks identified in risk assessments, and monitor compliance); *ACRAnet, Inc.*, FTC File No. 092-3088, Docket No. C-4331 (2011) (alleging unfair failure to employ reasonable security measures, including failure to develop and disseminate information security policies, perform risk assessments, address risks identified in risk assessments, and monitor compliance); *SettlementOne Credit Corp.*, FTC File No. 082-3208, Docket No. C-440 (2011) (alleging unfair failure to employ reasonable security measures, including failure to develop and disseminate information security policies, perform risk assessments, address risks identified in risk assessments, and monitor compliance); *Ceridian Corp.*, FTC File No. 102-3160, Docket No. C-4325 (2011) (alleging unfair failure to adequately assess the vulnerability of its network to commonly known or reasonably foreseeable attacks and failure to employ reasonable measures to detect or prevent unauthorized access to Personal Information); *Lookout Servs., Inc.*, FTC File No. 102-3076, Docket No. C-4326 (2011) (alleging unfair failure to implement reasonable policies and procedures for the security of sensitive consumer information and allegations relating to insecure user credentials); *Upromise, Inc.*, FTC File No. 102-3116, Docket No. C-4351 (2012) (alleging unfair failure to assess and address risks to consumer information); *EPN, Inc.*, FTC File No. 112-3143, Docket No. C-4370 (2012) (alleging unfair failure to adopt an appropriate information security program; assess risks to Personal Information; adequately train employees; and use reasonable methods to prevent, detect, and investigate unauthorized access to Personal Information); *Franklin's Budget Car Sales, Inc.*, FTC File No. 102-3094, Docket No. C-4371 (2012) (alleging unfair failure to adopt an appropriate information security program; assess risks to Personal Information; adequately train employees; and use reasonable methods to prevent, detect, and investigate unauthorized access to Personal Information); *Compete, Inc.*, FTC File No. 102-3155, Docket No. C-4384 (2012) (alleging unfair failure to design and implement reasonable information safeguards and use readily-available, low-cost measures to assess and address risks); *HTC Am., Inc.*, FTC File No. 122-3049, Docket No. C-4406 (2013) (alleging unfair failure to implement adequate security and privacy guidance and training for its staff; conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities; and follow well-known and commonly-accepted security practices in its industry).

Reply to Proposed Conclusion of Law No. 19

Complaint Counsel's Proposed Conclusion of Law No. 19 is a statement of fact not a conclusion of law and should be stricken accordingly.

Also, listing FTC complaints against companies that are not HIPPA "covered entities" is no substitute for the legal requirements of fair notice and public objective standards or regulations governing data security for covered entities like LabMD under HIPAA. *See* 5 U.S.C. § 552(a)(1)(D) (mandating Federal Register publication); *Util. Solid Waste*, 236 F.3d at 754; *Wyndham,* 2015 U.S. App. LEXIS 14839 at *50-51 n.23 (citations omitted). Fair notice also requires an objective, medical industry-specific "reasonableness" standard of care. *See S&H Riggers*, 659 F.2d at 1280-81, 85; *Fla. Mach. & Foundry*, 693 F.2d at 120.

As a matter of law, FTC should have published in the Federal Register applicable guides or policy statements prior to commencing this case, as it has often done. *See* 16 C.F.R. § 14.9 (titled "Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials," establishing same and warning "[a]ny respondent who fails to comply with [the specified] requirement may be the subject of a civil penalty or other law enforcement proceeding for violating the terms of a Commission cease-and-desist order or rule"); 16 C.F.R. § 453.1 (funeral rule definitions); 15 U.S.C. 57a (stating Commission authority).

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.*, 673 F.2d at 1010-11. Adjudication deals with what the law was; rulemaking deals with what the law will be. *Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 221 (1988). The function of filling in the interstices of the FTC Act should be performed, as

much as possible, "*through this quasi-legislative promulgation of rules to be applied in the future*." *See id.* Therefore, the Commission's adjudication here is arbitrary and capricious. *Ford Motor Co.*, 673 F.2d at 1010-11 (citation omitted).

20. The consent decrees approved by the Commission in data security matters all provide the same basic guidance by imposing relief that requires respondents to implement a comprehensive information security plan that includes the same fundamental security elements as required by the notice order. The consent decrees require a respondent to establish a comprehensive information security program with elements that (1) designate an employee or employees to coordinate and be accountable for the information security program; (2) identify 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; (3) design and implement 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; (4) develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and require service providers by contract to implement and maintain appropriate safeguards; and (5) evaluate and adjust the information security program in light of the testing and monitoring required by subpart (3), any material changes to respondents' operations or business arrangements, and any other circumstances that respondent knows or has reason to know may have a material impact on effectiveness of its information security program. The orders provide further guidance on subpart (2), risk identification, requiring respondents to assess 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 system failures. *See generally* cases cited in Conclusion of Law ¶ 19, *supra.*

Reply to Proposed Conclusion of Law No. 20

Complaint Counsel's Proposed Conclusion of Law No. 20 is a factual summary not a conclusion of law, and should be stricken accordingly.

A consent decree is not binding authority or a legally-cognizable "standard" of agency expectations. *Intergraph Corp.*, 253 F.3d at 698 (consent orders do "not establish illegal conduct"); *Altria Grp.*, 555 U.S. at 89 n.13; Jan M. Rybnicek & Joshua D. 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, 1305-06 (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."); *Wyndham*, 2015 U.S. App. LEXIS 14839 at *50-51 n.23 (citations omitted); *cf.* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8338-49, 8351, 8359-64, 8367-69, 8372-73 (Feb. 20, 2003); *see also* 45 C.F.R. pts. 160, 162, 164.

21. Complaint Counsel has demonstrated by a preponderance of the evidence that: (1) LabMD's data security failures caused or are likely to cause substantial injury to consumers, (2) consumers cannot reasonably avoid the substantial injury caused or likely to be caused by LabMD's data security failures, and (3) LabMD's data security failures are not outweighed by countervailing benefits to consumers or to competition. LabMD, therefore, has violated Section 5 of the FTC Act. *See* 15 U.S.C. § 45(n).

Reply to Proposed Conclusion of Law No. 21

Complaint Counsel's Proposed Conclusion of Law No. 21 is erroneous.

First, Complaint Counsel has failed to demonstrate that LabMD's data security practices are "unfair" under Section 5(a). *See* Reply to Proposed Conclusion of Law No. 3. Without this demonstration, LabMD cannot have "violated Section 5 of the FTC Act."

Second, "LabMD's data security failures" must cause (now) or be likely to cause (in the future) substantial injury. Section 5 does not use the word "caused."

Third, Section 5(n) states that "the Commission shall have no authority under this section or section 57a of this title 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." 15 U.S.C. § 45(n).

Complaint Counsel has not proven by a preponderance of the evidence that LabMD's data security was "unfair" as defined at Section 5(a) between January, 2005, and the present. It has not proven that LabMD's data security, if "unfair," was also "unlawful" under the Section 5(n) test. *See* 15 U.S.C. § 45(n); 1 U.S.C. § 1 ; *Carr*, 560 U.S. at 448; *Meyer*, 510 U.S. at 477; *Gwaltney*, 484 U.S. at 59

22. The order against LabMD proposed by Complaint Counsel is appropriate as a result of the company's violations of Section 5.

Reply to Proposed Conclusion of Law No. 22

Complaint Counsel's Proposed Conclusion of Law No. 22 is an unsupported factual statement not a conclusion of law and should be stricken accordingly.

Also, this Proposed Conclusion of Law is erroneous. To begin with, Complaint Counsel has not proven by a preponderance of the evidence that LabMD violated Section 5. It has not established that the challenged data security practices were "unfair" under Section 5(a) nor has it proven all of the elements in Section 5(n) as required to declare unfair practices unlawful and trigger relief. Furthermore, the order against LabMD proposed by Complaint Counsel is facially unlawful.

First, Article I of the Constitution establishes that all authority in FTC or other agencies is inherent to statutory grants. Nothing in Section 5 authorizes FTC to "deputize" private third parties as Complaint Counsel proposes, and the Proposed Order 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 the Proposed Order fails. *Dep't of Transp. v. Ass'n of Am. R.R.s*, 135 S. Ct. 1225, 1236 (2015) (Alito, J.

concurring); *see also 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 Notice Order also raises Appointments Clause, separation of powers, and due process concerns. *Ass'n of Am. R.R.s*, 135 S. Ct. 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 does not. "Indeed, it raises '[d]ifficult and fundamental questions' about 'the delegation of Executive power' when Congress authorizes citizen suits." *Id.* at 1237 (Alito, J., concurring) (citations omitted). 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 1238 (Alito, J. concurring) (citations omitted). *See Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936).

That 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 § 57a authority, not regulate through adjudication. *Cf.* 40 C.F.R. §§ 312.10, 312.11 (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.*, 673 F.2d at 1010-11.

Third, Complaint Counsel's proposal contains a prohibited "obey-the-law" provision, provided, of course, FTC gave LabMD lawful notice during the relevant time (2005-2010), as Complaint Counsel has argued. *SEC v. Goble*, 682 F.3d 934, 949 (11th Cir. 2012). If FTC did not give LabMD lawful notice, then, by definition, LabMD was denied due process. *Fabi Constr. Co.*, 508 F.3d at 1088.

Fourth, the Proposed Order contains fencing-in relief. However, Complaint Counsel has failed to carry its burden and prove such relief is proper. *Borg-Warner Corp. v. FTC*, 746 F.2d 108, 110-11 (2d Cir. 1984); *Litton Indus., Inc. v. FTC*, 676 F.2d 364, 370 (9th Cir. 1982). Even if such relief is proper, Complaint Counsel has failed to prove that the requested relief bears a reasonable relationship to the allegedly unlawful practices. Such relief "must be sufficiently clear that it is comprehensible to the violator, and must be 'reasonably related' to a violation of the [FTC] Act." *See In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 157, at *280-81 (F.T.C. Aug. 5, 2009) (citations omitted). 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 transferabilty of the unlawful practices to other products. *In re Thompson Med. Co., Inc.*, 104 F.T.C. 648, 833 (1984). It must be "reasonably calculated to prevent future violations of the sort found to have been committed." *See ITT Cont'l Baking Co. v. FTC*, 532 F.2d 207, 221-22 (2d Cir. 1976). Complaint Counsel has not proven any present Section 5 violations, much less that they were deliberate. There is no history of past

violations. And there is no evidence of transferability, particularly in light of technological changes.

Fifth, Complaint Counsel's proposed order is not equitable but punitive in nature, *see* CCPCL ¶ 76, and the Commission is not authorized to issue same. *Heater v. FTC*, 503 F.2d 321, 322-327 (9th Cir. 1974) (overturning an FTC order for restitution as inconsistent with the purpose of the FTC Act, which does not authorize punitive or retroactive punishment).

23. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 23

LabMD has no specific response to Proposed Conclusion of Law No. 23.

1.3.1 LabMD's Data Security Failures Caused or are Likely to Cause Substantial Injury to Consumers

1.3.1.1 Caused or Likely to Cause

24. A showing of substantial injury or the likelihood of substantial injury from the unauthorized disclosure of Personal Information does not require that an actual breach occur. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 19 ("[O]ccurences of actual data security breaches or 'actual, completed economic harms' are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted 'unfair…acts or practices.'") (citations omitted); *cf. FTC v. Toysmart.com LLC*, No. 00-11341 (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/sites/default/files/documents/cases/toysmartconsent.htm (consent order) (declining to wait for bankrupt company that intended to sell consumers' Personal Information in violation of its privacy policy representations to complete the planned sale before providing relief).

Reply to Proposed Conclusion of Law No. 24

Complaint Counsel's Proposed Conclusion of Law No. 24 is erroneous.

A showing of substantial injury requires proof by a preponderance of the evidence of actual or certainly impending harm. *Clapper*, 133 S. Ct. at 1147-48. Established judicial principles suggest "substantial injury" under Section 5(n) in data breach cases requires an actual data breach and harmed, or certainly impendingly harmed, consumers, not mere conjecture,

hypothesis, or speculation. *Wyndham*, 2015 U.S. App. LEXIS 14839; *Remijas v. Neiman Marcus Grp., LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487, at *11-12 (7th Cir. Jan. 23, 2015); *In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *accord Int'l Harvester Co.*, 104 F.T.C. at 1061, 1073 (injury must be substantial, not speculative). An increased risk of harm is plainly different from certainly impending harm, and certainly impending harm is what the law demands. *See Clapper*, 133 S. Ct. at 1148; *Reilly*, 664 F.3d at 44. *FTC v. Toysmart.com LLC* is a legally irrelevant consent order. *Altria Grp.*, 555 U.S. at 89 n.13.

25. Section 5 recognizes that Complaint Counsel does not need to wait for harm to manifest before challenging conduct that is likely to cause consumer injury. The inquiry turns on whether any potential or actual unauthorized disclosure of Personal Information held by a company due to unreasonable data security practices caused or is likely to cause consumer harm. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 18-19 (requiring assessment of whether a company's "data security procedures were 'unreasonable' in light of the circumstances"); *see also, e.g.*, Statement of Basis and Purpose, Debt Settlement Amendments to Telemarketing Sales Rule, 75 Fed. Reg. 48458, 48482, n. 334 (Aug. 10, 2010) (stating that while in rulemaking proceeding there was evidence that the collection of advance fees causes actual harm, the Section 5 unfairness standard does not require the Commission to "demonstrate *actual* consumer injury, but only the *likelihood* of substantial injury") (emphasis original)); *cf. Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487 at *11-12 (7th Cir. July 20, 2015) (finding injury sufficient to satisfy Article III standing requirements because "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" (quoting *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1147 (2013)).

Reply to Proposed Conclusion of Law No. 25

Complaint Counsel's Proposed Conclusion of Law No. 25 is erroneous.

First, the "inquiry" does not turn on "whether any potential or actual unauthorized disclosure of Personal Information held by a company due to unreasonable data security practices caused or is likely to cause consumer harm." Section 5 first requires proof of "unfairness" under Section 5(a), and then requires FTC to prove a challenged act or practice

"causes or is likely to cause" substantial injury, and then to prove by a least a preponderance of the evidence, the other Section 5(n) prongs, before it may declare an unfair practice unlawful. LabMD also repeats and incorporates by reference its reply to Complaint Counsel's Proposed Conclusion of Law No. 3.

Second, *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, demonstrates that Complaint Counsel has failed to prove substantial injury, not that it has established it. 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 certainly impending. Plaintiffs "cannot manufacture standing by incurring costs in anticipation of non-certainly impending 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 injury to a large number of consumers is certainly impending. Especially given the passage of time since the "security incidents" pled in the Complaint occurred, this case is in all fours with *Clapper*. Complaint Counsel unlawfully employs Section 5 on the pretext of an entirely speculative harm based on something that did not, and, based on the evidence, cannot happen.

Third, it is not clear what Complaint Counsel means by saying it "need not wait for harm to manifest." The Supreme Court requires actual or certainly impending harm for Article III standing, *see Clapper*, 133 S. Ct. at 1148, and FTC cannot plausibly claim that it can do with less to establish "substantial injury" and then declare unlawful acts and practices that victimized no one, and years after the fact. Section 5(n) was designed to limit FTC's unfairness authority, but FTC apparently recognizes no limits at all.

Instead, the law is that Complaint Counsel must prove actual data breaches *and* actual or certainly impending substantial injury *and* LabMD's data security practices were contrary to those of medical companies during the relevant time frame. *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12 (actual data breach and injury); *Wyndham*, 2015 U.S. App. LEXIS 14839 at *21-22 (actual data breach and injury); *S&H Riggers*, 659 F.2d at 1283 (mandating that reasonableness be tested according to prevailing industry standards).

Fourth, Complaint Counsel is bound by FTC's Policy Statement on Unfairness, to the extent it adds to Section 5(n) (though it may not be used to diminish the Commission's heavy burden of proof). This provides: "In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or

defenses arising from the transaction." *Int'l Harvester Co.*, 104 F.T.C. at 1073. Unwarranted health and safety risks may also support a finding of unfairness. However, these "risks" must be proven "likely" to cause monetary harm in each case. *Id.* Only an actual data breach and actual or certainly impending consumer economic loss or injury meet FTC's own criteria for substantial harm. *Accord* 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.")

Complaint Counsel has completely failed to prove by a preponderance of the evidence a consumer injury that is substantial, tangible and more than merely speculative. *See* (LabMD's Opening Statement, Tr. 51 (MR. SHERMAN: "[T]his case is more about what could have happened, it's more about what might happen, what might have happened, but it's certainly not about what happened. And the evidence will show that the government is unable to establish the link between what they allege are LabMD's data security practices and any harm to any consumer." JUDGE CHAPPELL: "What about the likelihood of harm?" MR. SHERMAN: "I submit to the court that the evidence will be deficient in connecting LabMD's alleged data security practices and the likelihood of harm. And I submit to the court that that is precisely

what they will be unable to prove.")). LabMD's Counsel was decidedly prescient in these remarks: Complaint Counsel long ago began trying to cover up what did happen in this case in favor of rank speculation and theories of harm utterly disconnected from the facts.

Where, as here, there has been no breach and no misuse of data, and where there is no evidence of actual or certainly impending substantial injury, Complaint Counsel has failed the Section 5(n) test. *Clapper*, 133 S. Ct. at 1148; *Reilly*, 664 F.3d at 44; *Wyndham*, 2015 U.S. App. LEXIS 14839 at *45-48; *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-17.

26. Likelihood of harm satisfies the unfairness analysis. *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *89 n.52 (1984) (rejecting dissent's assertion that the Commission was requiring actual harm rather than likelihood of harm, stating "[t]he ultimate question at issue is, indeed, risk. What is the risk of consumer harm?"); *see also id.* at n.45 (noting that while not usual, the reference to "risk" in the Unfairness Statement's discussion of an unfairness case involving health and safety risks "makes clear [that] unfairness cases may also be brought on the basis of likely rather than actual injury").

Reply to Proposed Conclusion of Law No. 26

Complaint Counsel's Proposed Conclusion of Law No. 26 is erroneous and misleading.

First, "likelihood of harm" does not satisfy the "unfairness" analysis under Section 5(a) because these factors are distinct.

Second, under Section 5(n), proof that a challenged "unfair" act or practice either causes or is likely to cause substantial injury is a necessary, but not sufficient, condition to declare a practice unlawful. The avoidance and countervailing benefit prongs must be addressed.

LabMD's Reply to Complaint Counsel's Proposed Conclusion of Law No. 3 is repeated and incorporated by reference.

27. Failure to maintain adequate data security for Personal Information is likely to cause consumers substantial harm. Kam, Tr. 463-64 (opining that LabMD's failure to provide reasonable security increased the risk of unauthorized disclosure of the information it maintains.); CX0742 (Kam Report) at 23 (LabMD's failure to provide reasonable security for sensitive information it maintains created "an elevated risk of unauthorized disclosure of this

information."); CX0741 (Van Dyke Report) at 3, 6 (reaching opinion that LabMD's unreasonable security placed consumers at significantly higher risk of becoming victims of identity theft); Van Dyke, Tr. 589 (stating that there is a correlation between exposure of consumer information and identity theft); CX0741 (Van Dyke) at 8 (demonstrating correlation between data breaches and identity theft).

Reply to Proposed Conclusion of Law No. 27

Complaint Counsel's Proposed Conclusion of Law No. 27 is a statement of fact and should be stricken accordingly. It is also erroneous, incomplete, and misleading.

As a matter of law, Kam's testimony is not reliable because his methods have neither been verified by testing nor peer reviewed nor evaluated for potential rate of error. *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 157 (1999); *EEOC v. Freeman*, 778 F.3d 463, 469 (2015) (citing cases); *Allen v. LTV Steel Co.*, 68 Fed. Appx. 718, 721-22 (7th Cir. 2003).

Nor is Kam qualified to give the expert opinion he provided. *Elcock v. Kmart Corp.*, 233 F.3d 734 (3rd Cir. 2000) (trial court erred in not holding a Daubert hearing, where damages expert relied on dubious methodology, and expert's qualifications were minimal; where qualifications are a "close call," this factor weighs in favor of excluding the testimony as unreliable).

Kam's opinion is undermined by his financial entanglements, *see Lust by & Through Lust v. Merrell Dow*, 89 F.3d 594, 597-98 (9th Cir. 1996), and his analysis does not "fit" the facts of the case as a matter of law because an expert witness's opinion that one thing caused another must identify and rule out other likely causes. *People Who Care v. Rockford Bd. of Educ.*, 111 F.3d 528, 537-38 (7th Cir. 1997); *Sorensen by & Through Dunbar v. Shaklee Corp*, 31 F.3d 638, 649 (8th Cir. 1994).

Kam's use of a survey is unreliable as a matter of law because it contains systematic errors such as nonresponse or sampling bias. *See Freeman*, 778 F.3d at 466, 469; *In re*

Countrywide Fin. Corp. Mortgage-Backed Secs. Litig. v. Countrywide Fin. Corp., 984 F. Supp. 2d 1021, 1038 (C.D. Cal. 2013). When an expert relies on uncorroborated assumptions for a factual premise, the opinion is unreliable as a matter of law. *Casey v. Geek Squad*, 823 F. Supp. 2d 334, 340-41 (D. Md. 2011); *cf. Nunez v. BNSF Ry. Co.*, 730 F.3d 681, 684 (7th Cir. 2013); *Guillory v. Domtar Indus*., 95 F.3d 1320, 1330-31 (5th Cir. 1996) ("Expert evidence based on a fictitious set of facts is just as unreliable as evidence based upon no research at all. Both analyses result in pure speculation.").

Kam uncritically relied on Boback and Tiversa, so his opinion is unreliable. (CX 0742 (Kam, Rep. at 19)); (Kam, Tr. 531-32, 542-46); *Guillory*, 95 F.3d at 1330-31. He testified:

> 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).

Because Kam's entire analysis of the likelihood of harm from the Day Sheets was premised on the CLEAR database, which was excluded from this case, his opinion lacks a reliable factual basis as a matter of law and must be excluded. *Geek Squad*, 823 F. Supp. 2d at 340-44. Kam's opinion falsely assumed that the suspects in whose Sacramento house LabMD's Day Sheets were found had "identity theft charges and convictions prior to the events in Sacramento on October 5, 2012," when in fact they did not. Therefore, Kam's opinion regarding consumer harm from the Day Sheets also is unreliable and irrelevant as a matter of law. *See Korte v. ExxonMobil Coal USA, Inc.*, 164 Fed. Appx. 553, 557 (7th Cir. 2006).

Regarding Van Dyke, he too relied on Boback and Tiversa in finding substantial injury. (CX 0741(Van Dyke, Rep. at 8)); (Van Dyke, Tr. 645-46).

Also, his statistical analysis fails *Daubert* as a matter of law. First, the Javelin survey was conducted via the internet without any reliable means of confirming that identities of those who receive the survey match those of the subjects the survey intends to target, giving rise to the likelihood of serious sampling error. Second, he projected an anticipated fraud impact to consumers caused by unauthorized disclosure of the 1718 File and the Day Sheets of between 7.1% and 13.1%. However, Van Dyke's claims were belied by empirical data: the actual fraud impact to consumers in this case proven by Complaint Counsel is 0% – there was no proof of a single consumer victim. This suggests the Javelin survey is methodologically flawed and that its results are inherently unreliable. *Freeman*, 778 F.3d at 466, 469 (citations omitted).

Speculation about possible identity theft, absent any evidence of actual or certainly impending substantial injury, does not satisfy Section 5(n). *Clapper*, 133 S. Ct. at 1148; *Reilly*, 664 F.3d at 44; *Wyndham*, 2015 U.S. App. LEXIS 14839 at *45-48; *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-17. But this is all Complaint Counsel has to offer.

28. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 28

LabMD has no specific response to Proposed Conclusion of Law No. 28.

1.3.1.2 Substantial Injury

29. 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." *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *101 n.12 (1984) (Unfairness Statement).

Reply to Proposed Conclusion of Law No. 29

Complaint Counsel's Proposed Conclusion of Law No. 29 is erroneous.

A practice is "unfair" if it is marked by injustice, partiality, or deception. *See* 15 U.S.C.§ 45(a); *Yates*, 135 S. Ct. at 1081-83, 1091; *Carr*, 560 U.S. at 448; *Meyer*, 510 U.S. at 477; *Wyndham*, 2015 U.S. App. LEXIS 14839 at *15-17, *54-55; Merriam-Webster's Dictionary, "Unfair" http://www.merriam-webster.com/dictionary/unfair (last visited Aug. 9, 2015).

30. In potentially exposing the Personal Information of 750,000 consumers to unauthorized disclosure, LabMD's data security failures are likely to cause injury to a large number of consumers.

Reply to Proposed Conclusion of Law No. 30

Complaint Counsel's Proposed Conclusion of Law No. 30 is a statement of fact and should be stricken accordingly.

Proposed Conclusion of Law No. 30 is misleading and irrelevant.

Complaint Counsel argues that "[i]n potentially exposing" LabMD's patients to "unauthorized disclosure" is apparently now "likely to cause injury to a large number of consumers" in 2015 and beyond. First, there is no evidence that supports this remarkable claim – none of Complaint Counsel's experts testified to this, and to the extent they opined regarding the future likelihood of injury at all, it was based on the perjury and fabricated evidence of

Boback and Tiversa. *See* (CX 0742 (Kam, Rep. at 19)); (Kam, Tr. 531-32, 542-46); (CX 0741(Van Dyke, Rep. at 8)); (Van Dyke, Tr. 645-46). Kam's testimony is instructive:

> 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).

Second, any injury must be "substantial" to have legal consequences under Section 5(n).

Third, this speculation does not meet Section 5(n) requirements. *See Clapper*, 133 S. Ct. at 1148; *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12 (actual data breach and injury); *Wyndham*, 2015 U.S. App. LEXIS 14839 at *21-22 (actual data breach and injury); *Reilly*, 664 F.3d at 44; *Int'l Harvester Co*., 104 F.T.C. at 1073 ("The Commission is not concerned with trivial or merely speculative harms"); *see also* 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."). In data breach cases where no breach and misuse, or certainly impending breach and misuse, is proven there has been no injury as a matter of law. *Clapper*, 133 S. Ct. at 1148; *Reilly*, 664 F.3d at 44; *Wyndham*, 2015 U.S. App. LEXIS 14839 at *45-48; *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-17. As a matter of law, only an actual data breach meets FTC's own criteria for substantial harm.

31. Commission action is appropriate where, inter alia, "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." *FTC v. Klesner*, 280 U.S. 19, 28 (1929).

Reply to Proposed Conclusion of Law No. 31

Complaint Counsel's Proposed Conclusion of Law No. 31 is erroneous.

First, Commission "action" is "appropriate" only within the parameters of Section 5.

Second, whether the harm is large or small, for FTC to exercise its Section 5 unfairness authority lawfully (as limited by Section 5(n)) against a given act or practice, it must prove that the targeted act or practice has a generalized, adverse impact on competition or consumers and connect to the "protection of free and fair competition in the Nation's markets." *Am. Bldg. Maint. Indus.*, 422 U.S. at 277; *Yates*, 135 S. Ct. at 1082-83, 1085; 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."); J. Howard Beales, Former Dir., Fed. Trade Comm'n, Speech: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, at § II (May 30, 2003) ("unfairness [has] a more prominent role as a powerful tool for the Commission to analyze and attack a wider range of practices that may not involve deception but nonetheless cause *widespread and significant consumer harm*") (emphasis added), *available at* https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection; 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.").

Third, Complaint Counsel misreads *Klesner*, and misapplies it in light of Section 5(n). Instead, *Klesner* suggests the Commission failed to properly evaluate, investigate, and protect the "public interest" when it commenced this action against LabMD without proof that the actual or certainly impending injury is "serious and widespread":

> [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.

280 U.S. at 28. 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.*, 45 F. Supp. 3d at 24 (citing cases). Furthermore, Section 5, by its plain language, does not justify aggregation of either acts and practices or of substantial injury.

32. Monetary harm exemplifies the injury prong of the unfairness standard. *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *97 (1984).

Reply to Proposed Conclusion of Law No. 32

Complaint Counsel's Proposed Conclusion of Law No. 32 is erroneous, irrelevant, and misleading.

First, monetary harm does not "[exemplify] the injury prong of the unfairness standard", rather, it is relevant to a finding of substantial injury that is a prong of the Section 5(n) unlawfulness test. It is irrelevant to Section 5(a) "unfairness."

Second, Complaint Counsel has not proven any monetary harm here, so it is irrelevant.

33. LabMD's data security failures are likely to cause consumers monetary harm from existing card fraud, existing non-card fraud, new account fraud, tax fraud, and medical identity theft. *See generally* CCFF § 9 LabMD's Data Security Practices Caused or are Likely to Cause Substantial Injury to Consumers that is Not Reasonably Avoidable by the Consumers Themselves.

Reply to Proposed Conclusion of Law No. 33

Complaint Counsel's Proposed Conclusion of Law No. 33 is a statement of fact and should be stricken accordingly.

Proposed Conclusion of Law No. 33 is also erroneous.

First, there is no testimony that LabMD's data security was inadequate after July 2010, and no evidence that pre-July 2010 data security practices are likely to cause a large number of consumers harm now or in the future. The plain language of Section 5(n) does not authorize the Commission to declare past conduct unlawful and, because Complaint Counsel failed to prove by a preponderance of the evidence that any of the challenged acts or practices occurred after July 2010, or are likely to cause substantial injury in the future, LabMD should prevail. 15 U.S.C. § 45(n); 1 U.S.C. § 1 ; *Carr*, 560 U.S. at 448; *Meyer*, 510 U.S. at 477; *Gwaltney*, 484 U.S. at 59; *United States v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953); *Borg-Warner Corp.*, 746 F.2d at 110-11; *see also WHX v. SEC*, 362 F.3d 854, 861 (D.C. Cir. 2004) ("WHX committed (at most) a single, isolated violation of the rule, it immediately withdrew the offending condition once the Commission had made its official position clear, and the Commission has offered no reason to doubt WHX's assurances that it will not violate the rule in the future. In light of these factors, none of which the Commission seems to have considered seriously, the imposition of the cease-and-desist order seems all the more gratuitous"); *see also FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 920 (1965) ("In this case the respondents produced three different commercials which employed the same deceptive practice. This we believe gave the Commission a sufficient basis for believing that the respondents would be inclined to use similar commercials with respect to the other products they advertise.").

34. The entirety of harms likely to be caused by an unfair act or practice need not be monetarily quantifiable. *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1364-65 (11th Cir. 1988) (affirming Commission grant of

summary judgment where injury included in part "intangible loss" relating to certainty of contract terms).

Reply to Proposed Conclusion of Law No. 34

Complaint Counsel's Proposed Conclusion of Law No. 34 is erroneous. *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1364-65 (11th Cir. 1988), simply does not stand for the proposition cited. The court there decided: "The harm resulting from Orkin's conduct consists of increased costs for services previously bargained for and includes the intangible loss of the certainty of the fixed price term in the contract." *Orkin*, 849 F.2d at 1364-65 (citation omitted). That is, but for the "increased costs" visited upon consumers, the "intangible loss" in *Orkin* would not have existed. Furthermore: "The Commission's finding of 'substantial' injury is supported by the undisputed fact that Orkin's breach of its pre-1975 contracts generated, during a four-year period, more than $7,000,000 in revenues from renewal fees to which the Company was not entitled." *Id.* at 1365 (emphasis added). Unlike this proceeding, where there is no actual or certainly impending injury or likelihood of injury, *Orkin* involved actual harm.

35. Defendant's acts or practices also cause substantial harm when consumers must spend "a considerable amount of time and resources" remediating problems caused by the defendant's conduct, such as closing compromised bank accounts. *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1115-16 (S.D. Cal. 2008) (basing finding of substantial harm in part on "the cost of account holders' time" where defendants' practices compromised bank account security); *see also Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487 at *9 (7th Cir. July 20, 2015) (observing in a data breach involving credit cards, "there are identifiable costs associated with the process of sorting things out"), *13-14 (lost time and money spent by consumers protecting themselves from future identity theft "easily qualifies as a concrete injury"), *21 (finding that mitigation expenses and future injury are judicially redressable); *FTC v. Kennedy*, 574 F. Supp. 2d 714, 721 (S.D. Tex. 2008) (finding substantial injury where, *inter alia*, "consumers were forced to expend substantial time and effort" seeking refunds and other remediation of the defendant's unfair conduct).

Reply to Proposed Conclusion of Law No. 35

Complaint Counsel's Proposed Conclusion of Law No. 35 is erroneous and irrelevant because it has nothing to do with this case. To begin with, *all* of the cited cases involved an actual, quantifiable loss, and not merely a speculative, hypothetical claim as Complaint Counsel has made here.

In *FTC v. Neovi, Inc.*, actual, concrete harm was the foundation for a finding of substantial harm:

> Defendants' own records show that their failure to employ and maintain adequate verification procedures, over approximately six years, led to substantial losses for consumers that had unauthorized checks drawn on their bank accounts. Consumers not only lost the use of funds withdrawn from their accounts, but they often spent a considerable amount of time and resources contesting the checks at their banks, protecting their accounts, and attempting to get their money back."

598 F. Supp. 2d at 1115-16.

The Seventh Circuit's decision in *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *8-9 (petition for *en banc* review filed on August 3, 2015), involved actual injury as well, for 9,200 consumers "incurred fraudulent charges." As to the "approximately 350,000 other customers whose data may have been hacked," the court found that future harm must be "certainly impending" to confer Article III standing. Mere allegations of possible future injury (as in this case) are not sufficient. *See Clapper*, 113 S.Ct. at 1147.

FTC v. Kennedy, 574 F. Supp. 2d 714, 721 (S.D. Tex. 2008), also involved actual harm. ("The evidence shows that numerous consumers were billed for a service that they did not want an (sic) in fact had refused. Therefore, consumers were forced to pay for a service that they never requested. Moreover, consumers were forced to expend substantial time and effort to obtain refunds and cancellation of the service. In spite of their efforts, all consumers have not received a full refund.").

36. LabMD's data security failures are likely to cause consumers substantial harm in the form of time spent remediating problems from new account fraud, existing non-card fraud, existing card fraud, and medical identity theft. *See generally supra* CCFF § 9 (LabMD's Data Security Practices Caused or are Likely to Cause Substantial Injury to Consumers that is Not Reasonably Avoidable by the Consumers Themselves and Are Not Outweighed by Countervailing Benefits to Consumers or Competition) *et seq.* (¶¶ 1472-1798)).

Reply to Proposed Conclusion of Law No. 36

Complaint Counsel's Proposed Conclusion of Law No. 36 is a statement of fact and should be stricken accordingly. It is also erroneous. No witness has testified that LabMD's post-July 2010 data security practices are likely to cause substantial injury. There is no evidence that LabMD's pre-July 2010 are likely to cause these injuries, given that Boback has been revealed a perjurer and CX0019 a fraud. In any event, there is no evidence of a single case of these injuries, much less widespread cases as the law requires, from either the Day Sheets or the 1718 File or anything else.

As a matter of law, speculation about the potential time and money consumers could spend resolving fraudulent charges cannot satisfy Section 5(n), or even confer standing under Article III. *See, e.g.*, *Reilly*, 664 F.3d at 46 (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 alleged 'increased risk of injury' claims"); *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 certainly impending" injury. *In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 28-33 (listing cases).

37. "Unwarranted health and safety risks may also support a finding of unfairness." *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *97 (1984) (Unfairness Statement). Indeed, the seminal unfairness case involved a product that caused physical injury to some consumers and was likely to harm more. *Int'l Harvester Co.*, 1984 WL 565290 at *90 & n.57.

Reply to Proposed Conclusion of Law No. 37

Complaint Counsel's Proposed Conclusion of Law No. 37 is erroneous and misleading. "Unwarranted health and safety risks" may support a finding of unfairness only if they are the result of an act or practice that is "unfair" for Section 5(a) purposes, understood to mean "marked by injustice, partiality, or deception." 15 U.S.C. § 45(a); *Yates*, 135 S. Ct. at 1081-83, 1091, and otherwise satisfy Section 5(n)'s limiting test. Emotional impact will not ordinarily make a practice unfair. *Int'l Harvester Co.*, 104 F.T.C. at 1073.

38. LabMD's data security failures are likely to cause consumers substantial harm in the form of health and safety risks caused by medical identity theft. *Supra* CCFF §§ 9.1.2.3.1 (Integrity of Consumer Health Records Compromised Due to Medical Identity Theft Causes of Risk of Physical Harm to Consumers) (¶¶ 1612-1618), 9.3.4 (Impact on Consumers From Medical Identity Theft Stemming From Unauthorized Disclosure of the 1718 File) (¶¶ 1678-1681).

Reply to Proposed Conclusion of Law No. 38

Complaint Counsel's Proposed Conclusion of Law No. 38 is a statement of fact and should be stricken accordingly. It is also erroneous. No witness has testified that LabMD's post-July 2010 data security practices are likely to cause substantial injury. There is no evidence that LabMD's pre-July 2010 practices are likely to cause these injuries, given that Boback has been revealed a perjurer and CX0019 a fraud. In any event, there is no evidence of a single case of these injuries, much less widespread cases as the law requires, from either the Day Sheets or the 1718 File or anything else.

39. Loss of privacy can result in a "host of emotional harms that are substantial and real and cannot fairly be classified as either trivial or speculative." *FTC v Accusearch, Inc.*, 2007 WL 4356786 at *8 (D. Wyo. Sept. 28, 2007).

Reply to Proposed Conclusion of Law No. 39

Complaint Counsel's Proposed Conclusion of Law No. 39 is erroneous.

Complaint Counsel wrongly relies on *FTC v Accusearch, Inc.*, No. 06-105, 2007 U.S. Dist. LEXIS 74905 (D. Wyo. Sept. 28, 2007), *aff'd FTC v. Accusearch, Inc.*, 2009 U.S. App. LEXIS 14480 (10th Cir. 2009). First, it fails to cite or distinguish a conflicting case within *Accusearch* itself. The District Court of Wyoming discussed without distinguishing the contrary holding in *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999). After noting that the Government may not satisfy its significant burden by "merely asserting a broad interest in privacy," the Court in *U.S. West* held that agencies "must specify the particular notion of privacy and interest served. Moreover, privacy is not an absolute good because it imposes real costs on society." *Id.* at 1235 (emphasis added). Further, "the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity." *Id.*

The *U.S. West* decision also supports what LabMD has been saying all along in this case: Only an actual data breach and misuse of data (or certainly impending injury from an actual data breach and misuse of data) meets FTC's own criteria for substantial harm. "A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level" of likely substantial injury because "it is not based on an identified harm." *Id.* (emphasis added).

Complaint Counsel's cited authority confirms that only an actual data breach and misuse of data, not speculative or guesswork injury, is required: "This Court is presented with evidence

of *actual consumer harm* where third parties have gone to considerable expense and effort to gain access to those records." *Accusearch,* 2007 U.S. Dist. LEXIS 74905 at *23.

40. The disclosure of sensitive medical information, resulting in the loss of consumer privacy, constitutes substantial injury. Kam, Tr. 395-96; *see also* Kam, Tr. 445-53 (exposure of 1718 File was likely to lead to reputational harm to consumers based on the release of sensitive information about medical tests performed on consumers); CX0742 (Kam Report) at 16, 21 (victims who may have cancer or sexually transmitted diseases are particularly vulnerable to reputational harm).

Reply to Proposed Conclusion of Law No. 40

Complaint Counsel's Proposed Conclusion of Law No. 40 is erroneous. It cites no authority for this proposition, other than Kam. But Kam is not reliable because his methods have neither been verified by testing nor peer reviewed nor evaluated for potential rate of error. *Kumho Tire Co.*, 526 U.S. at 157; *Freeman*, 778 F.3d at 469 (citing cases); *Allen*, 68 Fed. Appx. at 721-22. Nor is Kam qualified to give the expert opinion he provided, and his testimony should not be relied upon. *Elcock*, 233 F.3d 734 (trial court erred in not holding a Daubert hearing, where damages expert relied on dubious methodology, and expert's qualifications were minimal: where qualifications are a "close call," this factor weighs in favor of excluding the testimony as unreliable).

Kam's use of a survey is unreliable as a matter of law because it contains systematic errors such as nonresponse or sampling bias. *See Freeman*, 778 F.3d at 466, 469; *In re Countrywide*, 984 F. Supp. 2d at 1038. When an expert relies on uncorroborated assumptions for a factual premise for his opinion, the opinion is unreliable as a matter of law. *See Korte*, 164 Fed. Appx. at 557; *Geek Squad*, 823 F. Supp. 2d at 340-41; *cf. Nunez*, 730 F.3d at 684; *Guillory*, 95 F.3d at 1330-31 ("Expert evidence based on a fictitious set of facts is just as unreliable as evidence based upon no research at all. Both analyses result in pure

speculation."). Kam uncritically relied on Boback and Tiversa, so his opinion is unreliable as a matter of law. *Guillory*, 95 F.3d at 1330-31.

In addition, because Kam's entire analysis of the likelihood of harm from the Day Sheets was premised on the CLEAR database, which was excluded from this case, his opinion lacks a reliable factual basis as a matter of law and must be excluded. *Geek Squad*, 823 F. Supp. 2d at 340-44. Kam's opinion falsely assumed that the suspects in whose Sacramento house LabMD's Day Sheets were found had "identity theft charges and convictions prior to the events in Sacramento on October 5, 2012," when in fact they did not. Kam conducted essentially no analysis of the risk of harm to consumers from LabMD's general security measures. As a matter of law, an expert may not simply accept another expert's opinion: "[e]xperts may not . . . simply repeat or adopt the findings of [others] without investigating them." *See Hendrix v. Evenflo Co., Inc*., 255 F.R.D. 568, 607 (N.D. Fla. 2009), *aff'd* at 609 F. 3d 1183 (11th Cir. 2010). Therefore, Kam's opinion regarding consumer harm from the Day Sheets is unreliable and irrelevant as a matter of law. *See Korte*, 164 Fed. Appx. at 557.

Kam depended on Boback and Tiversa for his opinion regarding likelihood of substantial injury. *See* (CX 0742 (Kam, Rep. at 19)); (Kam, Tr. 531-32, 542-46). He testified:

> 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).

41. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 41

LabMD has no specific response to Proposed Conclusion of Law No. 41.

1.3.2 Consumers Cannot Reasonably Avoid the Substantial Injury Caused or Likely to Be Caused by LabMD's Data Security Failures

42. Consumers have no way to discover LabMD's unreasonable security practices, and in many cases do not know to what laboratory their specimen is sent for analysis. *Supra* CCFF § 9.5.1.1.1 (Consumers Did Not Know LabMD Would Test Their Specimen and Receive Their Personal Information) (¶¶ 1777-1782); *see FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1112 (S.D. Cal. 2008) (consumers could not reasonably avoid injury where, inter alia, they "had never requested goods or services" from defendant).

Reply to Proposed Conclusion of Law No. 42

Complaint Counsel's Proposed Conclusion of Law No. 42 is a statement of fact and should be stricken accordingly. It is also erroneous.

First, there is no evidence that patients were prevented from knowing that LabMD would be providing them with medical services. In fact, Complaint Counsel has previously argued that LabMD collected payment directly from at least some of them—if a patient was writing a check to a lab—presumably it was because the lab provided diagnostic work. LabMD

was a HIPAA "covered entity" and so its data security practices were regulated by the United States government. HIPAA data security standards are publicly available and HHS has taken no action against LabMD. Also, since 2009, LabMD has been legally obligated to notify patients if their information was subject to an unauthorized disclosure. These are robust protections for patient data.

Second, Complaint Counsel misapplies *FTC v. Neovi, Inc.*, where actual, concrete harm was the foundation upon which a finding of substantial injury was based:

> Defendants' own records show that their failure to employ and maintain adequate verification procedures, over approximately six years, led to substantial losses for consumers that had unauthorized checks drawn on their bank accounts. Consumers not only lost the use of funds withdrawn from their accounts, but they often spent a considerable amount of time and resources contesting the checks at their banks, protecting their accounts, and attempting to get their money back.

598 F. Supp. 2d at 1115-16 (emphasis added). Actual, definitive harm – which Complaint Counsel failed to prove in this case – and the absence of anything like the HIPAA data security and breach notification regime distinguish *Neovi* from this case.

43. Where consumers do not have a free and informed choice, injury is not reasonably avoidable. *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1168-69 (9th Cir. 2012) ("In determining whether consumers' injuries were reasonably avoidable, courts look to whether the consumers had a free and informed choice." (quoting *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010)). An injury is reasonably avoidable if consumers "'have reason to anticipate the impending harm and the means to avoid it, or they may seek to mitigate the damage afterward if they are aware of potential avenues toward that end.'" *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (quoting *In re Orkin Exterminating Co.*, 108 F.T.C. 341, 366 (1986)).

Reply to Proposed Conclusion of Law No. 43

Complaint Counsel's Proposed Conclusion of Law No. 43 is erroneous and misleading. It misapplies the cited authorities, which state the following rule: "An injury is reasonably avoidable if consumers 'have reason to anticipate the impending harm and the means to avoid it,' or if consumers are aware of, and are reasonably capable of pursuing, potential avenues

toward mitigating the injury after the fact." *Davis*, 691 F.3d at 1168-69 (citations omitted). As a result of the HIPPA Breach Notification Rule, 45 CFR §§ 164.400-414, patients have the means needed to mitigate. Therefore, any injury caused by a breach by LabMD is "reasonably avoidable." As the Ninth Circuit held:

> The annual fee was also avoidable after the account was opened. Pursuant to the Cardmember Agreement, which Davis admits he received after completing the application, the annual fee was completely refundable if Davis closed his account within 90 days without using the card. Davis refused to do so, citing the negative impact it would have on his credit score. The question, however, is not whether subsequent mitigation was convenient or costless, but whether it was "reasonably possible." Under these circumstances, we conclude that Davis reasonably could have avoided the annual fee, and therefore that the advertisements were not unfair under section 5.

Davis, 691 F.3d at 1169 (citation omitted).

44. Even where consumers know they are transacting with a particular company, they cannot always know the company's security practices in order to avoid injury at the hands of a company with unreasonable security practices. *Am. Fin. Svcs Ass'n v. FTC*, 767 F.2d 957, 976 (D.C. Cir. 1985) ("[C]ertain types of seller conduct or market imperfections may unjustifiably hinder consumers' free market decisions and prevent the forces of supply and demand from maximizing benefits and minimizing costs."); *see also BJ's Wholesale Club, Inc.*, FTC File No. 042-3160, Docket No. C-4148 (2005); *DSW, Inc.*, FTC File No. 052-3096, Docket No. C-4157 (2006); *TJX Cos., Inc.*, FTC File No. 072-3055, Docket No. C-4227 (2008); *CVS Caremark Corp.*, FTC File No. 072-3119, Docket No. C-4259 (2009); *Dave & Buster's, Inc.*, FTC File No. 082-3153, Docket No. C-4291 (2010); *Rite Aid Corp.*, FTC File No. 072-3121, Docket No. C-4308 (2010); *Upromise, Inc.*, FTC File No. 102-3116, Docket No. C-4351 (2012); *EPN, Inc.*, FTC File No. 112-3143, Docket No. C-4370 (2012); *Franklin's Budget Car Sales, Inc.*, FTC File No. 102-3094, Docket No. C-4371 (2012); *Compete, Inc.*, FTC File No. 102-3155, Docket No. C-4384 (2012); *HTC Am., Inc.*, FTC File No. 122-3049, Docket No. C-4406 (2013).

Reply to Proposed Conclusion of Law No. 44

Complaint Counsel's Proposed Conclusion of Law No. 44 is erroneous and irrelevant.

First, it misapplies *Am. Fin. Servs. Assoc. v. FTC*, 767 F.2d 957, 976 (D.C. Cir. 1985). That case involved a trade rule on creditor remedies. The court, after describing consumer credit practices, supported the Commission, saying "[s]uch corrective action is taken 'not to

second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.'" *Id.* Here, there is no evidence in the record of any "seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking." *Id.* No witness testified that LabMD did anything to interfere with patient choice with respect to pathology labs or anything else. Instead, the sole evidence is that LabMD was a HIPAA "covered entity," and that it complied with HIPAA data security regulations at all times. Furthermore, Complaint Counsel does not explain what it means for a patient to "know the company's security practices in order to avoid injury at the hands of a company with unreasonable security practices." Without evidence or explanation, this Proposed Conclusion of Law must fail.

Second, Complaint Counsel here cites a multitude of consent orders with companies, not one of which is a HIPAA covered entity, as if they are precedential in this case. They are not. *Intergraph Corp.*, 253 F.3d at 698 (consent orders do "not establish illegal conduct"); *Altria Grp.*, 555 U.S. at 89 n.13; Jan M. Rybnicek & Joshua D. 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, 1305-06 (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.").

45. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 45

LabMD has no specific response to Proposed Conclusion of Law No. 45.

1.3.2 LabMD's Data Security Failures are Not Outweighed by Countervailing Benefits to Consumers or to Competition

46. "'[W]hen a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition,'" the countervailing benefits prong of the unfairness test is "easily satisfied." *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (quoting *FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal 2000)).

Reply to Proposed Conclusion of Law No. 46

Complaint Counsel's Proposed Conclusion of Law No. 46 is erroneous and misleading.

First, the "countervailing benefits prong" is not part of "the unfairness test," instead it is part of the unlawfulness test in Section 5(n). LabMD's approach offered groundbreaking benefits to doctors and patients, delivering pathology results to doctors with unprecedented access to diagnostic results allowing them to more quickly tell anxiously waiting patients whether they had cancer and to begin treatment immediately, if needed. (Daugherty, Tr. 942, 944-46, 950-51, 959-62, 970, 982, 1036, 1063-65). However, FTC has failed in this case to provide for the record (and for LabMD's rebuttal) a reasoned countervailing benefit analysis as required by law. *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009) [hereinafter "*Fox Television II*"] (noting "the requirement that an agency provide reasoned explanation for its action").

Second, Complaint Counsel agains misapplies its cited authorities. In *FTC v. Neovi, Inc.*, 598 F. Supp. 2d at 1115-16, there was actual, concrete harm and this was the basis for finding substantial injury. Again, in *FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal 2000), there was actual, concrete injury, including fraud and monetary loss.

47. Where consumers do not knowingly purchase a product or service, there are unlikely to be countervailing benefits to a company's unfair practices. *FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012) (finding no countervailing benefits where consumers "did not give their consent to enrollment in OnlineSupplier, and thus, the harm resulted from a practice for which they did not bargain"). Consumers whose laboratory work was sent to LabMD often did not have a choice in which lab was used. *Supra* § 9.5.1.1.1

(Consumers Did Not Know LabMD Would Test Their Specimen and Receive Their Personal Information) (¶¶ 1777-1782).

Reply to Proposed Conclusion of Law No. 47

Complaint Counsel's Proposed Conclusion of Law No. 47 is erroneous and misleading.

First, there is no evidence that any doctor prohibited any LabMD patient from choosing a lab for diagnostic work.

Second, there is no evidence that LabMD's patients did not knowingly "purchase" diagnostic services. It is bizarre for Complaint Counsel to contend that a patient consulting with a doctor about prostrate cancer and needing a diagnosis is not "knowingly" "purchasing" that "service."

Third, Complaint Counsel again misapplies its cited authority. *Commerce Planet* (like every other case Complaint Counsel has cited) is wholly unavailing because the deceptive practices in that case involved actual consumer injury:

> Defendants deceptively marketed OnlineSupplier as a free auction kit on its website without adequately disclosing the program's negative option plan, which required consumers to affirmatively cancel their membership or otherwise incur a monthly charge to their credit card. The FTC allege[d] that consumers unwittingly signed up for OnlineSupplier, believing they had ordered a free kit, only to discover later that they had been enrolled in OnlineSupplier's continuity program when they saw monthly charges on their credit card bill. The FTC allege[d] that between July 2005 and March 2008, Commerce Planet obtained over $45 million from over 500,000 consumers.

FTC v. Commerce Planet, Inc., 878 F. Supp. 2d 1048, 1054 (C.D. Cal. 2012).

There is no need to reach a "countervailing benefits" analysis when then has been no actual or certainly impending substantial injury. But even if there was such an injury, Complaint Counsel's failure to submit evidence on this prong is fatal to its case. 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.*, 104 F.T.C. at 1073-74.

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.*, 104 F.T.C. at 1070. 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.*; *see also* CCPCL ¶ 14.

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. *Neovi, Inc.*, 598 F. Supp. 2d at 1115 (FTC offered expert testimony that the defendants' business model did not provide any advantage and that any benefits were small, that it did not have a positive impact in the marketplace and did not benefit competition).

48. Countervailing benefits are determined based on the specific practice at issue in a complaint, not the overall operation of a business. *FTC v. Accusearch, Inc*., 2007 WL 4356786 at *8 (D. Wyo. Sept. 28, 2007), judgment aff'd *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009) ("While there may be countervailing benefits to some of the information and services provided by 'data brokers' such as *Abika.com*, there are no countervailing benefits to consumers or competition derived from the specific practice of illicitly obtaining and selling confidential consumer phone records." (emphasis original)); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (upholding Commission finding of no countervailing benefits because an increase in fees "was not accompanied" by an increased level or quality of service); *Apple, Inc.*, No. 122-3108, Statement of Comm'r Maureen K. Ohlhausen at 2 (Jan. 15, 2014) (reiterating that countervailing benefit determination is made by "compar[ing] that harm to any benefits from that particular practice").

Reply to Proposed Conclusion of Law No. 48

Complaint Counsel's Proposed Conclusion of Law No. 48 is erroneous.

First, Complaint Counsel's authorities do not hold or discuss the proposition cited. Notably, *Accusearch* and *Orkin* both involved significant actual injury to consumers in the first instance. FTC's bill of particulars against LabMD does not contain a single instance of actual or certainly impending substantial injury to a single consumer.

Second, Commissioner Ohlhausen points out, "[t]he relevant statutory provision focuses on the substantial injury caused by an individual act or practice, which we must then weigh against countervailing benefits to consumers or competition from that act or practice." *Apple, Inc.*, No. 122-3108, Statement of Comm'r Maureen K. Ohlhausen at 3 (Jan. 15, 2014). As applied here, this principle confirms LabMD's contention that FTC wrongfully aggregated LabMD's supposedly insufficient data security practices. *See* Compl. ¶ 10 ("respondent engaged in a number of practices that taken together, failed to provide reasonable and appropriate security").

Third, even if Complaint Counsel has stated the law correctly, there is no evidence that FTC considered how each alleged deficiency might affect LabMD's operations. LabMD's

business model offered groundbreaking benefits to doctors and patients, delivering pathology results to doctors at unprecedented speed and providing 24/7 access, allowing them to more quickly tell anxiously waiting patients whether they had cancer and to begin treatment immediately, if needed. The company's IT architecture was specifically designed to accomplish these goals. (Daugherty, Tr. 942, 944-46, 950-51, 959-62, 970, 982, 1036, 1063-65). However, FTC failed to prove a reasoned countervailing benefit analysis as required by law.*Fox Television II*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action").

49. Consumers "realized no benefit" from LabMD's data security failures. *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *90 (1984).

Reply to Proposed Conclusion of Law No. 49

Complaint Counsel's Proposed Conclusion of Law No. 49 is a statement of fact and should be stricken accordingly. It is also erroneous and insufficient.

First, Complaint Counsel needs to specify the specific "data security failures" it alleges. There was no data breach here and no actual or certainly impending substantial injury to any patient. There is no allegation LabMD violated applicable HIPAA regulations. Therefore, there were no data security "failures" or departures from medical industry data security standards during the relevant time. *See Fabi Const. Co.*, 508 F.3d at 1088 (industry standards for building construction company applied); *Ensign-Bickford Co.*, 717 F.2d at 1422 (industry standards for pyrotechnic industry applied); *S&H Riggers*, 659 F.2d at 1280-83 (reasonable-person standard divorced from relevant industry standards or regulations violates due process). LabMD has not violated HIPAA/HITECH. *See* Complaint Counsel's Amended Response To LabMD, Inc.'s First Set Of Requests For Admission, *In the Matter of LabMD*, No. 9357, Responses No. 7 and No. 8, at pp. 8-9, appended to Complaint Counsel's Motion to Amend Complaint Counsel's

Response to Respondent's First Set of Requests for Admission (F.T.C. Apr. 1, 2014); *see also* Compl., *In the Matter of LabMD*, No. 9357 (F.T.C. Aug. 28, 2013).

Second, FTC failed to provide a reasoned countervailing benefit analysis as required by law. *Fox Television II*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action"). Therefore, this Proposed Conclusion of Law is not supportable. Section 5(n) requires FTC to conduct a countervailing benefit analysis, and declare unlawful only those unfair practices that fail review. 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.*, 104 F.T.C. at 1073-74. However, Complaint Counsel has offered nothing of the sort. *Compare Neovi, Inc.*, 598 F. Supp. 2d at 1115 (FTC offered expert testimony that the defendants' business model did not provide any advantage and that any benefits were small, that it did not have a positive impact in the marketplace and did not benefit competition).

> 50. Countervailing benefits are unlikely to be significant when more effective security measures could have been implemented at relatively low cost. *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *97 (1984) (Unfairness Statement) (stating that "[m]ost business practices entail a mixture of economic and other costs and benefits for purchasers" and framing the evaluation as to whether a practice is "injurious in its net effects," taking into account the "various costs that a remedy would entail").

Reply to Proposed Conclusion of Law No. 50

Complaint Counsel's Proposed Conclusion of Law No. 50 is erroneous and misleading.

First, Complaint Counsel does not cite to *Int'l Harvester* in appropriate context:

> [T]he injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces. Most business practices entail a mixture of economic and other costs and benefits for purchasers. A seller's failure to present complex technical data on his product may lessen a consumer's ability to choose, for example, but may also reduce the initial price he must pay for the article. The

> Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects. The Commission also takes account of the various costs that a remedy would entail. These 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."

Int'l Harvester Co., 104 F.T.C. at 1061.

Complaint Counsel's omission of the final sentence to this citation from *Int'l Harvester* renders Proposed Conclusion of Law No. 50 simply wrong as a matter of law. Complaint Counsel failed to evaluate any of "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" that its claim against LabMD might create – in other words, a proper cost-benefit analysis was required here. *See* CCPCL ¶ 14; *Sperry*, 405 U.S. at 248-49; *Fox Television II*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action").

> 51. LabMD could have discovered and corrected its security failures at low or no cost. *Supra* CCFF § 6 (LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low-Cost Measures) *et seq.* (¶¶ 1113-1185); *see also Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *91 (1984) ("Harvester's expenses were not large in relation to the injuries that could have been avoided.").

Reply to Proposed Conclusion of Law No. 51

Complaint Counsel's Proposed Conclusion of Law No. 51 is a statement of fact and should be stricken accordingly. It is also erroneous.

First, Complaint Counsel has not proven "security failures." The 1718 File, stolen by the ace hacker Wallace acting at the express direction of his boss, Boback, was not exposed on the internet, as Boback, Tiversa, Complaint Counsel, and Complaint Counsel's experts claimed. FTC proved nothing about the Day Sheets. And there are no victims. LabMD's "security

failures" exist only because Dr. Hill says that they do, not because of any objective event or evidence.

Second, claims about the cost of "correction" do not substitute for a proper cost-benefit analysis as Section 5(n) requires. *See* CCPCL ¶ 14. Complaint Counsel failed to prove by a preponderance of the evidence that any benefit in terms of reduced risk from changing LabMD's data security practices would have outweighed not only the costs to LabMD, but also the additional burdens to the doctors and their patients who benefitted from LabMD's system. Perhaps the data security demands made retroactively by FTC in Dr. Hill's 2014 opinion, over and above HIPAA, might have made no difference to LabMD's operations. But FTC never did this analysis or calculated net effects. As a result, FTC cannot meet the test of Section 5(n) and may not declare LabMD's data security practices unlawful. *Fox Television II*, 556 U.S. at 515; *Clinton*, 684 F.3d at 75-77 .

Third, Complaint Counsel misapplies *Int'l Harvester*. That case involved serious physical injury and death: "There clearly has been serious consumer injury. At least one person has been killed and eleven others burned. Many of the burn injuries have been major ones, moreover, resulting in mobility limitations, lasting psychological harm, and severe disfigurement." *Int'l Harvester Co.*, 104 F.T.C. at 1065. Here, there has been no injury at all.

52. Because they could have been discovered and corrected at low cost, LabMD's data security failures did not provide any advantage over competing laboratories' practices. *See FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (where business model incorporating unfair acts and practices provides no advantage in the marketplace, "any benefits were small").

Reply to Proposed Conclusion of Law No. 52

Complaint Counsel's Proposed Conclusion of Law No. 52 is a statement of fact and should be stricken accordingly. It is also erroneous.

First, FTC did not introduce any evidence or testimony establishing that "LabMD's data security failures did not provide any advantage over competing laboratories' practices." This is because it did not conduct the countervailing benefit analysis it was required to prepare to comply with Section 5(n). In fact, FTC introduced no comparison evidence at all.

Second, Complaint Counsel again misapplies *Neovi*, a case with actual, concrete, substantial injury to consumers. There, FTC presented an expert cost-benefit analysis of the defendant's business model. 598 F. Supp. 2d at 1116. Here, there was nothing of the sort.

53. Because LabMD could have discovered and corrected its security failures at low or no cost, its data security failures provide no countervailing benefit to consumers or competition. *See Int'l Harvester Co.*, Docket No. 9147, 104 F.T.C. 949, 1984 WL 565290 at *90 (1984) (identifying the "principal tradeoff to be considered" as "compliance costs").

Reply to Proposed Conclusion of Law No. 53

Complaint Counsel's Proposed Conclusion of Law No. 53 is a statement of fact and should be stricken accordingly. It is also erroneous and misleading.

First, Complaint Counsel offers no evidence demonstrating that it made any evaluation of the impact that the alleged, unspecified "corrections" of LabMD's unspecified "security failures" (over and above HIPAA) might have had on LabMD's operational efficiency, as required by Section 5(n). In fact, LabMD's IT architecture was optimized to provide efficient service and HIPAA-compliant security. *See* (Daugherty, Tr. 942, 944-46, 950-51, 959-62, 970, 982, 1036, 1063-65). Lacking appropriate expert testimony about the costs and benefits of LabMD's specific business and its particular operations, Complaint Counsel fails. *Neovi, Inc.*, 598 F. Supp. 2d at 1116.

Second, Complaint Counsel misapplies *Int'l Harvester* to this case. *Int'l Harverster* actually commits Complaint Counsel to a granular analysis of "net effects." According to the Commission:

> [C]onduct must be harmful in its net effects. This is simply a recognition of the fact that most conduct creates a mixture of both beneficial and adverse consequences . . . this part of the unfairness analysis requires us to balance against the risks of injury the costs of notification and the costs of determining what the prevailing consumer misconceptions actually are. *This inquiry must be made in a level of detail that the deception analysis does not contemplate.*

Int'l Harvester Co., 104 F.T.C. at 1061 (emphasis added). FTC did not analyze "net effects" here.

Also, the decision is relevant because it clarifies that the primary focus of the Unfairness Policy Statement is "to keep the FTC Act focused on the economic issues that are its proper concern. The Commission does not ordinarily seek to mandate specific conduct or specific social outcomes but rather seeks to ensure simply that markets operate freely so that consumers can make their own decisions." *Id.* FTC's conduct in this case has absolutely nothing to do with ensuring that medical markets "operate freely so that consumers can make their own decisions." Rather, FTC seeks to mandate specific conduct (which contradicts with HIPAA regulations).

54. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 54

LabMD has no specific response to Proposed Conclusion of Law No. 54.

1.4 Remedy

1.4.1 Corporate Liability

55. The Commission may enter an order against a corporation for violations of the FTC Act. 15 U.S.C. § 45(b).

Reply to Proposed Conclusion of Law No. 55

LabMD has no specific response to Proposed Conclusion of Law No. 55.

56. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 56

LabMD has no specific response to Proposed Conclusion of Law No. 56.

1.4.2 Entry of the Notice Order is Appropriate and Necessary

57. Entering an order to require LabMD to implement reasonable data security for consumer Personal Information and to obtain biennial assessments is appropriate because the findings of fact are "supported by substantial evidence upon the record as a whole." *Niresk Indus. Inc. v. FTC*, 278 F.2d 337, 340 (7th Cir. 1960) (citation omitted).

Reply to Proposed Conclusion of Law No. 57

Complaint Counsel's Proposed Conclusion of Law No. 57 is erroneous and unjustified.

First, the burden of proof under Section 5, especially with respect to Section 5(n), is at least a preponderance.

Second, requiring biennial assessments is unlawful. 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 to carry out these assessments.

Complaint Counsel would authorize 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 FTC thus breaks the law. *Ass'n of Am. R.R.s*, 135 S. Ct. at 1236; *Bennett*, 520 U.S. at 169.

Especially because FTC lacks properly promulgated data security rules or guidance for medical companies otherwise subject to HIPAA, Complaint Counsel's proposal raises Appointments Clause, separation of powers, and due process concerns. *Ass'n of Am. R.R.s*, 135 S. Ct. 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*, 298 U.S. at 311.

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."

Third, as a matter of law, Complaint Counsel's proposed order is not equitable but punitive in nature and the Commission is not authorized to issue punitive orders. *Heater*, 503 F.2d at 322-327 (overturning an FTC order for restitution as inconsistent with the purpose of the FTC Act, which does not authorize punitive or retroactive punishment).

58. An appropriate order must bear a reasonable relationship to the unlawful acts or practices alleged in the complaint. *See, e.g.*, *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 394-95 (1965); *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952); *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612-13 (1946). Within that framework, the Commission has "considerable discretion in fashioning an appropriate remedial order," *Daniel Chapter One*, Docket No. 9329, 2009 FTC LEXIS 157, at *275, including an order to cease and desist from conduct found to violate Section 5 of the FTC Act. 15 U.S.C. § 45(b); *FTC v. Nat'l Lead Co.*, 352 U.S. 419, 428 (1957).

Reply to Proposed Conclusion of Law No. 58

LabMD has no specific response to Proposed Conclusion of Law No. 58, except that "[o]rders of the Federal Trade Commission are not intended to impose criminal punishment or exact compensatory damages for past acts, but to prevent illegal practices in the future." *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952) (emphasis added).

59. The FTC has wide latitude in crafting appropriate relief. The Commission "cannot be required to confine its road block to the narrow lane the transgressor traveled; it must be allowed effectively to close all roads to the prohibited goal, so that its order may not be by-passed with impunity." *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952).

Reply to Proposed Conclusion of Law No. 59

LabMD has no specific response to Proposed Conclusion of Law No. 59.

60. LabMD has no intent to dissolve as a Georgia corporation. (JX0001-A (Joint Stips. of Law, Fact, and Auth.) at 3).

Reply to Proposed Conclusion of Law No. 60

Complaint Counsel's Proposed Conclusion of Law No. 60 is a statement of fact and should be stricken accordingly.

61. In the future, LabMD intends to employ the same policies and procedures to information in its possession as it employed in the past. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 5-6 (Resp. to Req. 38), 7 (Resp. to Interrog. 12).

Reply to Proposed Conclusion of Law No. 61

Complaint Counsel's Proposed Conclusion of Law No. 61 is a putative statement of fact and should be stricken accordingly. The evidence is that LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future.

62. LabMD retains the Personal Information of over 750,000 consumers. *Supra* CCFF § 4.6.1 (Amount of Personal Information Collected) (¶ 78).

Reply to Proposed Conclusion of Law No. 62

Complaint Counsel's Proposed Conclusion of Law No. 62 is a putative statement of fact and should be stricken accordingly. The evidence is LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future

63. LabMD continues to operate a computer network consisting of switches, routers, servers, workstation computers, printers, a scanner, and an Internet connection at Mr. Daugherty's residence, as well as a workstation at a condominium that can remotely connect to a server at the private residence network and a printer for the condominium workstation. *Supra* CCFF § 4.7.4 (Internal Network from January 2014 to Present) (¶¶ 251-260).

Reply to Proposed Conclusion of Law No. 63

Complaint Counsel's Proposed Conclusion of Law No. 63 is a putative statement of fact and should be stricken accordingly. The evidence is LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future

64. LabMD continues to provide past test results to healthcare providers and continues to collect on monies owed to it. *Supra* CCFF § 4.4 (Wind Down and Current Status) (¶ 63).

Reply to Proposed Conclusion of Law No. 64

Complaint Counsel's Proposed Conclusion of Law No. 64 is a putative statement of fact and should be stricken accordingly. The evidence is LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future.

65. Even if LabMD were not currently operating, it would not be a bar to entry of a notice order. *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953) (burden of proving that a case has become moot by reason of discontinuance of defendant's conduct is "a heavy one" that requires the defendant to demonstrate "'there is no reasonable expectation that the wrong will be repeated'" (citing *U.S. v. Alumunum Co. of Am.*, 148 F.2d 416, 448 (2d Cir. 1945)); *see also id.* at 632 ("The courts have rightly refused to grand defendants such a powerful weapon [procuring mootness by ceasing challenged conduct] against public law enforcement.").

Reply to Proposed Conclusion of Law No. 65

Complaint Counsel's Proposed Conclusion of Law No. 65 is erroneous and misleading. Complaint Counsel misapplies *W.T. Grant Co.*, 345 U.S. 629. There, the Court held:

> The purpose of an injunction is to prevent future violations, and, of course, it can be utilized even without a showing of past wrongs. But [Complaint Counsel] must satisfy the court that relief is needed. 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 be considered are the bona fides of the expressed intent to comply, the effectiveness of the discontinuance and, in some cases, the character of the past violations.

Id. at 633-34. Complaint Counsel's case terminates in July 2010, and it has shown no cognizable danger of recurrent violation.

66. As of February 2014, the paper records kept at Mr. Daugherty's residence were observed located in rooms throughout the house and were not secured in any way. (CX0725-A (Martin, Dep. at 22)).

Reply to Proposed Conclusion of Law No. 66

Complaint Counsel's Proposed Conclusion of Law No. 66 is a putative statement of fact and should be stricken accordingly. It also misstates the evidence, because Mr. Daugherty's residence was secure from outside intrusion. The evidence is LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future.

67. Likewise, the patient specimens in the basement were also not secured in any way. (CX0725-A (Martin, Dep. at 23)).

Reply to Proposed Conclusion of Law No. 67

Complaint Counsel's Proposed Conclusion of Law No. 67 is a putative statement of fact and should be stricken accordingly. It also misstates the evidence because Mr. Daugherty's residence was secure from outside intrusion. The evidence is LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future.

68. As of approximately February 2014, some of the items were kept in the garage and the garage was not always locked. (CX0713-A (Gardner, Dep. at 45)). When Ms. Parr went to Mr. Daugherty's home to help finish up some network work there, Mr. Daugherty was not there and the garage door was up. (CX0713-A (Gardner, Dep. at 45-46)).

Reply to Proposed Conclusion of Law No. 68

Complaint Counsel's Proposed Conclusion of Law No. 68 is a putative statement of fact and should be stricken accordingly. It also misstates the evidence, because Mr. Daugherty's residence was secure from outside intrusion. The evidence is LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future.

69. LabMD's retention of this Personal Information, continued operation of a computer network, and observed physical security issues demonstrates that "'there exists some cognizable danger of recurrent violation." *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1201 (10th Cir. 2009) (quoting *U.S. v. W.T.*

Grant Co., 345 U.S. 629, 633 (1953)); *see also FTC v. Commerce Planet, Inc., 878 F. Supp. 2d 1048, 1087-88 (C.D. Cal. 2012)* (finding permanent injunction appropriate where defendant continued to work in same business field, even though no longer involved in the same type of conduct); *FTC v. RCA Credit Servs., LLC*, 727 F. Supp. 2d 1320, 1337 (M.D. Fla. 2010) (finding that defendant's new business venture in a similar industry "presented significant opportunities for similar violations"); *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393-94 (D. Conn. 2009) (imposing a permanent injunction where discontinued conduct was "obvious and widespread" rather than "a single instance"). Furthermore, "[a] 'court's power to grant injunctive relief survives the discontinuance of the illegal conduct.'" *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1201 (10th Cir. 2009) (quoting *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953)).

Reply to Proposed Conclusion of Law No. 69

Complaint Counsel's Proposed Conclusion of Law No. 69 is a putative statement of fact and should be stricken accordingly. The evidence is LabMD complied with HIPAA data security and breach notification regulations in the past and will do so in the future. It is also erroneous.

First, Complaint Counsel has offered no evidence to support its claim that "LabMD's retention of this Personal Information, continued operation of a computer network, and observed physical security issues demonstrates that "there exists some cognizable danger of recurrent violation." None of its experts testified to this.

Second, there is no evidence of past data breaches or HIPAA violations in this case. On that record, the cases cited by Complaint Counsel are inapplicable. For example, *Commerce Planet* involved actual monetary harm of "$45 million in two years by tricking over 470,000 consumers into unwittingly submitting their credit card information, which was used to charge them a monthly subscription fee without their informed consent." *Commerce Planet, Inc.*, 878 F. Supp. 2d at 1063.

RCA Credit Services also involved substantial, actual, concrete harm to consumers: "Defendants disseminated their false representations to anyone who visited their website or

called their telephone number. The undisputed evidence shows that numerous consumers were in fact misled by the misrepresentations and were harmed economically as a result." *FTC v. RCA Credit Servs., LLC*, 727 F. Supp. 2d 1320, 1336 (M.D. Fla. 2010). And *Bronson Partners* is the same: "[D]efendants duped consumers into spending in excess of $ 1.9 million for fraudulent weight loss products. The advertising for Diet Tea and the Patch was false, misleading, and contained numerous wildly unsubstantiated claims and was distributed through multiple media means including magazines, catalogs and a website." *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009) (emphasis added).

The totality of the circumstances surrounding LabMD and its alleged violations (over and above HIPAA) must be considered. *SEC v. Murphy*, 626 F.2d 633, 655 (9th Cir. 1980); *SEC v. Holschuh*, 694 F.2d 130, 144 (7th Cir. 1982) (Among the factors court considered are the degree of scienter, whether the conduct was an isolated instance or recurrent, whether the defendants' current occupations position them to commit future violations, the degree of harm consumers suffered from defendants' unlawful conduct, and defendants' recognition of their own culpability and the sincerity of their assurances (if any) against future violations.). Simply put, Complaint Counsel failed to prove that LabMD engaged in past conduct which in any way indicates that there is a cognizable danger of a recurrent violation. *Borg-Warner Corp.*, 746 F.2d at 110-11 (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); *Litton Indus.*, 676 F.2d at 370 (the "ultimate question is the likelihood of the petitioner committing the sort of unfair practices they prohibit" in the future).

70. Injunctions issue based on the "'necessities of the public interest,'" balancing the interests of the parties who might be affected by the decision. *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009) (quoting *US v. Oakland Cannabis Buyers' Coop*., 532 U.S. 483, 496 (2001). Here, the interests

> to be balanced are the consumers' whose Personal Information LabMD holds, including consumers for whom LabMD performed no medical testing or other services, and LabMD's interests. As demonstrated *supra*, *see generally* § 9 (LabMD's Data Security Practices Caused or are Likely to Cause Substantial Injury to Consumers that is Not Reasonably Avoidable by the Consumers Themselves and Are Not Outweighed by Countervailing Benefits to Consumers or Competition) *et seq.* (¶¶ 1472-1798), future failures to maintain reasonable data security would likely result in substantial harm to consumers. *See FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009) (imposing injunction where "[f]uture violations of a similar nature would surely result in financial harm to consumers").

Reply to Proposed Conclusion of Law No. 70

Complaint Counsel's Proposed Conclusion of Law No. 70 is erroneous, legally insufficient, incomplete, and misleading.

First, Complaint Counsel wrongfully twists the evidence. It claims "the interests to be balanced are the consumers' whose Personal Information LabMD holds, including consumers for whom LabMD performed no medical testing or other services, and LabMD's interests." However, the testimony was that doctors decided what patient information to provide LabMD. 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…. It'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); *see also* (Daugherty, Tr. 942, 944-46, 950-51, 959-62, 970, 982, 1036).

Second, the holding in *Oakland Cannabis* is quite a bit more complex than suggested. After noting the extraordinary nature of injunctive relief, the Court had this to say about factors to be considered: "To the extent the district court considers the public interest and the conveniences of the parties, the court is limited to evaluating how such interest and conveniences are affected by the selection of an injunction over other enforcement mechanisms." *United States v. Oakland Cannabis Buyers' Coop*., 532 U.S. 483, 498 (2001). On a court's discretion in fashioning injunctive remedies:

> [T]he mere fact that the District Court had discretion does not suggest that the District Court, when evaluating the motion to modify the injunction, could consider any and all factors that might relate to the public interest or the conveniences of the parties, including the medical needs of the Cooperative's patients. On the contrary, a court sitting in equity cannot 'ignore the judgment of Congress, deliberately expressed in legislation.' A district court cannot, for example, override Congress' policy choice, articulated in a statute, as to what behavior should be prohibited. 'Once Congress, exercising its delegated powers, has decided the order of priorities in a given area, it is . . . for the courts to enforce them when enforcement is sought.' Courts of equity cannot, in their discretion, reject the balance that Congress has struck in a statute.'

Id. at 497 (citations omitted).

In this proceeding, there are no past violations because there is no unfairness under Section 5(a), or actual or certainly impending substantial injury necessary to even trigger a Section 5(n) analysis. *Bronson Partners* is no help to the government here: "defendants duped consumers into spending in excess of $ 1.9 million for fraudulent weight loss products. The advertising for Diet Tea and the Patch was false, misleading, and contained numerous wildly unsubstantiated claims and was distributed through multiple media means including magazines,

catalogs and a website." *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009). Complaint Counsel omits the *W.T. Grant* factors in asserting a putative propositional request for injunctive relief because, given the absence of testimony that LabMD's post-July 2010 data security practices violate either HIPAA or FTC's manufactured data security regime, Complaint Counsel has no case.

Simply put, Complaint Counsel failed to prove that LabMD engaged in past conduct which in any way indicates "that there is a cognizable danger of a recurrent violation." *Borg-Warner Corp.*, 746 F.2d at 110-11 (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); *Litton Indus.*, 676 F.2d at 370 (the "ultimate question is the likelihood of the petitioner committing the sort of unfair practices they prohibit" in the future); *see also W.T. Grant Co.*, 345 U.S. at 633.

71. That LabMD is not currently collecting new specimens for testing is not a bar to entry of the notice order. *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *92 (1984) (case not moot even where "the specific facts alleged" are "unlikely to arise again" if there is a possibility the respondent may "return to the general course of conduct with which it is charged").

Reply to Proposed Conclusion of Law No. 71

Complaint Counsel's Proposed Conclusion of Law No. 71 is erroneous and misleading Complaint Counsel misapplies the precedent. The Commission held in *Int'l Harvester* that the matter was not "moot" because, due to years of serious personal injuries and even deaths, complaint counsel was seeking a broad order against non-disclosure of hazards on any and all types of Harvester farm equipment, not merely gasoline-powered tractors. Although Harvester had ceased to sell such tractors, "the developments Harvester points to have . . . not given complaint counsel everything he might win through litigation, and the case is therefore not moot." *Int'l Harvester Co.*, 104 F.T.C. at 1067. The Commission's remedy, however, was

to do nothing, because "all-products orders are most appropriate vehicles for 'fencing-in' violators when there is a particularly great risk of a recurrence of the illegal conduct [and] Harvester's conduct does not lead us to such fears." Harvester's voluntary notice program had provided all of the relief that could be expected from a Commission order, and the changing technology "had obviated any concern that Harvester might return to its earlier violations" that caused harm. *Id.* at 1069-70.

Here, Complaint Counsel cannot win something under Section 5 that might conflict with HIPAA. In other words, Complaint Counsel can obtain nothing more from this litigation than HIPAA compliance. Given that there is no evidence LabMD ever violated HIPAA, and no evidence that LabMD ever violated FTC's "standards" post-July 2010, there is no evidence in the record of a "particularly great risk of a reoccurrence of the illegal conduct," and no reason to believe LabMD will not continue to comply with applicable regulations as it has since 2003. Furthermore, changing technology has left FTC's complaints about "inadequate" passwords, weak firewalls, and the like in the dust. *Int'l Harvester* therefore stands for the proposition that this case should be dismissed.

72. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 72

LabMD has no specific response to Proposed Conclusion of Law No. 72.

1.4.2.1 An Injunction is an Appropriate Remedy

73. Factors to consider in determining whether to impose an injunction based on past conduct include: "the egregiousness of the defendant's actions, the isolated or recurrent nature of the infraction, the degree of scienter involved, the sincerity of the defendant's assurances against future violations, the defendant's recognition of the wrongful nature of his conduct, and the likelihood that the defendant's occupation will present opportunities for future violations." *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009) (quoting *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 1013, 1017 (N.D. Ind. 2000). On the whole, these factors favor an injunction in this matter.

Reply to Proposed Conclusion of Law No. 73

Complaint Counsel's Proposed Conclusion of Law No. 73 is erroneous, misleading, and not supported by the facts in this proceeding. The last statement in Proposed Conclusion of Law No. 73 is wrong as a matter of law, as is any contemplation of an injunction as an appropriate remedy in this case when neither actual harm nor a likelihood of substantial harm has been proved regarding any consumer. *See Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (declining to order any remedy on facts showing company good faith effort to notify tractor defect and changing technology that led it to cease manufacturing gasoline-powered tractors entirely).

First, Complaint Counsel has misapplied an irrelevant authority. *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009) arises under 15 U.S.C. § 53(b), authorizing injunctive relief for deceptive advertising. This provision has nothing to do with "fencing in" relief under Section 5 for a case in which there is no evidence of a single consumer that has suffered or is likely to suffer substantial injury, no evidence of regulatory violations, and no evidence that the specific acts and technologies claimed to have constituted, taken together, an unfair and unlawful practice. *Cf. Borg-Warner Corp.*, 746 F.2d at 110-11. Among other things, *Direct Marketing* holds that the defendant bears the burden of proving an injunction is unnecessary. Here, however, Complaint Counsel bears the entire burden of proof:

> In *United States v. W.T. Grant Co.*, . . . the Court announced the principle that to obtain injunctive relief against illegal conduct that had been discontinued, the moving party must show that 'there exists some cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive.' In Commission proceedings it is 'the FTC staff's burden of showing that an injunction was warranted.' Contrary to the Commission's conclusion, we do not think complaint counsel carried the burden of showing that there was a 'cognizable danger of recurrent violation' in this case.

Borg-Warner Corp., 746 F.2d at 110 (citations omitted).

Second, Complaint Counsel failed to prove "that there is a cognizable danger of a recurrent violation." Here, as in *Borg-Warner*, the specific conduct that the Commission complained of (certain pre-July 2010 data security software, hardware, and employee training practices here; participation in the auto parts business and an interlocking directorate two and three years before, respectively, there) ceased years before the Commission's demand for a cease and desist order and "fencing in" relief. *Id.* at 110-11. "The likelihood . . . Borg-Warner [will return] to the automotive parts business is too conjectural and speculative to justify an injunction against future interlocking directorates between Borg-Warner and other companies in competition with it. Indeed, this conjectural speculation is the very kind of 'mere possibility' of recurrent violation that the Supreme Court stated in *Grant* was not sufficient to justify equitable relief against a terminated violation." *Id.*at 111.

Furthermore, the court ruled "[t]here are additional considerations that further undermine and vitiate the Commission's determination that there is a cognizable danger of recurrent violation." *Id.* For example, the violations the Commission found were "not flagrant or longstanding," the interlocking directorates "followed the common practice of placing representatives on the company's board of directors to monitor its investment," the total amount of sales with respect to which the Commission found that Borg-Warner and Bosch U.S. were competitors was relatively small, and Borg-Warner was screening all nominees to the board of directors." *Id.* Here too, the additional considerations, including but not limited to LabMD's HIPAA status and compliance, the absence of any data breach during the January 2005 to July 2010 time frame, and the current nature of its operations "further undermine and vitiate" Complaint Counsel's demand for injunctive relief. There is simply no basis in law to require LabMD to comply with onerous and punitive requirements such as establishing a

"comprehensive information security program," hiring outside professionals to conduct biannual audits, and hiring additional personnel to monitor the security of data that is not being actively used and is being kept on computers that are stored with the power off. *Borg-Warner Corp.*, 746 F.2d at 110-11.

Third, as a matter of law, Complaint Counsel failed to prove by a preponderance of the evidence that LabMD's past course of conduct provides a legally sufficient basis for believing that it will violate Section 5(n) in the future. *See Riordan v. SEC*, 627 F.3d 1230, 1234 (D.C. Cir. 2010). Such relief "must be sufficiently clear that it is comprehensible to the violator, and must be 'reasonably related' to a violation of the [FTC] Act." *See Daniel Chapter One*, 2009 FTC LEXIS 157 at *280-81 (citations omitted). Whether fencing-in relief bears a "reasonable relationship" to the conduct found to be unlawful depends on: "(1) the deliberateness and seriousness of the violation; (2) the degree of transferability of the violation to other products; and, (3) any history of prior violations." *See id.* It must be "reasonably calculated to prevent future violations of the sort found to have been committed." *See ITT Cont'l Baking Co.*, 532 F.2d at 221-22.

The first factor for fencing-in relief is "the deliberateness and seriousness of the present violation." *See Daniel Chapter One*, 2009 FTC LEXIS 157 at *280-81. As a matter of law, Complaint Counsel failed to prove by a preponderance of the evidence that LabMD knowingly violated Section 5 or that such violations were "serious." *Compare id.* at *281-82, *with In re POM Wonderful LLC*, No. 9344, 2012 FTC LEXIS 18, at *97-*98 (F.T.C. Jan. 11, 2012). Complaint Counsel does not dispute that LabMD's data security complied with HIPAA and failed to prove that a HIPAA-compliant data security program could be a "serious" violation of Section 5.

The second factor is "the degree of transferability of the violation to other products." *See Daniel Chapter One*, 2009 FTC LEXIS 157 at *280-81. As a matter of law, Complaint Counsel has failed to prove transferability in this case. The only evidence is that LabMD took its HIPAA obligations to protect patient data security very seriously and terminated employees who were found to violate company policy. *See* RPFOF ¶ 232.

The third factor is "history of prior violations." *See Daniel Chapter One*, 2009 FTC LEXIS 157 at *280-81. Complaint Counsel failed to prove any. Fencing-in relief is therefore both unnecessary and unlawfully punitive in this case. *See Riordan*, 627 F.3d at 1234 ("[W]e have stated that a cease-and-desist order is 'purely remedial and preventative' and not a 'penalty' or 'forfeiture.'" (citing *Drath v. FTC*, 239 F.2d 452, 454 (D.C. Cir. 1956)).

74. LabMD's data security failures were pervasive and persistent, rather than isolated, involving multiple types of problems over many years. *See, e.g.*, *supra* CCFF §§ 5.2 (LabMD Did Not Develop and Maintain a Comprehensive Written Information Security Program) *et seq.* (¶¶ 397-480) (many practices not memorialized until 2010, and 2010 written policies not comprehensive); 5.3 (LabMD Did Not Use Reasonable, Readily Available Measures to Identify Commonly Known or Reasonably Foreseeable Security Risks and Vulnerabilities) *et seq.* (¶¶ 483-808) (for years and over multiple antivirus programs, LabMD did not consistently update virus definitions in its antivirus software, run antivirus scans, or review the results of antivirus scans; and did not conduct penetration testing until 2010); 5.4 (LabMD Did Not Use Adequate Measures to Prevent Employees from Accessing Personal Information Not Needed to Perform Their Jobs) *et seq.* (¶¶ 811-849) (never deleted any Personal Information, did not implement access controls over a long period of time); 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) *et seq.* (¶¶ 852-900) (failed to provide security training to IT and non-IT employees over many years); 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq.* (¶¶ 903-993) (employees used weak passwords for years, and LabMD did not centrally manage passwords or provide for effective enforcement of its password policies until 2010); 5.7 (LabMD Did Not Maintain and Update Operating Systems and Other Devices) *et seq.* (¶¶ 996-1043) (used operating systems and programs years after the vendors stopped supporting them, and failed to patch vulnerabilities years after vendors warned of risks); 5.8 (LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information) *et seq.* (¶¶ 1045-1110) (gave some employees administrative rights over their computers

and unlimited internet access for years, stored backups of personal information on employee workstations for years).

Reply to Proposed Conclusion of Law No. 74

Complaint Counsel's Proposed Conclusion of Law No. 74 is a statement of fact and should be stricken accordingly. It is also erroneous, incomplete, misleading, and not supported by the facts in this proceeding.

Prior to this adjudication, FTC had never given notice that HIPAA-regulated companies must obey unpublished FTC Section 5 "standards" for a "comprehensive written security program," regulating administrative rights, updating virus scans, plugging ports, access controls, and other measures. Although the Commission publishes general statements of policy at 16 C.F.R. Part 14, and could have given such notice to LabMD and others at any point, there is none for medical data security. Instead, the Commission has created and applied data security standards as if they had been promulgated as a guide or trade rule. *Cf.* Fed. Trade Comm'n, "Start With Security," https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (June 2015); Fed. Trade Comm'n, "Information Compromise and the Risk of Identity Theft: Guidance for Your Business," https://www.ftc.gov/tips-advice/business-center/guidance/information-compromise-risk-identity-theft-guidance-your (June 2004) (directing businesses to preferred contractors); *see also* 16 C.F.R. § 14.9 (titled "Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials" and warning "[a]ny respondent who fails to comply with [the specified] requirement may be the subject of a civil penalty or other law enforcement proceeding for violating the terms of a Commission cease-and-desist order or rule"); 16 C.F.R. § 453.1 (funeral rule definitions). The Commission's use of adjudication to set or apply supposedly preexisting medical data security standards that might add to or alter existing APA-promulgated HIPAA

regulations or guidance, based on materials not previously published in the Federal Register is an abuse of discretion and contrary to law under the APA. 5 U.S.C. § 552(a)(1)(D). 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.*, 673 F.2d at 1010-11.

Second, Complaint Counsel's claims here, all based on the testimony of Dr. Hill who did not apply or know HIPAA, create a facial conflict with that regulatory regime and so this proceeding is unlawful. *Credit Suisse*, 551 U.S. at 275.

Third, only an actual data breach meets FTC's own criteria for substantial injury. Complaint Counsel has failed to prove that any of these alleged deficiencies were connected to the "Security Incidents" alleged in the Complaint, that these acts, which all pre-date July 2010, either continue or are likely to cause substantial injury (or any injury) to consumers in the future, that substantial injury is certainly impending, or that these acts were "unfair" under Section 5(a) and "unlawful" under Section 5(n).

75. LabMD, through its employees and contractors, made decisions regarding data security, such as failing to enforce its security policies, *supra* CCFF § 5.2.4 (LabMD Did Not Enforce Some of the Policies in its Policy Manuals) *et seq.* (¶¶ 458-480), failing to consistently run and review antivirus scans, *supra* CCFF § 5.3.2.1 (LabMD's Use of Antivirus Software Could Not Reliably Detect Security Risks Because It Did Not Consistently Update Virus Definitions, Run Scans, or Review Scans) *et seq.* (¶¶ 527-629), haphazardly deploying incomplete and ineffective manual inspections, *supra* CCFF § 5.3.2.3 (LabMD's Manual Inspections Could Not Reliably Detect Security Risks) *et seq.* (¶¶ 660-696), and permitting users on its system to use weak passwords for years, *supra* CCFF § 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq.* (¶¶ 903-993).

Reply to Proposed Conclusion of Law No. 75

Complaint Counsel's Proposed Conclusion of Law No. 75 is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, immaterial, misleading, and not supported by the facts in this proceeding.

Prior to this adjudication, FTC had never given notice that HIPAA-regulated companies must obey unpublished FTC Section 5 "standards" for a virus scans, authentication-related security measures, and manual inspections. Although the Commission publishes general statements of policy at 16 C.F.R. Part 14, and could have given such notice to LabMD and others at any point, there is none for medical data security. Instead, the Commission has created and applied data security standards as if they had been promulgated as a guide or trade rule. *Cf.* Fed. Trade Comm'n, "Start With Security," https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (June 2015); Fed. Trade Comm'n, "Information Compromise and the Risk of Identity Theft: Guidance for Your Business," https://www.ftc.gov/tips-advice/business-center/guidance/information-compromise-risk-identity-theft-guidance-your (June 2004) (directing businesses to preferred contractors); *see also* 16 C.F.R. § 14.9 (titled "Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials" and warning "[a]ny respondent who fails to comply with [the specified] requirement may be the subject of a civil penalty or other law enforcement proceeding for violating the terms of a Commission cease-and-desist order or rule"); 16 C.F.R. § 453.1 (funeral rule definitions). The Commission's use of adjudication to set or apply supposedly preexisting medical data security standards that might add to or alter existing APA-promulgated HIPAA regulations or guidance, based on materials not previously published in the Federal Register is an abuse of discretion and contrary to law under the APA. 5 U.S.C. § 552(a)(1)(D). 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.*, 673 F.2d at 1010-11.

Second, Complaint Counsel's claims here, all based on the testimony of Dr. Hill, who did not apply or know HIPAA, create a facial conflict with that regulatory regime and so this proceeding is unlawful. *Credit Suisse*, 551 U.S. at 275.

Third, only an actual data breach meets FTC's own criteria for substantial injury. Complaint Counsel has failed to prove that any of these alleged deficiencies were connected to the "Security Incidents" alleged in the Complaint, that these acts, which all pre-date July 2010, either continue or are likely to cause substantial injury (or any injury) to consumers in the future, that substantial injury is certainly impending, or that these acts were "unfair" under Section 5(a) and "unlawful" under Section 5(n). As a matter of law, it is arbitrary, capricious, contrary to law, and a violation of due process for Complaint Counsel to allege and/or the Commission to determine unreasonableness without specific reference to HIPAA/HITECH standards and regulations. *See Fabi Constr. Co.*, 508 F.3d at 1084; *Ensign-Bickford Co.*, 717 F.2d at 1422; *S&H Riggers*, 659 F.2d at 1280-83.

76. 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).

Reply to Proposed Conclusion of Law No. 76

Complaint Counsel's Proposed Conclusion of Law No. 76 is a statement of fact and should be stricken accordingly. It is also erroneous, incomplete, intentionally misleading, and not supported by the facts in this proceeding.

Complaint Counsel's Proposed Conclusion of Law No. 76 is proof that this action is retaliatory in nature and that the proposed Notice Order is to punish LabMD for defending itself against the Commission's allegations.

The undisputed evidence LabMD is a HIPAA-regulated cancer detection lab. The undisputed evidence is that it took its obligations to protect patient privacy very seriously. The undisputed evidence is also that it never suffered a data breach and that not a single consumer has suffered any injury, "substantial" or otherwise because of its patient privacy practices. *Cf. Wyndham*, 2015 U.S. App. LEXIS 14839; *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12.

The undisputed evidence is Tiversa and Boback victimized LabMD and others for commercial gain, then lied about it to LabMD, the Eleventh Circuit, and this Court. The undisputed evidence is Tiversa and Boback created a business model based on deception, smoke, and mirrors to cheat unsuspecting companies. The undisputed evidence is that Tiversa and Boback fabricated evidence in this case, and that FTC relied on it, and Complaint Counsel defended it.

Yet Complaint Counsel now suggests that a punitive, twenty-year order is appropriate against a company that has never even been alleged to have violated HHS's comprehensive patient privacy protection laws, and without proof of unfairness, one actual data breach, or one consumer victim, because LabMD dared defy FTC and demand that the government enforce

against the fraudster, not its victims. The sheer arrogance of FTC and its Complaint Counsel in this case, where, for the first time in decades, the Justice Department granted criminal immunity in a FTC administrative proceeding to a witness who described multiple felonious criminal acts against LabMD, but more importantly, the American taxpayer, is difficult to understand. Complaint Counsel's assertion in this "conclusion of law" that LabMD deserves punitive injunctive relief for asking FTC to pursue Tiversa is a profound abuse of government power.

> 77. "[T]he FTC need not show that the defendants are likely to engage in violations involving precisely the same conduct. An injunction is justified if the FTC shows that similar violations are likely to occur." *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009) (citing *TRW, Inc. v. FTC*, 647 F.2d 942, 954 (9th Cir. 1981); *see also FTC v Accusearch, Inc.*, 2007 WL 4356786 at *9 (D. Wyo. Sept. 28, 2007) (citing *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 632 (1953) ("[T]he Commission need not show that the defendants are likely to engage in the *same precise conduct* found to be in violation of the law, but rather only that similar violations are likely to occur." (emphasis original)); *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009) ("Injunctive relief looks to future harm and is designed to deter conduct rather than punish." (citation omitted)).

Reply to Proposed Conclusion of Law No. 77

Complaint Counsel's Proposed Conclusion of Law No. 77 is a redundant statement of fact and should be stricken accordingly.

Again, Complaint Counsel has misapplied the relevant authorities. The cited district court cases are irrelevant. *Accusearch*, 570 F.3d at 1201, states the "cognizable danger of recurrent violation" standard of *W.T. Grant Co.*, 345 U.S. at 633, but it does not stand for the proposition cited by Complaint Counsel. *Borg-Warner Corp.*, 746 F.2d at 110-11 (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.*, 676 F.2d at 370, 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. 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.

78. LabMD retains the Personal Information of 750,000 consumers, which continues to be at risk. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 5, Adm. 23).

Reply to Proposed Conclusion of Law No. 78

Complaint Counsel's Proposed Conclusion of Law No. 78 is a statement of fact and should be stricken accordingly. It is also false. Complaint Counsel has offered no evidence that patient information is currently "at risk" in violation of HIPAA or Section 5. *See, e.g.*, (RX 525 (Kaufman, Dep. at 57-62 (relying solely on Hill, whose opinion stops in July, 2010, and Boback, who lied, for evidence of non-compliance and continuing harm))). Furthermore, "at risk" has no legal meaning. Complaint Counsel must reference the standards of Section 5 or HIPAA and does not do so.

79. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 79

LabMD has no specific response to Proposed Conclusion of Law No. 79.

1.4.3 Fencing-In Relief is Appropriate

80. The seriousness and deliberateness of LabMD's data security failures, the duration of its unreasonable security practices, and the transferability of the risks posed by unreasonable data security to all 750,000 consumers on whom LabMD holds Personal Information warrant broad fencing-in relief. *See infra* CCCL ¶¶ 81-89; *infra* CCCL §§ 1.4.3.1 (LabMD's Failure to Address its Data Security

Failures Was Deliberate) (¶¶ 91-103), 1.4.3.2 (LabMD's Data Security Failures Were Serious) (¶¶ 105-110), 1.4.3.3 (LabMD's Data Security Failures Are Transferrable) (¶¶ 112-114).

Reply to Proposed Conclusion of Law No. 80

Complaint Counsel's Proposed Conclusion of Law No. 80 is is a statement of fact and should be stricken accordingly. It is also erroneous. intentionally misleading, and not supported by the facts in this proceeding.

On the record, the notion of serious and deliberate "data security failures" without allegations of HIPAA violations or evidence of unfairness under Section 5(a), an actual data breach, or any consumer injury, much less substantial injury, as required by Section 5(n), is bizarre. *Compare Borg-Warner Corp.*, 746 F.2d at 110-11, *with FTC v. Wyndham*, 10 F. Supp. 3d 602, 609 (D. N.J. 2014), *aff'd* 2015 U.S. App. LEXIS 14839 (3d Cir. 2015), *and Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12. Complaint Counsel's Proposed Conclusion of Law No. 80 again suggests this proceeding is about retaliation and punishment for a company that had the temerity to say "no" to FTC staff, not about protecting consumers. *See, e.g.*, *Int'l Harvester Co.*, 104 F.T.C. at 1061 ("[T]he FTC Act [should be] focused on economic issues that are its proper concern. The Commission does not ordinarily seek to mandate specific conduct or specific social outcomes, but rather seeks to ensure simply that markets operate freely so that consumers can make their own decisions."). Only an actual data breach meets FTC's own criteria for substantial harm.

81. "[T]he Commission has wide discretion in its choice of a remedy deemed adequate to cope with the unlawful practices disclosed," and "is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past." *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952).

Reply to Proposed Conclusion of Law No. 81

Complaint Counsel's Proposed Conclusion of Law No. 81 is erroneous and misleading

Again, Complaint Counsel misapplies relevant authorities. To begin with, the actual quotation reads:

> Orders of the Federal Trade Commission are not intended to impose criminal punishment or exact compensatory damages for past acts, but to prevent illegal practices in the future. In carrying out this function the Commission is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past. If the Commission is to attain the objectives Congress envisioned, it cannot be required to confine its road block to the narrow lane the transgressor has traveled; it must be allowed effectively to close all roads to the prohibited goal, so that its order may not be by-passed with impunity.

Ruberoid Co., 343 U.S. at 473. In other words, there must be some connection between past violations and future conduct. *Int'l Harvester Co.*, 104 F.T.C. at 1061, 1069-70.

Instead, *Borg-Warner Corp.*, 746 F.2d at 110-11 (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.*, 676 F.2d at 370, 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. 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. *See also W.T. Grant Co.*, 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.").

82. The Commission is permitted "to frame its order broadly enough to prevent respondents from engaging in similarly illegal practices in [the] future." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965)).

Reply to Proposed Conclusion of Law No. 82

LabMD has no specific response to Proposed Conclusion of Law No. 82 except to note that the Commission must prove "illegal practices" and that the cited authority dealt with deception, not unfairness. *Cf. Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

83. The Commission can issue orders with fencing-in provisions that are broader than respondent's unlawful conduct. *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006).

Reply to Proposed Conclusion of Law No. 83

Complaint Counsel's Proposed Conclusion of Law No. 82 is erroneous and misleading.

First, the Commission must prove "illegal practices" and that the cited authority deals with deception, not unfairness. *Cf. Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

Second, Complaint Counsel descibes the "what" (FTC issues orders with fencing-in provisions) but not the "why": "Fencing-in remedies are designed to prevent future unlawful conduct." *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006). This is the central point: whether the requested injunction is broader than the conduct at issue is irrelevant in this proceeding. But the reason for such punitive relief, to deter future conduct, is very much at issue because LabMD has no prior violations of Section 5 and Complaint Counsel can point to no actual injury or harm of any kind which would provide a basis for this Tribunal's concern with future conduct.

Instead, *Borg-Warner Corp.*, 746 F.2d at 110-11 (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.*, 676 F.2d at 370, 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. 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. *See also UW.T. Grant Co.*, 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.").

84. Fencing-in provisions are appropriate where they are "reasonably related" to the conduct at issue. *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 216 (D. Mass. 2009). The fencing-in provisions in the Notice Order are related to Respondent's security practices and the protection of consumer Personal Information.

Reply to Proposed Conclusion of Law No. 84

Complaint Counsel's Proposed Conclusion of Law No. 84 is erroneous, misleading, and unsupported by the facts in this proceeding.

First, Complaint Counsel (again) misapplies the cited authority. *Direct Marketing* is a deception case with actual consumer harm. *Litton Indus.*, 676 F.2d at 370, 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. 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, because the relief cannot be "reasonably related" to the conduct at issue without disregard for the law and prior violations. *Accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

Second, there is no evidence in the record demonstrating that the proposed Notice Order will improve LabMD's medical data security or be consistent with HIPAA. Complaint Counsel bears the burden of proof, and it certainly could have asked Dr. Hill these things. However, it chose not to do so. Imposing the 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 II*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action"); *Credit Suisse*, 551 U.S. at 275.

> 85. Fencing-in relief is appropriate to ensure that a respondent does not engage in similar practices in the future. *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citations omitted); *FTC v. RCA Credit Servs., LLC*, 727 F. Supp. 2d 1320, 1335 (M.D. Fla. 2010).

Reply to Proposed Conclusion of Law No. 85

Complaint Counsel's Proposed Conclusion of Law No. 85 is erroneous incomplete, misleading, and not supported by the facts in this proceeding.

Proposed Conclusion of Law No. 85 is duplicative of No. 69 and should be stricken accordingly. In any event, Complaint Counsel (again) misapplies the cited authority. In each case cited, there was actual and substantial consumer injury. Here, there is none. Regardless, *Litton Indus.*, 676 F.2d at 370, should control. 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. 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, because the relief cannot be "reasonably related" to the conduct at issue without disregard for the law and prior violations. *Accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

86. Factors to consider in determining whether fencing-in relief is appropriate include: "(1) the deliberateness and seriousness of the violation, (2) the degree of transferability of the violation to other products, and (3) any history of prior violations." *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citations omitted); *see also Thompson Med. Co.*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6 at *414-415 (1984).

Reply to Proposed Conclusion of Law No. 86

Complaint Counsel's Proposed Conclusion of Law No. 86 is erroneous, irrelevant, immaterial, legally insufficient, incomplete, unjustifiably conclusory, and not supported by the facts in this proceeding. It is also repetitive of prior Proposed Conclusions and should be stricken on that basis alone.

Complaint Counsel (again) misapplies its cited authorities. *Kraft* and *Thompson* are both deception cases with actual consumer harm. This is an unfairness case with no consumer injury of any sort. Also, in *Thompson,* the Commission stated:

> To ensure that a multi-product fencing-in order such as this one 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 transferabilty of the unlawful

> practices to other (93) products. The more egregious the facts with respect to a particular element, the less important it is that another negative factor be present.

104 F.T.C. at 833. In this case, *there is no present violation.*

Litton Indus., 676 F.2d at 370, 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. 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, because the relief cannot be "reasonably related" to the conduct at issue without disregard for the law and prior violations. *Accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

> 87. "'The reasonable relationship analysis operates on a sliding scale – any one factor's importance varies depending on the extent to which the others are found. . . . All three factors need not be present for a reasonable relationship to exist.'" *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 309 (May 17, 2012) (quoting *Telebrands Corp. v. FTC*, 457 F.3d 354, 358-59 (4th Cir. 2006)).

Reply to Proposed Conclusion of Law No. 87

Complaint Counsel's Proposed Conclusion of Law No. 87 is erroneous, irrelevant, immaterial, misleading, unjustifiably conclusory, and not supported by the facts in this proceeding.

To show a "reasonable relationship," Complaint Counsel must first establish "present injury." *Thompson*, 104 F.T.C. at 833. It has not done so.

Also, *Litton Indus.*, 676 F.2d at 370, 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. 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, because the relief cannot be "reasonably related" to the conduct at issue without disregard for the law and prior violations. *Accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

Finally, there is no evidence in the record demonstrating that the proposed Notice Order will improve LabMD's medical data security or be consistent with HIPAA. Complaint Counsel bears the burden of proof, and it certainly could have asked Dr. Hill to opine with respect to these things during the years she was engaged as FTC's expert. However, it chose not to do so. Imposing the 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 II*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action"); *Credit Suisse*, 551 U.S. at 275.

88. "[I]t is the circumstances of the violation as a whole, and not merely the presence of absence of any one [] factor, that justifies a broad order." *Kraft v. FTC*, 970 F.2d 311, 327 (7th Cir. 1992) (citations omitted).

Reply to Proposed Conclusion of Law No. 88

LabMD has no specific response to Proposed Conclusion of Law No. 88, except to note that *Kraft* is distinguishable on its facts, and that, given the circumstances "as a whole" here, no

fencing-in order can be justified. *See Thompson*, 104 F.T.C. at 833; *Litton Indus.*, 676 F.2d at 370; *see also Fox Television II*, 556 U.S. at 515; *Credit Suisse*, 551 U.S. at 275.

89. "The more egregious the facts with respect to a particular element, the less important it is that another negative factor be present." *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 392 (9th Cir. 1982).

Reply to Proposed Conclusion of Law No. 89

LabMD has no specific response to Proposed Conclusion of Law No. 89, except to note that *Sears* is a deception case that is distinguishable on its facts, and that, given the circumstances "as a whole" here, no fencing-in order can be justified. *See Thompson*, 104 F.T.C. at 833; *Litton Indus.*, 676 F.2d at 370; *see also Fox Television II*, 556 U.S. at 515; *Credit Suisse*, 551 U.S. at 275. In fact, in *Sears*, the court held: "Where a fair assessment of an advertiser's conduct shows a ready willingness to flout the law, sufficient cause for concern regarding further, additional violations exists. Two factors or elements frequently influence our decision-the deliberateness and seriousness of the present violation, and the violator's past record with respect to unfair . . . practices." This holding immediately preceeded and was the context for Complaint Counsel's citation. *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 392 (9th Cir. 1982).

90. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 90

LabMD has no specific response to Proposed Conclusion of Law No. 90.

1.4.3.1 LabMD's Failure to Address its Data Security Failures Was Deliberate

91. LabMD, through its employees and contractors, had control over and made decisions regarding data security. (CX0709 (Daugherty, Dep. at 13-14) (testifying that other than the physical medical operations of LabMD, Mr. Daugherty had final authority over LabMD's operations); (CX0725-A (Martin, Dep. at 159), CX0727-A (Parr, Dep. at 105-06), CX0705-A (Bradley, Dep. at 136-37) (all stating that all IT expenditures at LabMD had to be approved by Mr. Daugherty); CX0724 (Maire, Dep. at 12) (testifying that Mr. Boyle directed the day-to-day work in the IT department at LabMD); (CX0733 (Boyle, LabMD Designee, IHT) at 60-61) (confirming that Mr. Boyle and Mr. Daugherty were the final approvers for any IT security policies); (CX0733 (Boyle, LabMD Designee, IHT) at 92-93, 104, 125-26, 147, 202, 204) (explaining that LabMD's memorialized security policies in 2010 were written by Mr. Boyle, Mr. Hyer, Mr. Daugherty, and Ms. Gilbreth and approved by Mr. Boyle and Mr. Daugherty)).

Reply to Proposed Conclusion of Law No. 91

Complaint Counsel's Proposed Conclusion of Law No. 91 is a statement of fact and should be stricken accordingly.

92. Even where LabMD had policies for data security in place, it often violated or failed to fully implement the policies. *See infra* CCCL ¶¶ 93-103.

Reply to Proposed Conclusion of Law No. 92

Complaint Counsel's Proposed Conclusion of Law No. 92 is a statement of fact and should be stricken accordingly. It is also contrary to the evidence.

93. For example, LabMD's policies as memorialized in 2010 required employees to encrypt emails containing sensitive information. However, LabMD did not provide employees with tools with which to encrypt email containing sensitive information. *See supra* CCFF § 5.2.4.3 (LabMD Did Not Enforce Its Recommendation That Employees Encrypt Emails (¶¶ 474-480)).

Reply to Proposed Conclusion of Law No. 93

Complaint Counsel's Proposed Conclusion of Law No. 93 is a statement of fact and should be stricken accordingly. It is also contrary to the evidence.

94. Another of LabMD's policies memorialized in 2010 required the identification and removal of unauthorized software; however, for as long as three years an employee with access to Personal Information had installed and used an unauthorized P2P file-sharing program. *See supra* CCFF §§ 5.2.4.1 (LabMD Did Not Enforce Its Policy to Restrict Downloads from the Internet (¶¶ 458-462), 5.2.4.2 (LabMD Did Not Enforce Its Policy To Detect and Remove Unauthorized Applications) (¶¶ 465-471)).

Reply to Proposed Conclusion of Law No. 94

Complaint Counsel's Proposed Conclusion of Law No. 94 is a statement of fact and should be stricken accordingly. It is also contrary to the evidence.

95. LabMD adopted a compliance program in January 2003 which required the company to implement policies and procedures to "monitor and insure that patient information is secure, kept private and only used for care, billing or operational uses." (CX0005 (LabMD Compliance Program effective Jan. 2003) at 4). However, LabMD did not implement any policies or procedures to satisfy these information security requirements, and did not create written policies until 2010. *See supra* CCFF § 5.2.2.1.2 (LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program) (¶¶ 434-438).

Reply to Proposed Conclusion of Law No. 95

Complaint Counsel's Proposed Conclusion of Law No. 95 is a statement of fact and should be stricken accordingly. It is also contrary to the evidence.

96. LabMD's employees and outside contractors notified LabMD that its security was inadequate, and LabMD failed to act on those warnings within a reasonable time frame. *Kraft v. FTC*, 970 F.2d 311, 327 (7th Cir. 1992) (finding a violation deliberate where the company did not act on warnings); *see infra* CCCL ¶¶ 97, 102-103. LabMD's conduct shows a pattern of carelessness and delay, and demonstrates the deliberateness of its data security failures.

Reply to Proposed Conclusion of Law No. 96

Complaint Counsel's Proposed Conclusion of Law No. 96 is a statement of fact and should be stricken accordingly It is also contrary to the evidence

Complaint Counsel misapplies the cited authority, which has no correlation to the present proceeding. *Kraft* was a deception case in which the court noted: "The deceptive claims were apparent from the face of the ad, but even if they somehow eluded Kraft, the Commission reasonably concluded that the steady stream of warnings should have put Kraft on notice that its surveys were somehow inadequate or defective. Kraft made three modifications to the ads, but two of them were implemented at the very end of the campaign, more than two years after it had begun." *Kraft v. FTC*, 970 F.2d 311, 328 (7th Cir. 1992).

This is a data security unfairness case, where there is no allegation that the respondent violated the applicable regulatory standards. In a case without a documented post-July 2010 violation, a data breach, or any evidence of any consumer injury or competitive impact, FTC applies "standards" compiled for the first time in a litigation expert report years after the fact to declare unfairness. Instead, *Wyndham* is the relevant precedent here with respect to warning. *Wyndham*, 2015 U.S. App. LEXIS 14839 at *15-17, *54-55; *accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

97. LabMD had notice of a security breach relating to P2P file sharing as early as May 2008. *See supra* CCFF § 8.1.3 (1718 File Found on Peer-to-Peer Network) (¶ 1395).

Reply to Proposed Conclusion of Law No. 97

Complaint Counsel's Proposed Conclusion of Law No. 97 is a statement of fact and should be stricken accordingly. It is also erroneous, incomplete, intentionally misleading, unjustifiably conclusory, and not supported by the facts in this proceeding. The term "security breach" has no legal effect or definition, not under HIPAA or under any of the "standards" FTC purports to apply in this case.

98. LabMD had a policy prohibiting employees from using the Internet for non-work purposes; this would include downloading software and the use of peer-to-peer file-sharing. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 7;

CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 7; CX0714-A ([Fmr. LabMD Empl.], Dep. at 38); CX0730 (Simmons, Dep. at 16-17, 93); RX0481 (LabMD Electronics Policy (2004) (prohibits personal Internet use).

Reply to Proposed Conclusion of Law No. 98

Complaint Counsel's Proposed Conclusion of Law No. 98 is a statement of fact and should be stricken accordingly.

99. However, even after May 2008, LabMD did not provide non-IT employees with any training regarding security mechanisms or the consequences of reconfiguring security settings in applications. *See supra* CCFF § 5.5.2 (LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information) *et seq.* (¶¶ 866-891).

Reply to Proposed Conclusion of Law No. 99

Complaint Counsel's Proposed Conclusion of Law No. 99 is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, incomplete, intentionally misleading, and not supported by the facts in this proceeding. Complaint Counsel offers no evidence LabMD's training practices were unfair under Section 5(a) or unlawful under Section 5(n); violated HIPAA; or that LabMD was on notice FTC expected something different than HIPAA compliance under Section 5. Consequently, this conclusion of law establishes that Complaint Counsel has not carried its burden of proof and that FTC's action against LabMD violates due process for lack of fair notice and is precluded by HIPAA. *Fox Television*, 132 S. Ct. at 2317 ("[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Credit Suisse*, 551 U.S. at 275.

100. Furthermore, many LabMD employees were given administrative rights over their workstations, which allows a user to download software, such as peer-to-peer file-sharing software. *See supra* CCFF § 5.8.1 (LabMD Employees Were Given Administrative Access to Workstation Computers) (¶¶ 1056-1063).

Reply to Proposed Conclusion of Law No. 100

Complaint Counsel's Proposed Conclusion of Law No. 100 is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, incomplete, intentionally misleading, and not supported by the facts in this proceeding. Complaint Counsel offers no evidence LabMD's adminstrative rights practices were unfair under Section 5(a) or unlawful under Section 5(n); violated HIPAA; or that LabMD was on notice FTC expected something different from HIPAA compliance under Section 5. Consequently, this conclusion of law establishes that Complaint Counsel has not carried its burden of proof and that FTC's action against LabMD violates due process for lack of fair notice and is precluded by HIPAA. *Fox Television*, 132 S. Ct. at 2317 ("[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Credit Suisse*, 551 U.S. at 275.

101. LabMD's manual computer inspections were not proactively deployed to search out unauthorized uses of LabMD's network, but were used only in response to employee issues with their workstations. *See supra* CCFF § 5.3.2.3 (LabMD's Manual Inspections Could Not Reliably Detect Security Risks) *et seq.* (¶¶ 660-696). Furthermore, manual inspections are not an adequate substitute for automated mechanisms. *See supra* CCFF § 5.3.2.3 (LabMD's Manual Inspections Could Not Reliably Detect Security Risks) (¶¶ 660-665).

Reply to Proposed Conclusion of Law No. 101

Complaint Counsel's Proposed Conclusion of Law No. 101 is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, incomplete, intentionally misleading, and not supported by the facts in this proceeding. Complaint Counsel offers no evidence LabMD's inspection practices were unfair under Section 5(a) or unlawful under Section 5(n); violated HIPAA; or that LabMD was on notice FTC expected something different from HIPAA compliance under Section 5. Consequently, this conclusion of law establishes that Complaint Counsel has not carried its burden of proof and that FTC's action against LabMD

violates due process for lack of fair notice and is precluded by HIPAA. *Fox Television*, 132 S. Ct. at 2317 ("[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Credit Suisse*, 551 U.S. at 275.

102. When a third party identified security issues on LabMD's servers and provided solutions, LabMD failed to remediate the problems over several months. (*Supra* CCFF §§ 5.3.4.3.1.1 (The Mapper Server Had an Anonymous FTP Vulnerability that Could Allow Export of All Data on the Server) (¶¶ 759-771)(vulnerability identified in May 2010 scan still present in July 2010); 5.3.4.3.1.3 (The Mapper Server Had a Vulnerability that Could Be Exploited To Access Any Files Available On Mapper) (¶¶ 781-788) (vulnerability identified in May 2010 scan still present in July 2010); 5.3.4.3.1.4 (The Mapper Server Had a Vulnerability that Could Be Exploited To Steal FTP Usernames and Passwords) (¶¶ 792-797) (vulnerability identified in May 2010 scan still present in September 2010)).

Reply to Proposed Conclusion of Law No. 102

Complaint Counsel's Proposed Conclusion of Law No. 102 is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, incomplete, intentionally misleading, and not supported by the facts in this proceeding. Complaint Counsel offers no evidence LabMD's "remediation practices" over "several months" were unfair under Section 5(a) or unlawful under Section 5(n); violated HIPAA; or that LabMD was on notice FTC expected something different from HIPAA compliance under Section 5. Consequently, this conclusion of law establishes Complaint Counsel has not carried its burden of proof and that FTC's action against LabMD violates due process for lack of fair notice and is precluded by HIPAA. *Fox Television*, 132 S. Ct. at 2317 ("[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Credit Suisse*, 551 U.S. at 275.

103. LabMD also failed to update its antivirus software for several months even after it was informed that the software was no longer supported. *Supra* CCFF § 5.3.2.1.1.1 (LabMD Did Not Consistently Update Symantec Virus Definitions on Servers) (¶¶ 547-550).

Reply to Proposed Conclusion of Law No. 103

Complaint Counsel's Proposed Conclusion of Law No. 103 is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, incomplete, intentionally misleading, and not supported by the facts in this proceeding. Complaint Counsel offers no evidence LabMD's training practices were unfair under Section 5(a) or unlawful under Section 5(n); violated HIPAA; or that LabMD was on notice FTC expected something different than HIPAA compliance under Section 5. Consequently, this conclusion of law establishes that Complaint Counsel has not carried its burden of proof and that FTC's action against LabMD violates due process for lack of fair notice and is precluded by HIPAA. *Fox Television*, 132 S. Ct. at 2317 ("[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Credit Suisse*, 551 U.S. at 275.

104. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 104

LabMD has no specific response to Proposed Conclusion of Law No. 104

1.4.3.2 LabMD's Data Security Failures Were Serious.

105. LabMD's data security failures were serious: LabMD failed to provide reasonable security for Personal Information within its computer network. (CX0740 (Hill Report) ¶ 49)); *see also supra* CCFF § 5 (LabMD Failed to Provide Reasonable Security for Personal Information on its Computer Network) *et seq.* (¶¶ 382-1110).

Reply to Proposed Conclusion of Law No. 105:

This conclusion of law is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, incomplete, intentionally misleading, and not supported by the facts in this proceeding.

Complaint Counsel has not proven that LabMD failed to comply with HIPAA, was on notice FTC expected something different than HIPAA compliance under Section 5, or that a HIPAA-compliant medical lab could have "serious" data security failures. Consequently, this

conclusion of law establishes that FTC's action against LabMD violates due process for lack of fair notice and is precluded. *Fox Television*, 132 S. Ct. at 2317 ("[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Credit Suisse*, 551 U.S. at 275.

Notwithstanding Complaint Counsel's reliance on the deficient expert testimony of Dr. Raquel Hill, *see* RPFF ¶¶ 86-89; RCOL ¶¶ 172-175, LabMD's practices and polices do evidence reasonable patient data security. *See, e.g.*, RPFF ¶¶ 92-216. Furthermore, in this case there was never a data breach or a single consumer injured, substantial or otherwise. Accordingly, the "data security failures" cannot be "serious" as a matter of law. *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

106. The seriousness of the violations in this case are illustrated by the types of Personal Information LabMD holds, *supra* CCFF § 9.2.1 (LabMD Stores the Types of Information Used to Commit Identity Frauds) (¶¶ 1642-1643), and the harm likely to be caused to consumers, including identity theft, medical identity theft, and other harms, by breach of this Personal Information. *Supra* CCFF § 9.2 (LabMD's Security Failures Placed All Consumers Whose Personal Information is on Their Network at Risk) *et seq.* (¶¶ 1642-1658).

Reply to Proposed Conclusion of Law No. 106:

This conclusion of law is a statement of fact and should be stricken accordingly. It is also erroneous, irrelevant, incomplete, intentionally misleading, and not supported by the facts in this proceeding.

First, the "violations" referenced presumably relate to Section 5. Complaint Counsel offers no evidence that LabMD was on notice FTC expected something different than HIPAA compliance under Section 5. Consequently, this Conclusion of Law establishes that FTC's action against LabMD violates due process for lack of fair notice and is precluded by HIPAA. *Fox Television*, 132 S. Ct. at 2317 ("[T]he due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"); *Credit Suisse*, 551 U.S. at 275.

Second, there is no evidence from Dr. Hill or anyone else that harm is "likely" to be caused now or in the future by the data security "failures" between January 2005 and July 2010, or that there are any data security "failures" in violation of Section 5 *after* July 2010. Consequently, the claim that harm is "likely" must be rejected as bogus. *Compare Wyndham*, 2015 U.S. App. LEXIS 14839, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

Third, no authority holds that in the absence of actual or certainly impending substantial consumer injury a "violation" of Section 5 possibly can be "serious."

107. The seriousness of the violations are also illustrated by the duration of LabMD's data security failures. *See Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (finding a violation serious due to, inter alia, its two and one-half year duration); *see, e.g.*, *supra* CCCL § 1.4.2.1 (An Injunction is an Appropriate Remedy) (¶¶ 73-78).

Reply to Proposed Conclusion of Law No. 107:

This conclusion of law is incorrect, misleading and unsupported by the record.

Complaint Counsel is intentionally obtuse. It has never specified when each of the alleged "data security failures" supposedly occurred. However, Dr. Hill testified that her report was limited to the time between January 2005 and July 2010, and FTC has testified this is the entirety of its case against Respondent. (RX 525 (Kaufman, Dep. at 67 (relying solely on Dr. Hill)). Therefore, LabMD has not even been alleged to have violated Section 5 for over five years. Complaint Counsel cites no case or Commission holding that long-passed "violations" of Section 5, whether involving data security or anything else, which caused neither actual nor certainly impending consumer injury (substantial or otherwise), can be "serious"as a matter of law. It cites none because such would be an absurd and unlawful holding. *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

108. The inability of consumers to protect themselves from the risks LabMD's failures posed to their Personal Information is another indicium of seriousness. *See Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 312 (May 17, 2012) (finding violation serious where consumers did not have to ability to evaluate health claims made in advertisement); *Thompson Med. Co*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6 at *414-17 (finding violation serious where consumers could not readily judge the truth or falsity of the claims at issue); *supra* § 9.5.1 (The Consumer Is Not in a Position to Know of a Company's Security Practices) *et seq.* (¶¶ 1773-1795).

Reply to Proposed Conclusion of Law No. 108:

LabMD has no specific response to Proposed Conclusion of Law No. 108 except to note that Complaint Counsel has failed to prove the patients potentially affected by the speculative, inchoate harms alleged in this case 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*, 691 F.3d at 1168-69. *Davis* framed the issue as "not whether subsequent mitigation was convenient or costless, but whether it was reasonably possible." *Id.*; *see also 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."). Complaint Counsel has never explained how or why the HIPAA Breach Notification Rule fails to operate. Furthermore, no authority holds that in the absence of actual or certainly impending substantial consumer injury a "violation" of Section 5 possibly can be "serious."

109. The seriousness of the violations in this case are illustrated by the breaches of the 1718 File and the Day Sheets. *Supra* CCFF § 8 (Security Incidents at LabMD) *et seq.* (¶¶ 1354-1469).

Reply to Proposed Conclusion of Law No. 109:

This conclusion of law is erroneous, misleading and unsupported by the record.

No authority holds that in the absence of actual or certainly impending substantial consumer injury a "violation" of Section 5 possibly can be "serious." Tiversa's theft of the 1718 File occurred in February 2008. FTC has not offered one consumer victim. FTC has proven nothing about the Day Sheets. But, notwithstanding the fact that the FBI investigated the matter, not a single consumer victim has been identified. Furthermore, Complaint Counsel has failed to prove by a preponderance of the evidence the allegation in ¶ 21 of the Complaint, *viz.*, that "[a] number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identify thieves." These Day Sheets were found in paper form, (CX 0720 (Jestes, Dep. at 58)), and were never

stored electronically. (CX 0714-A ([LabMD Billing Employee], Dep. at 65-66); (RX 497 (Gilbreth, Dep. at 42-44)). Complaint Counsel has proven nothing about the Day Sheets, other than they were "found" in California. (Hill, Tr. 220-21; CX 0720 (Jestes Dep. at 46)).

Complaint Counsel has failed to produce a scintilla of evidence demonstrating consumer injury as defined by Section 5(n). None of the government's experts has testified that the "violations" that allegedly occurred between January 2005 and July 2010 now cause or in the future are likely to cause substantial consumer injury. There is no "serious" violation here as a matter of law. *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

110. Complaint Counsel alleged a number of data security failures in its Complaint. (Compl. ¶ 10). Even if LabMD is not found to have maintained unfairly unreasonable security as to each of the items, its failures are still serious and warrant fencing-in relief. *Cf. Bristol-Myers Co.*, 102 F.T.C. 21, 1983 FTC LEXIS 64 at *377-80 (1983); *Fedders Corp.*, 85 F.T.C. 38, 1975 FTC LEXIS 282, at *71-72 (1975) (both finding fencing-in relief appropriate even where only a small number of products or advertisements were found to violate Section 5).

Reply to Proposed Conclusion of Law No. 110:

This conclusion of law is erroneous, misleading and contrary to the record.

Complaint Counsel misapplies the cited authorities. *Fedders* was a deceptive advertising case in which the respondent argued that it was entitled to relief from an order on the grounds that so few of its ads were deceptive as to be insubstantial. Based on 173 false ads in a two year period, the Commission rejected Fedders' argument. *See* 85 FTC at 37-38. *Bristol-Myers* was a drug false advertising/claims case, one having nothing to do with the facts here and not standing for the proposition cited. *See* 102 FTC at 21. In neither of these cases did

FTC allege that a list of specific acts, "taken together," were the gravamen of a Section 5 violation, as it does here.

Complaint Counsel did not allege, and Dr. Hill did not testify, that any of LabMD's supposed "violations," standing alone, were unreasonable or that they caused, or are likely to cause, substantial consumer injury. Instead, this case was the whole. Therefore, as a matter of law, if Complaint Counsel fails to prove every one of its claims, it cannot by its own standard, satisfy Section 5(n).

Finally, Complaint Counsel has failed to produce a scintilla of evidence demonstrating consumer injury as defined by Section 5(n). None of the government's experts has testified that the "violations" that allegedly occurred between January 2005 and July 2010 now cause or in the future are likely to cause substantial consumer injury. No authority holds that in the absence of actual or certainly impending substantial consumer injury a "violation" of Section 5 possibly can be "serious." There is no "serious" violation here as a matter of law. *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

111. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 111:

LabMD has no specific response to Proposed Conclusion of Law No. 111.

1.4.3.2 LabMD's Data Security Failures Are Transferable

112. "The prevention of 'transfers' of unfair trade practices is a fundamental goal of the Commission's remedial work." *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 394 (9th Cir. 1982).

Reply to Proposed Conclusion of Law No. 112:

LabMD has no specific response to Proposed Conclusion of Law No. 112.

113. LabMD's data security failures continue to place the Personal Information of all 750,000 consumers in its possession at risk, not just those included in the 1718 File and Day Sheets. Further, if LabMD resumes collecting the Personal Information of additional consumers, its failures place those consumers at risk as well. Because LabMD retains the Personal Information of 750,000 consumers, has not dissolved as a Georgia corporation, and does not intend to dissolve or to safely dispose of consumers' Personal Information, the dangers posed by LabMD's conduct are transferable to any future forms of operation the company might take. *See FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 215 (D. Mass. 2009) (imposing fencing-in injunction "[e]ven though the [] defendants currently have no employees and are not engaged in any business, they could resume such activities in the future"); *U.S. v. Bldg. Insp. of Am.*, 894 F. Supp. 507, 521 (D. Mass. 1995) (finding injunction appropriate where company had ceased operation but "remains a going concern and could resume at any time"); *cf. Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *92 (1984) ("[A]n obligation should ordinarily extend as long as the risk of harm exists.").

Reply to Proposed Conclusion of Law No. 113:

This conclusion of law is a statement of fact and should be stricken accordingly. It is also erroneous, false, and unsupported by the record.

To begin with, none of Complaint Counsel's experts have testified that the information of LabMD's patients is now "at risk" (whatever the legal meaning of that term) or that it could be in the future. No witness has testified that LabMD's data security practices after July, 2010, fail Section 5. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law. *Compare Wyndham*, 2015 U.S. App. LEXIS 14839, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury). Therefore, there is no grounds for a "transferability" finding.

114. There are no steps that consumers can take themselves to protect their Personal Information that LabMD currently holds and prevent future harm. *Supra* CCFF

§ 9.2.2 (LabMD's Failure to Secure the Personal Information it Stores Places Consumers at Greater Risk of Identity Theft) (¶¶ 1653-1658). Consumers did not know, in most cases, that their Personal Information was sent to LabMD nor its security practices, *supra* CCFF § 9.5.1 (The Consumer Is Not in a Position to Know of a Company's Security Practices) *et seq.* (¶¶ 1773-7797), CCCL § 1.3.2 (Consumers Cannot Reasonably Avoid the Substantial Injury Caused or Likely to Be Caused by LabMD's Data Security Failures) (¶¶ 42-44), and even if they did have such knowledge identity theft cannot be fully remediated after notice, *supra* CCFF § 9.4.2.5.1. (Consumers Cannot Avoid All Harms Through Notification of Unauthorized Disclosures of Information) (¶¶ 1769-1770).

Reply to Proposed Conclusion of Law No. 114:

Complaint Counsel's Conclusion of Law No. 114 is a statement of fact and should be stricken accordingly. It is also erroneous and misleading. The law is that "an injury is reasonably avoidable if consumers "have reason to anticipate the impending harm and the means to avoid it," or if consumers are aware of, and are reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact." *Davis*, 691 F.3d at 1168-69 (citations omitted). As a result of the HIPPA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, patients have the means needed to mitigate. Therefore, any injury due to a breach by LabMD is "reasonably avoidable." *See Davis*, 691 F.3d at 1169.

LabMD incorporates by reference its responses to Proposed Conclusions of Law 42-44.

115. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 115:

LabMD has no specific response to Proposed Conclusion of Law No. 115.

1.4.3.3 The History of LabMD's Data Security Failures Warrants Fencing-In Relief

116. There is no evidence of prior violations of the FTC Act by LabMD. Where the first two factors sufficiently establish a reasonable relationship between the remedy and the violation, this factor is not necessary to the appropriateness of fencing-in relief in an order. *Telebrands Corp. v. FTC*, 457 F.3d 354, 362 (4th Cir. 2006); *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 314 (May 17, 2012).

Reply to Proposed Conclusion of Law No. 116:

Complaint Counsel's Proposed Conclusion of Law No. 116 is erroneous.

There is indeed no evidence of prior Section 5 violations by LabMD. *Litton Indus.*, 676 F.2d at 370, therefore, 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. 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 because the relief cannot be "reasonably related" to the conduct at issue without disregard for the law and prior violations. *Accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

Critically, there is no evidence in the record demonstrating that the proposed Notice Order will improve LabMD's medical data security or be consistent with HIPAA. Complaint Counsel bears the burden of proof, and it certainly could have asked Dr. Hill these things. However, it chose not to do so. Imposing the 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 II*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action"); *Credit Suisse*, 551 U.S. at 275.

LabMD incorporates by reference its responses to Complaint Counsel's Proposed Conclusions of Law Nos. 80-90, as appropriate.

117. However, LabMD's conduct occurred over a long period of time, which indicates both seriousness and continuous violations. LabMD's data security failures persisted from at least 2005 through at least the close of evidence in the hearing. *See, e.g., supra* CCFF §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) *et seq.* (¶¶ 415-443); 5.3.4 (LabMD Did Not Use Penetration Testing Before 2010) (¶¶ 715-726); 5.4.2.1 (LabMD Had No Policy for Deleting Personal Information and Maintained the Information Indefinitely) (¶¶ 835-841) (LabMD has retained all the Personal Information it has ever collected); 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) *et seq.* (¶¶ 852-900) (LabMD did not provide employees any training on data security); 5.6.2.2 (LabMD Did Not Prevent Employees from Using the Same Password for Years) (¶¶ 954-957) (employee used insecure login credentials from 2006 through 2013); 5.7.1 (Some LabMD Servers Used a Windows Operating System Years After Microsoft Had Stopped Updating and Supporting It) (¶¶ 1003-1008).

Reply to Proposed Conclusion of Law No. 117:

Complaint Counsel's Proposed Conclusion of Law No. 117 is a statement of fact and should be stricken accordingly. It is also erroneous, intentionally misleading, and false.

Complaint Counsel failed to offer any testimony that LabMD's post-July 2010 data security practices were unreasonable. No one has testified that its existing data security practices cause or are likely to cause substantial injury to consumers. No one has testified that its pre-July 2010 data security practices are likely to cause substantial injury to consumers in the future.

No witness has testified that LabMD's data security practices after July 2010 fail Section 5. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law. *Compare Wyndham*, 2015 U.S. App. LEXIS 14839, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In*

re Sci. Applications Int'l Corp., 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

118. LabMD's data security failures were diverse, and covered a wide spectrum of data security practices, including failure to develop, implement, and maintain a comprehensive information security program, *supra* CCFF § 5.2 (LabMD Did Not Develop and Maintain a Comprehensive Written Information Security Program) *et seq.* (¶¶ 397-480); failure to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network, *supra* CCFF 5.3 (LabMD Did Not Use Reasonable, Readily Available Measures to Identify Commonly Known or Reasonably Foreseeable Security Risks and Vulnerabilities) *et seq.* (¶¶ 483-808); failure to use adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs, *supra* CCFF § 5.4 (LabMD Did Not use Adequate Measures to Prevent Employees From Accessing Personal Information Not Needed to Do Their Jobs) *et seq.* (¶¶ 811-849); failure to train employees to safeguard Personal Information, *supra* 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) (*et seq.* (¶¶ 852-900); failure to require employees or other users with remote access to the networks to use authentication-related security measures, *supra* CCFF § 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq.* (¶¶ 903-993); failure to maintain and update operating systems of computers and other devices on its network, *supra* CCFF § 5.7 (LabMD Did Not Maintain and Update Operating Systems and Other Devices) *et seq.* (¶¶ 996-1043); and failure to use readily available measures to prevent or detect unauthorized access to Personal Information on its computer networks, *supra* CCFF § 5.8 (LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information) *et seq.* (¶¶ 1045-1110).

Reply to Proposed Conclusion of Law No. 118:

Complaint Counsel's Proposed Conclusion of Law No. 118 is a statement of fact and should be stricken accordingly. It is also erroneous, intentionally misleading, and false.

Complaint Counsel failed to offer any testimony that LabMD's post-July 2010 data security practices were unreasonable. No one has testified that its existing data security practices cause or are likely to cause substantial injury to consumers. No one has testified that its pre-July 2010 data security practices are likely to cause substantial injury to consumers in the future.

No witness has testified that LabMD's data security practices after July 2010 fail Section 5. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law. *Compare FTC v. Wyndham*, 2015 U.S. App. LEXIS 14839, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

119. These facts demonstrate a history of violations of the unfairness provision of the FTC Act.

Reply to Proposed Conclusion of Law No. 119:

Complaint Counsel's Proposed Conclusion of Law No. 119 is erroneous.

To prove a Section 5 violation, first, Complaint Counsel must prove by a preponderance of the evidence that the data security acts and practices identified in the Complaint were "unfair" under Section 5(a) – that is, marked by injustice, partiality, or deception. *See* 15 U.S.C. § 45(a); *Yates*, 135 S. Ct. at 1081-83, 1091; *Carr*, 560 U.S. at 448; *Meyer*, 510 U.S. at 477; *Wyndham*, 2015 U.S. App. LEXIS at 14839, *15-17, *54-55; Merriam-Webster's Dictionary, "Unfair" http://www.merriam-webster.com/dictionary/unfair (last visited Sept. 3, 2015). There is no evidence that any of LabMD's data security practices were "unfair" under Section 5.

Second, Complaint Counsel must satisfy all of the Section 5(n) factors to declare unlawfulness. On the evidence, it cannot do this.

Third, Complaint Counsel must prove LabMD had fair notice of ascertainably certain standards that were not in conflict with HIPAA. *Wyndham*, 2015 U.S. App. LEXIS 14839. It cannot do this either.

120. The lack of prior adjudicated violations of the FTC Act is not a bar to entry of fencing-in provisions. *Kraft v. FTC*, 970 F.2d 311, 327 (7th Cir. 1992) (concluding claim that fencing-in provision was inappropriate because of a lack of prior violations "without merit").

Reply to Proposed Conclusion of Law No. 120:

Complaint Counsel's Proposed Conclusion of Law No. 120 is erroneous.

There is indeed no evidence of prior Section 5 violations by LabMD. Thus, *Litton Indus.*, 676 F.2d at 370, 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. 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, because the relief cannot be "reasonably related" to the conduct at issue without disregard for the law and prior violations. *Accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70. Critically, there is no evidence in the record demonstrating that the proposed order will improve LabMD's medical data security or be consistent with HIPAA. Complaint Counsel bears the burden of proof, and it certainly could have asked Dr. Hill these things. However, it chose not to do so.

LabMD incorporates by reference its responses to Complaint Counsel's Proposed Conclusions of Law Nos. 80-90, as appropriate.

121. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 121:

LabMD has no specific response to Proposed Conclusion of Law No. 121.

1.4.4 The Notice Order's Provisions are Appropriate

1.4.4.1 The Twenty Year Duration of the Order is Appropriate

122. A twenty year order duration is consistent with the Commission's prior orders. *See, e.g.*, *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012); *Daniel Chapter One*, Docket No. 9329, 2010 FTC LEXIS 11, at *9-10.

Reply to Proposed Conclusion of Law No. 122:

Complaint Counsel's Proposed Conclusion of Law No. 122 is irrelevant.

The appropriateness of equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. Consent Orders are not competent legal authority here. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement."); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312; 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed twenty year order duration is consistent with the Commission's prior orders is irrelevant.

123. A twenty year order duration is appropriate given the length of time over which LabMD's unreasonable data security practices extended. *Supra* CCCL ¶ 117;

> *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012) (finding 20 year order duration appropriate where advertisements were disseminated over a course of at least 6 years).

Reply to Proposed Conclusion of Law No. 123:

Complaint Counsel's Proposed Conclusion of Law No. 123 is erroneous.

Complaint Counsel did not offer evidence, much less prove, that LabMD's allegedly "unreasonable" data security practices extended beyond July, 2010. There is no evidence of prior Section 5 violations by LabMD at all. *Litton Indus.*, 676 F.2d at 370, therefore, 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. 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, because the relief cannot be "reasonably related" to the conduct at issue without disregard for the law and prior violations. *Accord Int'l Harvester Co.*, 104 F.T.C. at 1069-70. Critically, there is no evidence in the record demonstrating that the proposed order will improve LabMD's medical data security or be consistent with HIPAA.

Absent a satisfactory demonstration of the past "egregiousness of [LabMD's] action, the isolated or recurrent nature of the [alleged] infraction[s] involved, . . . and the likelihood that [LabMD's present acts and practices] will present opportunities for future violations," the need

for injunctive relief cannot arise. *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 1013, 1017 (N.D. Ind. 2000). Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law. *Compare Wyndham*, 2015 U.S. App. LEXIS 14839, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury). There is nothing in the record to suggest that a twenty year duration is appropriate; instead, it is unlawfully punitive. *See Heater*, 503 F.2d at 322-27; *Litton Indus.*, 676 F.2d at 370.

LabMD incorporates by reference its responses to Complaint Counsel's Proposed Conclusions of Law Nos. 80-90, as appropriate.

124. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 124:

LabMD has no specific response to Proposed Conclusion of Law No. 124.

1.4.4.2 Part I: Comprehensive Information Security Program

125. Part I of the Notice Order requires LabMD to establish, implement, and maintain a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of Personal Information collected from or about consumers. The program must be in writing, and should contain administrative, technical, and physical safeguards appropriate to LabMD's size and complexity, the nature and scope of its activities, and the sensitivity of the Personal Information collected from or about consumers. The safeguards must include (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; (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 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 Conclusion of Law No. 125:

Complaint Counsel's Proposed Conclusion of Law No. 125 is a statement of fact and should be stricken accordingly.

Also, the Notice Order is not authorized by 15 U.S.C. § 45(b), which provides:

> Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint. The person, partnership, or corporation so complained of shall have the right to appear at the place and time so fixed and show cause why an order should not be entered by the Commission requiring such person, partnership, or corporation to cease and desist from the violation of the law so charged in said complaint.

Therefore, the Notice Order is *ultra vires* and demonstrates that the Commission has prejudged this matter.

126. Part I's requirement for the establishment, implementation, and maintenance of a comprehensive information security program is reasonably related to, and highly correlated with, the allegations of the Complaint, which alleges in Paragraph 10(a) that LabMD "did not develop, implement, or maintain a comprehensive information security program to protect consumers' Personal Information." Compl. ¶ 10(a).

Reply to Proposed Conclusion of Law No. 126:

This conclusion of law is false and unsupported by the record.

First, the Notice Order is *ultra vires* and unlawful. 15 U.S.C. § 45(b).

Second, Complaint Counsel has failed to establish by a preponderance of the evidence that LabMD's past or current data security practices did or were likely to cause substantial injury during the Relevant Period, let alone whether such practices are likely to reoccur and then to cause substantial consumer injury, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition, in the future. *See* 15 U.S.C. § 45(n).

Third, Complaint Counsel has failed to prove by a preponderance of the evidence that LabMD was not compliant with all applicable HIPAA/HITECH regulations and standards, or that LabMD's compliance with such HIPAA/HITECH regulations and standards was unreasonable and caused or was likely to cause substantial harm to consumers. *See Diebold*, 585 F.2d at 1336; *compare Daniel Chapter One*, 2009 FTC LEXIS 157 at *281-82, *with POM Wonderful*, 2012 FTC LEXIS 18. Because Complaint Counsel has failed to demonstrate an underlying violation of the FTC Act, the proposed requirement for the establishment, implementation, and maintenance of a comprehensive information security program cannot be reasonable related to the allegations against LabMD. *See* Compl. ¶ 10(a).

Fourth, Part I of the Notice Order is a prohibited "obey-the-law" provision. *See* LabMD's Reply to Complaint Counsel's Proposed Conclusion of Law No. 57. If FTC gave LabMD notice during the Relevant Period that Section 5 required the sort of data security acts and practices contemplated by a "comprehensive information security program," as Complaint Counsel has argued it has, then the proposed order is invalid. *Goble*, 682 F.3d at 949. 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. *Fabi Constr. Co.*, 508 F.3d at 1088.

127. Part I of the Notice Order is consistent with the provisions in the Commission's Safeguards Rule of the Gramm-Leach Bliley Act. 16 C.F.R. § 314.4.

Reply to Proposed Conclusion of Law No. 127:

Complaint Counsel's Proposed Conclusion of Law No. 127 is irrelevant. The Commission's Safeguards Rule, 16 C.F.R. § 314.4, does not purport to apply to HIPAA-covered entites and LabMD is not a financial institution under the regulatory jurisdiction of the Commission. Also, the Notice Order is *ultra vires* and unlawful. 15 U.S.C. § 45(b).

128. Part I of the Notice Order is also consistent with relief approved in Commission settlements relating to unfair data security practices. *See, e.g.*, CCCL ¶¶ 17, 18; *see also U.S. v. Consumer Portfolio Servs., Inc.*, Case No. 8:14-cv-00819-ABC-RNB, at 6-7, Section IV (Stipulated Order for Perm. Injunct.) (C.D. Cal. June 11, 2014), available at http://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc (requiring debt collector to implement a comprehensive data integrity program with elements similar to a comprehensive data security program).

Reply to Proposed Conclusion of Law No. 128:

Complaint Counsel's Proposed Conclusion of Law No. 128 is irrelevant.

First, the Notice Order is *ultra vires* and unlawful, 15 U.S.C. § 45(b); *Ass'n of Am. R.R.s*, 135 S. Ct. 1225.

Second, the appropriateness of equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371.

Consent Orders are not competent legal authority here. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement"); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312; 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed twenty year order duration is consistent with the Commission's prior orders is irrelevant. *Accord Borg-Warner Corp.*, 746 F.2d at 110; *see Litton Indus.*, 676 F.2d at 371.

Third, the example offered by Complaint Counsel is inapposite as it concerns deceptive loan servicing and violations of the Fair Debt Collection Practices Act and the Fair Credit Report Act's Furnisher Rule – deceptive acts that resulted in actual consumer harm, including the unjust enrichment of the respondent. *See* Compl., *United States v. Consumer Portfolio Servs., Inc.*, No. 14-00819 (C.D. Cal. May 28, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140529cpscmpt.pdf; *see also* Press Release, "Auto Lender will Pay $5.5 Million to Settle FTC Charges It Harassed Consumers, Collected Amounts They Did Not Owe," (May 29, 2014) ("A national subprime auto lender will pay more than $5.5 million to settle Federal Trade Commission charges that the company used illegal tactics to service and collect consumers' loans, including collecting money consumers did not owe, harassing consumers and third parties, and disclosing debts to friends, family, and employers."), *available at* https://www.ftc.gov/news-events/press-releases/2014/05/auto-lender-will-pay-55-million-settle-ftc-charges-it-harassed.

129. The Commission has provided a large amount of guidance to businesses for complying with the Safeguards Rule and on general data security practices. *See, e.g.*, Financial Institutions and Customer Information: Complying with the Safeguards Rule, *available at* http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule; Protecting Personal Information: A Guide for Business, *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business; *see generally* FTC Bureau of Consumer Protection Business Center:

Data Security, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

Reply to Proposed Conclusion of Law No. 129:

Complaint Counsel's Proposed Conclusion of Law No. 129 is erroneous, irrelevant, and misleading.

FTC must provide *ex ante* "ascertainable certainty" of the standards that it will apply to declare conduct permitted or prohibited under Section 5. *Fox Television*, 132 S. Ct. at 2317 ("Just as in the First Amendment context, the due process protection against vague regulations 'does not leave [regulated parties] . . . at the mercy of *noblesse oblige*.'"). "Public statements" and "educational materials" are not constitutionally adequate standards. *See Am. Bus. Ass'n.*, 627 F.2d at 529; *Wilderness Soc'y*, 434 F.3d at 595-96. Complaints and consent decrees are not sufficient either. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement."); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312; 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, 1305-06 (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.").

Also, 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*, 236 F.3d at 754; *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. 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." *Ensign-Bickford Co.*, 717 F.2d at 1422; *Morales*, 527 U.S. at 63-64.

The testimony of Daniel Kaufman, taken after the MTD Order was issued, demonstrates the Commission's failure to provide fair notice. (RX 532 (Kaufman, Dep. at 163-220)). The consent decrees, public statements, education materials, industry guidance pieces, and Congressional testimony that the Commission relies upon in this case, (RX 532 (Kaufman, Dep. at 163-220)), are all legally insufficient. *See Altria Grp.*, 555 U.S. at 89 n.13; *Am. Bus. Ass'n.*, 627 F.2d at 529; *Wilderness Soc'y*, 434 F.3d at 595-96.

Indeed, Kaufman's testimony fails to establish *any* of the standards Complaint Counsel would have one believe existed, but it does establish that the Commission has violated the Administrative Procedure Act by attempting to enforce statements of general policy and interpretations of general applicability without actual and timely notice. *See* 5 U.S.C. § 552(a). Fair notice also requires an objective, medical industry-specific "reasonableness" standard of care, and not something like Dr. Hill's unreliable general "IT industry" standard. *See S&H Riggers*, 659 F.2d 1273, 1280-81 (5th Cir. 1981); *Fla. Mach. & Foundry*, 693 F.2d at 120.

130. Other sources, such as NIST, SANS, and US CERT, have also provided guidance for implementing a comprehensive information security program.

(*Supra* CCFF § 6.2 (Comprehensive Information Security Program) (¶¶ 1121-1124)).

Reply to Proposed Conclusion of Law No. 130:

Complaint Counsel's Proposed Conclusion of Law No. 130 is irrelevant, erroneous, and misleading.

The Commission's reference to or attempted incorporation of guidance on comprehensive information security programs from non-Commission sources is insufficient to establish legally-enforceable standards and, in any case, does not obviate the requirement that the Commission publish applicable standards in the Federal Register. *See* 5 U.S.C. § 552(a)(1)(D); *Util. Solid Waste*, 236 F.3d at 754.

Also, due process mandates an objective, medical industry-specific "reasonableness" standard of care and not a general "IT industry" standard. *See S&H Riggers*, 659 F.2d at 1280-81, 85; *Fla. Mach. & Foundry*, 693 F.2d at 120. This proposed conclusion of law does not account for contradictions between NIST and SANS, on the one hand, and HIPAA, on the other hand. CX 0405, HHS' Security Series 6 entitled "Basics of Risk Analysis and Risk Management," states:

> The Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to '[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.' . . . Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, "Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations."

(CX 0405 (HIPAA Security Series 6, at 1-2)). Hill never accounted for this language. (Hill, Tr. 235-36).

HIPAA is based on risk assessment and scalability, which FTC failed to properly consider. See 42 U.S.C. § 1320d-2(d)(1)(A)(v); 45 C.F.R. §§ 164.302, 164.308(a)(1), 164.312(a)(1); HIPAA Security Series, "7 Security Standards: Implementation for the Small Provider," vol. 2, paper 7 (Dec. 10, 2007), at 1-3 ("Factors that determine what is 'reasonable' and 'appropriate' include cost, size, technical infrastructure and resources."), 12 ("The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts.") (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015).

131. Given this extensive guidance, the provision is sufficiently clear and precise that its requirements can be understood, *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 392 (1965) (citing *FTC v. Henry Broch & Co.*, 368 U.S. 360, 367-68 (1962)).

Reply to Proposed Conclusion of Law No. 131:

Complaint Counsel's Proposed Conclusion of Law No. 131 is erroneous, misleading, and contrary to the facts of this case.

First, it is not clear what the "provision" is that Complaint Counsel cites: Section I of the Notice Order or Section 5 generally.

Second, the Commision's "large amount of guidance . . . on general data security practices," is similarly irrelevant. The record clearly demonstrates that the Commission failed to provide LabMD with adequate *ex ante* notice of what FTC prohibited and permitted with respect to HIPAA-regulated entities. This is a violation of due process. *See Fox Television*, 132 S. Ct. at 2317; *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987). The consent

decrees, public statements, education materials, industry guidance pieces, and Congressional testimony that the Commission relies upon in this case, (RX 532 (Kaufman, Dep. at 163-220)), are legally insufficient to demonstrate otherwise.

The APA requires agencies to "publish in the Federal Register for the guidance of the public . . . substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency[.]" 5 U.S.C. § 552(a)(1)(D). It further provides that, except to the extent "that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published." 5 U.S.C. § 552(a)(1)(E).

As a matter of law, then, the APA obligates the Comission to "separately state and currently publish in the Federal Register for the guidance of the public . . . *statements of general policy or interpretations of general applicability* formulated and adopted by the agency[.]" *See* 5 U.S.C. § 552(a)(1)(D) (emphasis added). The APA bars agencies from enforcing statements of general policy and interpretations of general applicability "[e]xcept to the extent that a person has actual and timely notice" by Federal Register publication. *See* 5 U.S.C. § 552(a)(1)(E); *Util. Solid Waste*, 236 F.3d at 754.

The Commission promulgates general statements of policy at 16 C.F.R. Part 14, but there is none for medical data security. The Commission promulgates guides for business, but there are none for medical data security. *See, e.g.*, 16 C.F.R. pt. 251. The Commission promulgates trade rules for business, but there are none for medical data security. *See, e.g.*, 16 C.F.R. pt. 455.

Complaint Counsel cites as "standards" in this case materials that have not been published in the Federal Register in violation of 5 U.S.C. § 552(a)(1)(D). *See* Complaint Counsel's Pre-Trial Brief, *In the Matter of LabMD, Inc.*, No. 9357, at 13-14, 18-20 (F.T.C. May 6, 2014) (citations omitted). It has created and applied data security standards as if they had been promulgated as a guide or trade rule. Complaint Counsel's use of adjudication to set or apply supposedly preexisting medical data security standards that might add to or alter existing APA-promulgated HIPAA regulations or guidance, based on materials not previously published in the Federal Register, is an abuse of discretion and contrary to law under the APA.

Third, nothing in the Notice Order explains how conflicts between Section 5 and HIPAA are to be avoided or resolved. Incredibly, in its attempt to regulate a HIPAA covered entity, FTC ignores the HIPAA Security Rule and HIPAA Breach Notification Rule entirely. This demonstrates that FTC has overstepped and lacks legal authority for this adjudication. *Accord Credit Suisse*, 551 U.S. at 272-73; *Wyndham*, 2015 U.S. App. LEXIS 14839 at *39-41 (discussing agency's obligation to provide fair notice and "ascertainable certainty"); *Ford Motor Co.*, 673 F.2d 1008; *Bell Aerospace Co.*, 416 U.S. 267.

132. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 132:

LabMD has no specific response to Proposed Conclusion of Law No. 132.

1.4.4.3 Part II: Initial and Biennial Assessments

133. Part II of the Notice Order requires LabMD to obtain initial and then biennial assessments and reports for twenty years from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The Notice Order provides examples of the types of qualifications that are sufficient for such qualified, objective, and independent third-party professionals.

Reply to Proposed Conclusion of Law No. 133:

Complaint Counsel's Proposed Conclusion of Law No. 133 is a statement of fact and should be stricken accordingly.

LabMD notes the Notice Order is *ultra vires* and unlawful. 15 U.S.C. § 45(b); *Ass'n of Am. R.R.s*, 135 S. Ct. 1225.

134. The provision enumerates the elements that must be included in the assessment, which must: (1) set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained; (2) explain how the 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; (3) explain how the safeguards that have been implemented meet or exceed the provisions in Part I of the order; and (4) certify that respondent's security program provides reasonable assurance that the security, confidentiality, and integrity of Personal Information is protected.

Reply to Proposed Conclusion of Law No. 134:

Complaint Counsel's Proposed Conclusion of Law No. 134 is a statement of fact and should be stricken accordingly.

LabMD notes the Notice Order is *ultra vires* and unlawful. 15 U.S.C. § 45(b); *Ass'n of Am. R.R.s*, 135 S. Ct. 1225.

135. This provision is consistent with prior Commission orders in data security cases. *See, e.g.*, Conclusions of Law ¶¶ 17, 18.

Reply to Proposed Conclusion of Law No. 135:

Complaint Counsel's Proposed Conclusion of Law No. 135 is irrelevant.

First, the Notice Order is *ultra vires* and unlawful. 15 U.S.C. § 45(b); *Ass'n of Am. R.R.s*, 135 S. Ct. 1225.

Second, equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746

F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. Consent Orders are not competent legal authority here. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement"); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312; 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed relief is consistent with the Commission's prior orders is irrelevant. *Accord Borg-Warner Corp.*, 746 F.2d at 110-11; *Litton Indus.* 676 F.2d at 371.

136. Such independent third-party review is appropriate fencing-in relief. *See Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 314 (May 17, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/05/120521pomdecision.pdf (the requirement of competent and reliable scientific evidence "based on the expertise of professionals in the relevant area" is "typical"); *see, e.g., U.S. v. Consumer Portfolio Servs., Inc.*, No. 8:14-cv-00819-ABC-RNB, Section V at 8-9 (Stip. Order for Perm. Injunct.) (C.D. Cal. June 11, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc (requiring that defendant obtain an assessment and report regarding its comprehensive data integrity program from a qualified, objective, independent, third-party professional); *FTC v. Smolev*, No. 01-8922 CIV-Zloch Sections V.B.2 at 17, VI at 18-20 (Stip. Final Judgment) (S.D. Fla. Oct. 24, 2001), *available at* http://www.ftc.gov/enforcement/cases-proceedings/992-3255/smolev-ira-bruce-turiansky-triad-discount-buying-service-inc (requiring, under certain circumstances, defendant to use an independent third-party verifier for telemarketing transactions); *FTC v. Special Data Processing Corp.*, Case No. 8:04-cv-1955-T-23EAJ, Sections IV.B.3. at 13 and V. at 13-15 (Stip. Judgment) (M.D. Fla. Sept. 30, 2004), *available at* http://www.ftc.gov/enforcement/cases-proceedings/002-3213/special-data-processing-corporation (Stip. Judgment) (M.D. Fla. Sept. 29, 2004) (requiring, under certain circumstances, defendant to use an independent third-party verifier for telemarketing transactions); *cf.*

Removatron Int'l Corp., 111 F.T.C. 206, 305-06 (1988) (according "substantial weight" to FDA determination regarding product).

Reply to Proposed Conclusion of law No. 136:

Complaint Counsel's Proposed Conclusion of Law No. 136 is irrelevant.

First, the Notice Order is *ultra vires* and third party review is unlawful. 15 U.S.C. § 45(b); *Ass'n of Am. R.R.s*, 135 S. Ct. 1225.

Second, equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. Consent Orders are not competent legal authority here. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement."); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312; 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed relief is consistent with the Commission's prior settlements is irrelevant.

Third, none of the cited settlements is factually analogus to this case. Those cases involved actual or certainly impending consumer injury. This case does not. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law. *Compare Wyndham*, 2015 U.S. App. LEXIS

14839, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70 (involving death and serious injury).

Absent a satisfactory demonstration of the past "egregiousness of [LabMD's] action, the isolated or recurrent nature of the [alleged] infraction[s] involved, . . . and the likelihood that [LabMD's present acts and practices] will present opporutnities for future violations," the need for injunctive relief cannot arise. *Think Achievement Corp.*, 144 F. Supp. 2d at 1017; *Borg-Warner Corp.*, 746 F.2d at 110.

137. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 137:

LabMD has no specific response to Proposed Conclusion of Law No. 137.

1.4.4.3.1 Part II's Fencing-In Provision is Appropriate.

138. Fencing-in relief is "designed to prevent future unlawful conduct, and provides for order provisions that are broader than the conduct found to violate Section 5." *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006) (citing *Telebrands*, 140 F.T.C. 278, 281 n.3 (2005)); *Am. Home Prods. v. FTC*, 695 F.2d 681, 705 (3d Cir. 1982); *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citing *FTC v. Colgate-Palmolive*, 380 U.S. 374, 395 (1965)); *Sears v. FTC*, 676 F.2d 385, 391-92 (9th Cir. 1982)).

Reply to Proposed Conclusion of Law No. 138:

Complaint Counsel's Proposed Conclusion of Law No. 138 is erroneous and irrelevant. LabMD incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, as appropriate.

139. The Commission's "wide discretion" to craft that remedy is subject to only two constraints: the order must bear a "reasonable relation" to the unlawful practices, *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612-13 (1946); and it must be sufficiently clear and precise that its requirements can be understood, *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 392 (1965).

Reply to Proposed Conclusion of Law No. 139:

Complaint Counsel's Proposed Conclusion of Law No. 139 is erroneous and misleading.

First, the Commission's discretion is limited to cases and conduct that present a present or certainly impending future violation of Section 5(a) and 5(n). 15 U.S.C. §§ 45(a), (n); *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. This case, and LabMD's conduct, does not fall into this basket.

Second, FTC's discretion is not umlimited. There must be a connection between the remedy and the putative illegal conduct. *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. 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. 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.

140. Pursuant to this discretion, courts have affirmed Commission orders requiring remedies as diverse as prohibitions on individual use of zone pricing (*FTC v. Nat'l Lead Co*., 352 U.S. 419, 431 (1957)); cancellation of existing contracts (*North Tex. Specialty Physicians v. FTC*, 528 F.3d 346, 372 (5th Cir. 2008)); mandated divestiture of assets to create a competitor (*Chicago Bridge & Iron Co. N.V. v. FTC*, 534 F.3d 410, 441 (5th Cir. 2008)); requirements for varying levels of substantiation for future claims (*See, e.g*., *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 389 n.10, 400 (9th Cir. 1982) (requiring competent and reliable evidence for future performance claims for major household appliances); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192, 197 (D.C. Cir. 1986) (requiring at least two adequate and well-controlled, double-blinded clinical studies for future efficacy claims for a topical analgesic)); disclosure requirements (*Porter & Dietsch, Inc. v. FTC*, 605 F.2d 294, 306-07 (7th Cir. 1979)) and trade name

> excision (*Cont'l Wax Co. v. FTC*, 330 F.2d 475, 479-80 (2d Cir. 1964)). The underlying inquiry in all these orders is the same: what is the necessary remedy to ensure that respondents do not again violate the FTC Act? *See FTC v. Colgate-Palmolive Co*., 380 U.S. 374, 392 (1965).

Reply to Proposed Conclusion of Law No. 140:

Complaint Counsel's Proposed Conclusion of Law No. 140 is irrelevant.

First, the appropriateness of equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. Consent Orders are not competent legal authority here. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement"); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312. Neither are settlements. 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed relief is consistent with the Commission's prior settlements is irrelevant.

Second, none of the cited settlements is factually analogus to this case. Those cases involved actual or certainly impending consumer injury. This case does not. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law. *Compare Wyndham*, 10 F. Supp. 3d at 609, *with*

Neiman Marcus, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48. There is no basis here for equitable relief. *Borg-Warner Corp.*, 746 F.2d at 110; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

141. The Commission may order "provisions that are broader than the conduct that is declared unlawful." *Telebrands Corp*., 457 F.3d at 357 n.5 (citing *Telebrands*, 140 F.T.C. at 281 n.3); *see also, e.g.*, *FTC v. Colgate-Palmolive Co*., 380 U.S. 374, 394-95 (1965); *FTC v. Ruberoid Co*., 343 U.S. 470, 473 (1952); *POM Wonderful*, 2013 FTC LEXIS 6, at *50 (Jan. 10, 2013), *aff'd* 777 F.3d 478 (D.C. Cir. 2015). To the extent the proposed notice order goes beyond LabMD's specific practices, such fencing-in relief is appropriate in light of LabMD's multiple and systemic data security failures. The Notice Order is narrowly crafted to prevent LabMD from continuing to place consumers' Personal Information at risk, while still allowing LabMD to collect, use, and store Personal Information to conduct its business.

Reply to Proposed Conclusion of Law No. 141:

Complaint Counsel's Proposed Conclusion of Law No. 141 is erroneous, misleading, and contrary to the facts of this case.

First, LabMD incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, as appropriate.

Second, there is no evidence in the record that the Notice Order will allow LabMD to conduct its business. Complaint Counsel could have asked Dr. Hill to evaluate the impact of the proposed relief, but it did not do so. (Although Dr. Hill, with no knowledge of the medical business, could not have rendered a competent opinion in any event.) This is a critical failure. As the Commission suggests:

> [C]onduct must be harmful in its net effects [to be unfair]. This is simply a recognition of the fact that most conduct creates a mixture of both beneficial and adverse consequences. In analyzing an omission (i.e., LabMD's alleged failure to have 'reasonable' data security) the unfairness analysis requires us to balance gainst (sic) the risks of injury the costs of [cure]. . . . This inquiry must be made in a level of detail that deception analysis does not contemplate.

Int'l Harvester Co., 104 F.T.C. at 1061. Complaint Counsel's failure to conduct this detailed analysis, and to put in testimony with respect to the balance between risk and cost, means that any finding against LabMD is arbitrary and capricious. *Fox Television II*, 556 U.S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action").

142. This fencing-in relief is reasonably related to LabMD's conduct. *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612 (1946). Even where the company had data security policies, it did not adequately enforce them, or provide the tools needed to implement them. *Supra* CCFF § 5.2.4 (LabMD Did Not Enforce Some of the Policies in its Policy Manuals) *et seq.* (¶¶ 458-480). For example, despite a policy against the installation of installation of personal programs and personal use of the Internet, LimeWire was installed and used a LabMD employee's computer. *See supra* CCFF §§ 5.2.4.1 (LabMD Did Not Enforce Its Policy to Restrict Downloads from the Internet) (¶¶ 458-462), 8.1.2 (1718 File Shared on Gnutella Network through LimeWire on a LabMD Billing Computer) (¶¶ 1363-1372), CCCL § 1.4.3.1 (LabMD's Failure to Address its Data Security Failures was Deliberate) (¶¶ 91-103). Although LabMD's policies stated that emails containing sensitive information were required to be encrypted, employees testified that no tools were provided to encrypt such emails. *See supra* CCFF § 5.2.4.3 (LabMD Did Not Enforce Its Recommendation that Employees Encrypt Emails) (¶¶ 474-480).

Reply to Proposed Conclusion of Law No. 142:

Complaint Counsel's Proposed Conclusion of Law No. 142 is a statement of fact and should be stricken accordingly. It is also erroneous, misleading, and contrary to the facts of this case.

The proposed fencing-in relief does not bear a "reasonable relationship" to LabMD's conduct. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years, based on "standards" concocted as part of a litigation case by an expert without knowledge of the medical industry, and applied retroactively between four and nine years after the fact, cannot possibly justify a twenty-year future fencing-in. *Wyndham*, 2015 U.S. App. LEXIS 14839; *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12; *In re*

Sci. Applications Int'l Corp., 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48. Hypothetical potential "exposure," non-existent injury, and *post hoc* standards cannot justify equitable relief here. *Borg-Warner Corp.*, 746 F.2d at 110; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

LabMD also incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, as appropriate.

143. A fencing-in provision must be "sufficiently clear that it is comprehensible to the violator, and must be 'reasonably relat[ed]' to a violation of the act." *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citing *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965)).

Reply to Proposed Conclusion of Law No. 143:

LabMD has no response to Complaint Counsel's Proposed Conclusion of Law No. 143. The cases say what they say.

144. The four provisions of the fencing-in relief laid out in Part II, along with the necessary credentials of the third party, are clear and precise, particularly given that a virtually identical provision has been imposed in many of the Commission's past orders. (*Supra* CCCL ¶ 18).

Reply to Proposed Conclusion of Law No. 144:

Complaint Counsel's Proposed Conclusion of Law No. 144 is irrelevant and erroneous.

First, the appropriateness of equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. Consent Orders are not competent legal authority here. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement");

Gen. Motors Corp., 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement."); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312. Neither are settlements. 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed relief is consistent with the Commission's prior settlements is irrelevant.

Second, past orders involved actual or certainly impending consumer injury. This case does not. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law. *Compare Wyndham*, 2015 U.S. App. LEXIS 14839, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48.

The proposed fencing-in relief does not bear a "reasonable relationship" to LabMD's conduct. Alleged "data security failures" that do not result in a single consumer victim over a period of more than ten years, based on "standards" concocted as part of a litigation case by an expert without knowledge of the medical industry, and applied retroactively between four and nine years after the fact, cannot possibly justify a twenty-year future fencing-in. Hypothetical potential "exposure," non-existent injury, and *post hoc* standards cannot justify equitable relief here. *Borg-Warner Corp.*, 746 F.2d at 110; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

LabMD also incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, and 142, as appropriate.

145. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 145:

LabMD has no specific response to Proposed Conclusion of Law No. 145.

1.4.4.4 Part III: Notice to Affected Individuals

146. Part III of the Notice Order requires LabMD to notify Affected Individuals in the 1718 File regarding the unauthorized disclosure of their Personal Information.

Reply to Proposed Conclusion of Law No. 146:

Complaint Counsel's Proposed Conclusion of Law No. 146 is a statement of fact and should be stricken accordingly. LabMD notes that the Notice Order was not authorized by Section 5 and is unlawful.

147. Without notification, consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information or that they can take actions to reduce their risk of harm from identity crime. (*Supra* CCFF § 9.3.4.3 (With No Notification of Unauthorized Disclosure, No Mitigation of Harm is Possible) (¶¶ 1708-1711).

Reply to Proposed Conclusion of Law No. 147:

Complaint Counsel's Proposed Conclusion of Law No. 147 is a statement of fact and should be stricken accordingly. LabMD notes only that the basis for this statement is the wholly unreliable testimony of Richard Kam.

148. Notice to affected consumers is an appropriate remedy. *Int'l Harvester Co.*, 104 F.T.C. 949, 1009 (1984) (noting that an order requiring disclosure of a hazard to consumers "is our ordinary and presumptive response" that is appropriate "even when the respondent has ceased engaging in the conduct in question"); *see also FTC v Accusearch, Inc.*, 2007 WL 4356786 at *9 (D. Wyo. Sept. 28, 2007) (noting, where defendant's had unfairly procured the consumers' phone records, that consumer notice may be an appropriate equitable remedy) and No. 2:06-CV-105-WFD (Order and Judgment for Permanent Injunction and Other Equitable Relief) (Dec. 20, 2007) (requiring defendant to provide FTC with contact information for affected consumers so the Commission could provide notice); *FTC v. Bayview Solutions, LLC*, Case No. 1:14-cv-01830, at 7, Section IV (Stip. Prelim. Injunct.) (D.D.C. Nov. 3, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/150421bayviewstip.pdf

(requiring notice to consumers whose Personal Information defendants disclosed without implementing and using reasonable safeguards to maintain and protect the privacy, security, confidentiality, and integrity of the information); *FTC v. Cornerstone & Co., LLC*, Case No. 1:14-CV-01479, Section IV at 7 (Prelim. Injunct.) (D.D.C. Sept. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141001cornerstoneorder.pdf (requiring notice to consumers whose Personal Information defendants disclosed without implementing and using reasonable safeguards to maintain and protect the privacy, security, confidentiality, and integrity of the information); *U.S. v. InfoTrack Info. Svcs, Inc*., No. 1:14-cv-02054 (N.D. Ill. Mar. 25, 2014) (Stip. Final Judgment), *available at* https://www.ftc.gov/system/files/documents/cases/140409infotrackorder_0.pdf (requiring notice to consumer that was included in a sex offender registry consumer report when information provided to potential employers); *TRENDnet, Inc.*, FTC Docket No. C-4426, FTC File No. 122-3090 (FTC Sept. 4, 2013) (consent order), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf (notice of security flaw that may have allowed unauthorized users to view live feed of in-home cameras); *Compete, Inc.*, FTC Docket No. C-4384, FTC File No. 102-3155 (FTC Feb. 20, 2013) (consent order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competedo.pdf (notice that personal information may have been transmitted insecurely); *Upromise, Inc.*, FTC Docket No. C-4351, FTC File No. 102-3116 (FTC Mar. 27, 2012) (consent order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf (notice that personal information may have been transmitted insecurely).

Reply to Proposed Conclusion of Law No. 148:

Complaint Counsel's Proposed Conclusion of Law No. 144 is irrelevant and erroneous.

First, equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371.

Second, consent orders are not competent legal authority. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement"); *Trans*

Union Corp., 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312. Neither are settlements. 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed relief is consistent with the Commission's prior settlements is irrelevant.

Third, past cases and orders involved actual or certainly impending consumer injury. This case does not. Alleged "data security failures" that do not result in a single actual data breach or a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law nor justify this draconian "relief." *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48.

In truth, the proposed fencing-in relief does not bear a "reasonable relationship" to LabMD's conduct. Alleged "data security failures" that do not cause one consumer victim or HIPAA regulatory violation over a period of more than ten years, based on "standards" concocted as part of a litigation case by an expert without knowledge of the medical industry, and applied retroactively between four and nine years after the fact, cannot possibly justify what FTC demands here. In fact, this is just another data point demonstrating that FTC is retaliating against LabMD for defending its rights. Hypothetical potential "exposure," non-existent injury, and *post hoc* standards cannot justify the equitable relief requested here. *Borg-Warner Corp.*, 746 F.2d at 110; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

LabMD also incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, and 142, as appropriate.

149. Notice to Affected Consumers' insurance companies is also an appropriate remedy, to provide them with an opportunity to protect consumers' identity from misuse. Third party notices are a commonly used remedy to mitigate harms. *See, e.g.*, *PPG Architectural Finishes, Inc*., No. C-4385, 2013 FTC LEXIS 22, at *8-9, 13-14 (Mar. 5, 2013) (consent order) (notices sent to dealers, distributors, and other entities to stop using prior advertising materials with deceptive no VOCs claim for paint and to apply the enclosed stickers to product labeling); *Oreck Corp*., 151 F.T.C. 289, 371-72, 376-77 (May 19, 2011) (consent order) (notice sent to franchisees); *Indoor Tanning Ass'n*., 149 F.T.C. 1406, 1439, 1443-44 (May 13, 2010) (notices sent to association members and other prior recipients of point-of-sale materials); *Cytodyne LLC*, 140 F.T.C. 191, 209, 214-15 (Aug. 23, 2005) (consent order) (notices sent to purchaser for resale of weight-loss supplement); *Snore Formula, Inc*., 136 F.T.C. 214, 298-99, 304-05 (July 24, 2003) (consent order) (notices sent to distributors who had purchased the product from the respondents or one of the respondents' other distributors); *MaxCell BioScience, Inc*., 132 F.T.C. 1, 58-59, 66-67 (July 30, 2001) (consent order) (notice to distributors); *Alternative Cigarettes, Inc*., No. C-3956, 2000 FTC LEXIS 59, at *24, 31-33 (Apr. 27, 2000) (consent order) (notices to retailers, distributors, or other purchasers for resale to which respondents supplied cigarettes); *Body Sys. Tech., Inc*., 128 F.T.C. 299, 312, 318-19 (Sept. 7, 1999) (consent order) (notice to distributors); *Brake Guard Prods., Inc*., 125 F.T.C. 138, 259-60, 263-64 (Jan. 15, 1998) (consent order) (notice to resellers); *Phaseout of Am., Inc*., 123 F.T.C. 395, 457, 461-63 (Feb. 12, 1997) (consent order) (notice to resellers); *Consumer Direct, Inc*., No. 9236, 1990 FTC LEXIS 260, at *10-11, 20-21 (May 1, 1990) (consent order) (notice to credit card syndicators); *Third Option Labs., Inc*., 120 F.T.C. 973, 996, 1001 (Nov. 29, 1995) (consent order) (notice to resellers); *Canandaigua Wine Co*., 114 F.T.C. 349, 359-60 (June 26, 1991) (consent order) (notice to distributors and retailers).

Reply to Proposed Conclusion of Law No. 149:

Complaint Counsel's Proposed Conclusion of Law No. 149 is irrelevant, erroneous, and misleading.

First, equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371.

Second, consent orders are not competent legal authority. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement."); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312. Neither are settlements. 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed relief is consistent with the Commission's prior settlements is irrelevant.

Third, past cases and orders involved actual or certainly impending consumer injury. This case does not. Alleged "data security failures" that do not result in a single actual data breach or a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law or justify this draconian "relief." *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48.

The proposed fencing-in relief does not bear a "reasonable relationship" to LabMD's conduct. Alleged "data security failures" that do not cause one consumer victim or HIPAA regulatory violation over a period of more than ten years, based on "standards" concocted as part of a litigation case by an expert without knowledge of the medical industry, and applied retroactively between four and nine years after the fact, cannot possibly justify notice to

insurance companies whose patients' information was stolen in February 2008 and then given to FTC.

Complaint Counsel's demand for relief is just another data point proving that this action is in retaliation for LabMD standing up and defending its rights. No case holds that the hypothetical potential "exposure," non-existent injury, and *post hoc* standards applied against LabMD is sufficient to support what FTC seeks here. *Borg-Warner Corp.*, 746 F.2d at 110; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70.

LabMD also incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, and 142, as appropriate.

150. Equitable relief, including for consumer notice, "remain[s] viable even if an injunction is otherwise unnecessary." *FTC v Accusearch, Inc.*, 2007 WL 4356786 at *9 (D. Wyo. Sept. 28, 2007).

Reply to Proposed Conclusion of Law No. 150:

This conclusion of law is misleading as stated.

While equitable relief "remain[s] viable even if an an injunction is otherwise unnecessary," *Accusearch*, 2007 U.S. Dist. LEXIS 74905 at *26, the availability of equitable remedies in the absence of an injunction still depends on the Commission's ability to prove improper conduct on the part of defendant, *Int'l Harvester Co.*, 104 F.T.C. at 1069-71, as well as defendant's likelihood of "'engag[ing] in similar unfair acts of practices' in the future." *Accusearch*, 570 F.3d at 1202 (citation omitted); *see W.T. Grant Co.*, 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."). In this case, Complaint Counsel has continually failed to demonstrate LabMD's violation of Section 5 and to persuasively argue the necessity for the punitive fencing-in relief the Commission seeks.

151. LabMD has provided notice to consumers in the Day Sheets, *supra* CCFF § 8.2.4.1 (LabMD Notice to Affected Consumers) (¶¶ 1461-1469), indicating that this Order provision is reasonable. *Daniel Chapter One*, Docket No. 9329, 2009 FTC LEXIS 157, at *275 (noting that the Commission has "considerable discretion in fashioning an appropriate remedial order").

Reply to Proposed Conclusion of Law No. 151:

Complaint Counsel's Proposed Conclusion of Law No. 151 is erroneous and misleading. LabMD complied with the HIPAA Breach Notification Rule. However, that does not indicate that the Order provision in question is reasonable. There is no evidence that the patients on the 1718 File stolen by Tiversa have suffered any injury at all in the past seven and one-half years.

Equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371. It has not done so. *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48.

The proposed fencing-in relief does not bear a "reasonable relationship" to LabMD's conduct. Alleged "data security failures" that do not cause one consumer victim or HIPAA regulatory violation over a period of more than ten years, based on "standards" concocted as part of a litigation case by an expert without knowledge of the medical industry, and applied retroactively between four and nine years after the fact, cannot possibly justify notice to insurance companies whose patients' information was stolen in February 2008 and then given to FTC. This demand is just another example of FTC's punitive demands. Hypothetical potential "exposure," non-existent injury, and *post hoc* standards cannot justify equitable relief here. *Borg-Warner Corp.*, 746 F.2d at 110; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70. LabMD also

incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, and 142, as appropriate.

152. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 152:

LabMD has no specific response to Proposed Conclusion of Law No. 152.

1.4.4.5 Parts IV-VIII: Recordkeeping Provisions

153. One of the purposes of injunctive relief is "monitoring compliance with the law and the terms of the injunction." *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009).

Reply to Proposed Conclusion of Law No. 153:

LabMD has no specific response to Complaint Counsel's Proposed Conclusion of Law No. 153, except to note that Complaint Counsel has (once again) misapplied its cited authority. *Direct Marketing* is a deceptive advertising case with actual harm, not an unfairness case in which there is no actual or certainly impending substantial injury.

154. Monitoring provisions to ensure compliance with injunctions are appropriate to include in FTC orders. *FTC v. RCA Credit Svcs, LLC*, 727 F. Supp. 2d 1320, 1335 (M.D. Fla. 2010).

Reply to Proposed Conclusion of Law No. 154:

LabMD has no specific response to Complaint Counsel's Proposed Conclusion of Law No. 154, because the case says what it says. LabMD notes, however, that monitoring is appropriate only if Complaint Counsel carries its burden of establishing a "cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive." *Borg-Warner Corp.*, 746 F.2d at 110 (citing *W.T. Grant Co.*, 345 U.S. 629).

155. The recordkeeping provisions in Parts IV-VIII of the Notice Order are consistent with those in other FTC orders. *See, e.g.*, cases cited in CCCL ¶ 19; *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012). Part IV is a record-keeping requirement. Part V sets forth Order distribution

requirements. Part VI requires LabMD to file notifications about changes in corporate structure. Part VII sets forth compliance reporting requirements. Finally, Part VIII is a sunsetting provision.

Reply to Proposed Conclusion of Law No. 155:

Complaint Counsel's Proposed Conclusion of Law No. 155 is irrelevant, erroneous, and misleading.

First, the Notice Order is *ultra vires* and unlawful. 15 U.S.C. § 45(b); *Ass'n of Am. R.R.s*, 135 S. Ct. 1225.

Second, equitable relief is determined on a case-by-case basis and Complaint Counsel must prove cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive. *W.T. Grant Co.*, 345 U.S. at 633; *Borg-Warner Corp.*, 746 F.2d at 110; *see also Litton Indus.*, 676 F.2d at 371.

Third, what FTC may have done in other consent orders or cases is irrelevant. Consent Orders are not competent legal authority here. 15 U.S.C. § 45(m)(2); *Altria Grp.*, 555 U.S. at 89 n.13 ("a consent order is in any event only binding on the parties to the agreement"); *Gen. Motors Corp.*, 897 F.2d at 36 ("Unlike an agency regulation which has industry-wide effect, a consent order is binding only on the parties to the agreement."); *Trans Union Corp.*, 245 F.3d 809; *Beatrice Foods*, 540 F.2d at 312. Neither are settlements. 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, 1305-06 (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."). Thus, whether Complaint Counsel's proposed relief is consistent with the Commission's prior settlements is irrelevant.

Fourth, FTC's past cases and orders involved actual or certainly impending consumer injury. This case does not. Alleged "data security failures" that do not result in a single actual data breach or a single consumer victim over a period of more than ten years cannot be "serious" as a matter of law or justify this draconian "relief." *Compare Wyndham*, 10 F. Supp. 3d at 609, *with Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at *11-12, *and In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 24; *see also Clapper*, 133 S. Ct. at 1147-48.

The proposed fencing-in relief does not bear a "reasonable relationship" to LabMD's conduct. Alleged "data security failures" that do not cause one consumer victim or HIPAA regulatory violation over a period of more than ten years, based on "standards" concocted as part of a litigation case by an expert without knowledge of the medical industry, and applied retroactively between four and nine years after the fact, cannot possibly justify notice to insurance companies whose patients' information was stolen in February 2008 and then given to FTC.

This demand is just another example of FTC's attempt to punish LabMD for daring to defy the agency's demands. FTC is demanding more from LabMD for falling victim to a thief and fraudster (Tiversa), in a case without a single consumer victim, than it has from other who have actually harmed consumers. *Compare* Compl. Counsel's [Corrected] Post-trial Brief Attachment 1 ([Proposed] Order] at pts. IV-VIII *with FTC v. Medicor, LLC*, No. 1-1896, 2002 U.S. Dist. LEXIS 16220, at *6-8 (C.D. Cal. July 19, 2002) *and FTC v. Jordan Ashley, Inc.*, No. 93-2257, 1994 U.S. Dist. LEXIS 7494, at *31-33 (S.D. Fla. Apr. 5, 1994). Complaint Counsel would compel LabMD, among other things, to hire outside contractors to conduct biannual assessments, send letters to all persons on the 1718 File (despite any lack of any evidence of actual or non-speculative future substantial injury), and establish a hotline and website. The

additional requirement to implement certain record retention and reporting requirements for up to twenty years is simply inappropriate, unsupported by the record, and part-and-parcel of unlawfully punitive "fencing-in" relief. *See, e.g.*, *Riordan*, 627 F.3d at 1234. Hypothetical potential "exposure," non-existent injury, and *post hoc* standards cannot justify what Complaint Counsel demands here. *Borg-Warner Corp.*, 746 F.2d at 110; *Int'l Harvester Co.*, 104 F.T.C. at 1069-70. LabMD also incorporates its references to Complaint Counsel's Proposed Conclusions of Law Nos. 57, 80-90, 116-121, and 142, as appropriate.

156. Intentionally left blank.

Reply to Proposed Conclusion of Law No. 156:

LabMD has no specific response to Proposed Conclusion of Law No. 156.

Notice of Electronic Service

I hereby certify that on September 03, 2015, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s Reply to Complaint Counsel's Proposed Conclusions of Law, 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 03, 2015, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s Reply to Complaint Counsel's Proposed Conclusions of Law, 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