No. 16-16270

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

LabMD, Inc.,

Petitioner,

v.

Federal Trade Commission,

Respondent.

Petition for Review from the Federal Trade Commission, *In the Matter of LabMD, Inc.*, FTC Matter/File Number: 102 3099, Docket Number: 9357

BRIEF OF PETITIONER, LABMD, INC.

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

David T. Cohen
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
(212) 596-9000

Michelle L. Visser
ROPES & GRAY LLP
Three Embarcadero Center
San Francisco, CA 94111-4006
(415) 315-6300

Douglas Hallward-Driemeier
ROPES & GRAY LLP
2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
(202) 508-4600

Counsel for LabMD, Inc.

UNITED STATES COURT OF APPEALS

FOR THE

ELEVENTH CIRCUIT

LABMD, INC, Petitioner, v. FEDERAL TRADE COMMISSION, Respondent.	)	Case File No. 16-16270 FTC Docket No. 9357

CORPORATE DISCLOSURE STATEMENT AND CERTIFICATE OF INTERESTED PERSONS

Pursuant to Federal Rule of Appellate Procedure 26.1, Petitioner LabMD, Inc. ("LabMD"), by and through its undersigned counsel, hereby states that LabMD does not have a parent corporation and that no publicly held corporation owns ten percent or more of LabMD's stock. Further, pursuant to Eleventh Circuit Rule 26.1-1, Petitioner hereby certifies that the following persons and entities have an interest in the outcome of this petition:

Barrickman, Allred & Young, LLC, Counsel for Scott Moulton

Bavasi, Haley, Attorney, Ropes & Gray LLP

Berger, Laura, Attorney, FTC

Boback, Robert J., nonparty below

Brill, Julie, Former Commissioner, FTC

Brown, Jarad A., Attorney, FTC

Brown, Reginald J., Attorney, Counsel for Tiversa

Bryan Cave LLP, Counsel for Richard Wallace

Buchanan, Mary Beth, Attorney, Bryan Cave LLP

Burrows, Robyn N., Attorney, formerly of Cause of Action

Cause of Action, Counsel for LabMD

Chappell, D. Michael, Chief Administrative Law Judge, FTC

Clark, Donald S., Secretary, FTC

Claybaugh, Melinda, Attorney, FTC

Cohen, David T., Attorney, Ropes & Gray LLP

Cox, Megan, Attorney, FTC

Daugherty, Michael J., Chief Executive Officer, LabMD

Dinsmore & Shohl LLP, Counsel for LabMD

Epstein, Daniel Z., Attorney, formerly of Cause of Action

Federal Trade Commission ("FTC"), Respondent

Feldman, John P., Attorney, Reed Smith LLP

Forensic Strategy Services, LLC, nonparty below

Gelsomini, Nicole, Attorney, Ropes & Gray LLP

Gersh, Deborah L., Attorney, Ropes & Gray LLP

Hallward-Driemeier, Douglas, Attorney, Ropes & Gray LLP

Harris, Lorinda B., Attorney, formerly of Cause of Action

Harris, Sunni R., Attorney, Dinsmore & Shohl LLP

Hoffman, Matthew M., Attorney, FTC

Howard, Elizabeth G., Attorney, Barrickman, Allred & Young, LLC

Huntington, Kent G., Attorney, formerly of Cause of Action

Johnson, M. Eric, Professor, Vanderbilt University

Kaufman, Daniel, Deputy Director, FTC Bureau of Consumer Protection

Khetan, Prashant K., Attorney, formerly of Cause of Action

Kotlyar, Leon, Attorney, Ropes & Gray LLP

Krebs, John, Attorney, FTC

LabMD, Inc., Petitioner

Lassack, Margaret L., Attorney, FTC

Lattimore, Ashton R., Attorney, Ropes & Gray LLP

Lechner, Jr., Alfred J., Attorney, Cause of Action

Marcus, Joel, Attorney, FTC

Marshall, Erica L., Attorney, Cause of Action

Massari, Patrick J., Attorney, Cause of Action

McSweeny, Terrell, Commissioner, FTC

Meal, Douglas H., Attorney, Ropes & Gray LLP

Mehm, Ryan M., Attorney, FTC

Metzler, Jr., Theodore P., Attorney, FTC

Morgan, Hallee K., Attorney, Cause of Action

Moulton, Scott, President, Forensic Strategy Services, LLC, nonparty below

Moundas, Christine, Attorney, Ropes & Gray LLP

Nordsieck, David W., Attorney, Ropes & Gray LLP

Ohlhausen, Maureen K., Commissioner, FTC

O'Leary, Kevin D., Associate General Counsel, Dartmouth College

Pepson, Michael D., Attorney, Cause of Action

Ramirez, Edith, Chairwoman, FTC

Reed Smith LLP, Counsel for Robert J. Boback and Tiversa

Ropes & Gray LLP, Counsel for LabMD

Rubinstein, Reed D., Attorney, Dinsmore & Shohl LLP

Santiesteban, Joseph, Attorney, Ropes & Gray LLP

Schell, Jacquelyn N., Attorney, Bryan Cave LLP

Schoshinski, Robert, Assistant Director, FTC

Settlemyer, Carl H., Attorney, FTC

Shaw, Jarrod D., Attorney, Reed Smith LLP

Sheer, Alain, Attorney, FTC

Sherman, II, William A., Attorney, Dinsmore & Shohl LLP

Shonka, David C., Attorney, FTC

Struble, Thomas, Attorney, TechFreedom

Szoka, Berin, Attorney, TechFreedom

TechFreedom, *amicus curiae* below

Tiversa Holding Corporation, nonparty below

Tiversa, Inc., nonparty below

VanDruff, Laura Riposo, Attorney, FTC

Visser, Michelle L., Attorney, Ropes & Gray LLP

Wallace, Richard, nonparty below

Wright, Joshua D., Former Commissioner, FTC

Yodaiken, Ruth, Attorney, FTC

Dated: December 27, 2016

Respectfully Submitted,
Counsel for LabMD, Inc.

/s/ Douglas H. Meal

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

Michelle L. Visser
ROPES & GRAY LLP
Three Embarcadero Center
San Francisco, CA 94111-006
(415) 315-6300

Douglas Hallward-Driemeier
ROPES & GRAY LLP
2009 Pennsylvania Avenue, NW
Washington, DC 20006-6807
(202) 508-4600

David T. Cohen
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
(212) 841-9000

STATEMENT REGARDING ORAL ARGUMENT

Pursuant to Fed. R. App. P. 34(a) and Eleventh Circuit Rule 34-3(c), Petitioner LabMD requests oral argument. This case presents significant issues of statutory and constitutional interpretation. It also concerns evidentiary issues arising from the substantial record compiled during the administrative proceedings that took place before the FTC. Oral argument could assist this Court in consideration both of the legal issues raised herein and of the record.

TABLE OF CONTENTS

Page

TABLE OF CITATIONS

Page(s)

CASES

STATUTES AND RULES

OTHER AUTHORITIES

STATEMENT OF SUBJECT-MATTER AND APPELLATE JURISDICTION

This is a petition for review of an order ("Order") and related opinion ("Opinion") of the Federal Trade Commission (the "Commission" or "FTC") finding that Petitioner LabMD, Inc.'s ("LabMD") data security practices were unfair under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("Section 5"). The Order was served on August 1, 2016. LabMD timely filed this petition on September 29, 2016. *See* 15 U.S.C. § 45(c); FED. R. APP. P. 15(a). This Court has jurisdiction under 15 U.S.C. § 45(c).

STATEMENT OF THE ISSUES PRESENTED

1. Whether the Commission exceeded its legal authority in finding LabMD's data security practices "unfair" under Section 5.

2. Whether the Opinion is unsupported by substantial evidence.

3. Whether the Order's remedies and relief are invalid even assuming a Section 5 violation.

4. Whether, in light of substantial reasons to believe the FTC may have violated LabMD's First and Fourth Amendment rights, LabMD is entitled to further discovery.

STATEMENT OF THE CASE

I. NATURE OF THE CASE

In this federal agency enforcement action, the FTC overstepped its authority and, in the process, destroyed a small medical testing company. As described below, the FTC's attempt to expand its powers, at LabMD's expense, contravened the text, and Congress's and the Commission's own prior interpretations, of Section 5; created an impermissible conflict with comprehensive federal healthcare legislation; violated LabMD's due process rights; repeatedly and inexplicably ignored crucial record evidence, including evidence of LabMD's substantial data security measures; and exceeded the statutory limits on the agency's remedial authority. The Commission's overreach here is particularly troublesome because there is substantial reason to believe (1) the agency itself had a hand in the very

data theft the Commission used to justify its action against LabMD, and (2) the Commission proceeded against LabMD in retaliation for its CEO's exercise of his First Amendment rights when it "coincidentally" announced its intention to bring this action just three days after LabMD's CEO announced his book decrying the FTC's overreach. The Order should be vacated.

II. STATEMENT OF FACTS

LabMD is a small, now-defunct medical laboratory that previously conducted diagnostic testing for cancer by using medical specimen samples, along with relevant patient information, to provide diagnoses to its physician customers. (Doc. 326, 18-19 ¶¶ 26-28.) As a medical facility that collected personal health information ("PHI"), LabMD was subject to detailed medical data security regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). (Doc. 355, Op. 12 & n.22.) To protect patients' data, LabMD employed a comprehensive security program that included a compliance program, training, firewalls, network monitoring, password controls, access controls, antivirus, and security-related inspections. (*See, e.g.*, CX0443-44; CX0446-47; RX0533, 16-22; Tr. 15, 148:22-149:25; CX0001; CX0626.)

In early 2008, Tiversa Holding Corporation ("Tiversa") stole a LabMD file (the "1718 File") from a LabMD workstation. Tiversa committed the theft by exploiting a vulnerability in a "peer-to-peer" file-sharing application (the "P2P

vulnerability") that, contrary to LabMD policy, an employee used to listen to music while at that workstation. (Doc. 326, 25 ¶ 86; CX0001-02.) The 1718 File had been stored on the workstation no earlier than June 2007 and contained a limited amount of PHI[1] relating to approximately 9,300 (the "1718 File Patients") of the approximately 750,000 patients as to which LabMD then held PHI. (Doc. 355, Op. 1, 3, 17.)

Tiversa committed this theft just a few months after meeting privately with the FTC and describing Tiversa's ability to use the P2P vulnerability to hack into unsuspecting companies and steal consumers' personal information.[2] (*See* Doc. 326, 30-31 ¶¶ 130-34; Tr. 51, 1348:19-1352:13.) After stealing the 1718 File, Tiversa undertook to extort LabMD, repeatedly contacting LabMD to sell its service to "remediate" the P2P vulnerability. (Doc. 326, 30 ¶¶ 128-29.) LabMD refused Tiversa's services and instead on its own eliminated the P2P vulnerability from the workstation in May 2008. (Doc. 326, 58.) The period during which the 1718 File was subject to the P2P vulnerability thus began no earlier than June 2007 and ended no later than May 2008 (the "Relevant Period").

[1] Specifically, names, addresses, birthdates, Social Security numbers, insurance information, and laboratory test codes (but not test results). (Doc. 326, 24 ¶¶ 82-83.)

[2] The FTC's exact response to Tiversa's description of the P2P vulnerability is unknown, because LabMD was denied discovery regarding that response. (*See* Doc. 49, 2, 5-7; Doc. 62, 2, 4-5; Doc. 65, 2-5.)

After LabMD's refusal to pay off Tiversa, Tiversa entered into a deal with the FTC pursuant to which Tiversa transferred the 1718 File to the FTC through a shell company created for that purpose. (Doc. 326, 30-32 ¶¶ 131-45.) In January 2010, based entirely on the stolen 1718 File, the FTC began an investigation into LabMD's data security practices. (Doc. 326, 6.) On July 22, 2013—"coincidentally" just three days after LabMD's CEO disclosed his intent to publish a book criticizing the FTC's investigatory overreach—the FTC informed LabMD that it intended to issue an administrative complaint against the company, which it did the following month. *See LabMD, Inc. v. F.T.C.*, 776 F.3d 1275, 1277 (11th Cir. 2015). The complaint alleged LabMD had violated Section 5's prohibition on "unfair" acts and practices because its data security practices did not include certain measures that, "taken together," were necessary to provide "reasonable" security. (Doc. 2, ¶ 10.)

In fall 2013, after having again met with the FTC,[3] Tiversa fabricated false evidence that the 1718 File had spread across the Internet, and provided that fabricated evidence to the FTC. (Doc. 326, 32 ¶¶ 146-49.) During the administrative trial, the FTC relied heavily on the fabricated evidence, offering it in support of the FTC's core allegation that consumers had suffered, or were likely

[3] Here again, LabMD was denied discovery into the communications between the FTC and Tiversa at, leading up to, or following the meeting. (*See* Doc. 49, 2, 5-7; Doc. 62, 2, 4-5; Doc. 65, 2-5.)

to suffer, substantial injury by reason of LabMD's supposedly lax data security practices in regard to the 1718 File. (Doc. 326, 60.) When the fabrication was revealed mid-trial, the FTC was forced to withdraw that "evidence." (Doc. 326, 10.) Ultimately, the FTC never produced any *non*-fabricated evidence that the 1718 File had ever been stolen by anyone other than Tiversa or had otherwise "spread" across the Internet. (Doc. 326, 10-11, 32-33, 159.) Nor did the FTC present any evidence that any of the few unauthorized persons and entities who *did* obtain the 1718 File[4] used or were likely to use it in a way that harmed the 1718 File Patients. (Doc. 326, 69.)

Undeterred by the significant evidentiary gaps in its case, the FTC forged ahead. In so doing, because its only "evidence" of actual or likely injury had been shown to be fabricated, the FTC was cornered into two new interpretations of Section 5: first, that the *mere disclosure* of personal information to an unauthorized third party, without more, creates a conceptual "loss of consumer privacy" that in and of itself is "substantial injury" under Section 5; and second, that *unlikely* consumer injury can nonetheless be "likely" under Section 5 if its magnitude would be "large." These two new theories that the FTC resorted to at the eleventh hour in order to continue its obsessive pursuit of its case against LabMD were to become the centerpieces of the FTC's decision finding LabMD liable under

[4] Namely, Tiversa, the FTC, and a Dartmouth professor who received the file from Tiversa in connection with government-funded research. (Doc. 326, 69 n.34.)

Section 5, and those two theories now stand as two of LabMD's principal grounds for challenging that decision in this appeal.

Meanwhile, in January 2014, as a result of the crushing burdens imposed upon it by the FTC's investigation and ensuing action, LabMD was forced to wind down operations and stop diagnosing cancer. (Doc. 359, Ex. 18, ¶ 3.) LabMD's financial condition is beyond repair, and it has no prospect of resuming business. (*Id.* at ¶¶ 5-8.)

III. PROCEDURAL HISTORY

After the administrative trial, the Administrative Law Judge (the "ALJ") dismissed the FTC's complaint, holding that the FTC failed to prove LabMD's supposedly lax data security practices caused or are likely to cause "substantial injury" as required by Section 5(n). (Doc. 326, 88.) On appeal, however, the FTC followed its established pattern of reversing the ALJ in favor of itself,[5] finding that LabMD's alleged failure to employ certain additional or reconfigured security measures (the "Additional Security Measures") rendered LabMD's security for the 1718 File "unreasonable." (Doc. 355, Op. 1, 11-12.) The FTC further found that

[5] As former FTC Commissioner Joshua Wright noted, "[i]n the past nearly 20 years" before the LabMD action, the "FTC ha[d] ruled in favor of [its] Staff on appeal in 100% of cases." *The Need for Limits on Agency Discretion & the Case for Section 5 Guidelines*, Presentation of Commissioner Joshua F. Wright, FTC, at 7 (Dec. 16, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/need-limits-agency-discretion-case-section-5-guidelines/131216section5_wright.pdf.

certain of the Additional Security Measures would have reduced the risk of the 1718 File's being stolen had they been deployed. (Doc. 355, Op. 16.) Based on those findings, and despite there being no evidence that the 1718 File was ever used by anyone in any way that caused tangible injury to any consumer, the FTC found that LabMD's purported failure to employ the Additional Security Measures:

1. caused "substantial injury" to consumers under Section 5(n) because Tiversa's theft of the 1718 File in and of itself caused each 1718 File Patient to suffer a *conceptual* "privacy harm," even though that theft did not in and of itself have *any* effect—tangible *or* intangible—on any of those patients (Doc. 355, Op. 17-19), and in any event,
2. was, at some point in the past, "likely" to cause substantial injury under Section 5(n), notwithstanding the injury's "low likelihood," because over eight years earlier, during the Relevant Period, the 1718 File theoretically "could have" been obtained via the P2P vulnerability by unauthorized parties other than Tiversa who *could have* used the file in ways that *could have* resulted in tangible

and intangible harm to 1718 File Patients. (Doc. 355, Op. 20-25.)

Based on these findings, the FTC found LabMD's alleged failure to employ the Additional Security Measures "unfair" under Section 5. (Doc. 355, Op. 1, 16.)

Rather than addressing LabMD's purported Section 5 violation by directing LabMD to "cease and desist" that violation (the sole form of relief permitted by Section 5), the Order's relief provisions consist *entirely* of burdensome mandatory injunctive terms that are impossibly vague, not necessary to achieving a cessation of LabMD's allegedly unfair practice, and oblivious to the then circumstances of LabMD, which had ceased operations over two years earlier. Thus, the Order directs the now-defunct LabMD not to merely cease and desist from the practice it voluntarily discontinued over eight years before, but instead to, among other things, (i) establish and maintain a "reasonable" comprehensive information security program; (ii) obtain biennial assessments of its program compliance by an outside auditor; and (iii) notify the 1718 File Patients in a form approved by the FTC. (Doc. 355, Order 2-4.)

LabMD filed its instant petition on September 29, 2016 (Dkt. 9/29/2016) and subsequently moved this Court for a stay of the Order pending review. (Dkt. 10/7/2016 ("Stay Motion").) This Court granted LabMD's motion on November 10, 2016. (Dkt. 11/10/2016 ("Stay Opinion").) In granting the stay, the Court

observed that LabMD "has (at least) presented a serious legal question," because there are "compelling reasons why the FTC's interpretation" of Section 5 "may not be reasonable." Stay Opinion at 8. The Court explained that "it is not clear that a reasonable interpretation of ["substantial injury" under] § 45(n) includes intangible harms like those that the FTC found in this case." *Id.* The Court further held that it did "not believe" the FTC's reading of Section 5(n)'s word "likely" as including something that has a low likelihood "is reasonable." *Id.* at 10.

IV. STANDARD OF REVIEW

LabMD petitions under 15 U.S.C. § 45(c) and 5 U.S.C. § 706, and requests that the Court vacate the Order because (1) the Opinion and the Order are "not in accordance with law," exceed the authority of the FTC, and constitute "an abuse of discretion"; (2) there is a lack of substantial evidence to support the Opinion's factual findings; and (3) additional discovery should be taken to determine whether the Commission violated LabMD's constitutional rights. *See* 5 U.S.C. § 706(2); 15 U.S.C. § 45(c).

The Court reviews the Commission's legal conclusions and its application of the facts to the law *de novo*. *Polypore Int'l, Inc. v. F.T.C.*, 686 F.3d 1208, 1213 (11th Cir. 2012).[6] The FTC's findings of fact are reviewed under the "substantial evidence" standard. *Schering-Plough Corp. v. F.T.C.*, 402 F.3d 1056, 1062–63

[6] As described *infra* in Section I.A.1, no deference to the Commission's legal conclusions and applications is due here.

(11th Cir. 2005). "Substantial evidence" is "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Consolidated Edison Co. v. N.L.R.B.*, 305 U.S. 197, 229 (1938). However, the Court "may . . . examine the FTC's findings more closely where," as here, "they differ from those of the ALJ." *Schering-Plough*, 402 F.3d at 1062.

SUMMARY OF THE ARGUMENT

The Order should be vacated because it and the Opinion rest upon a plethora of erroneous legal conclusions and findings unsupported by substantial evidence.

As shown in Section I below, the Order must be vacated because the FTC's conclusion that LabMD violated Section 5 exceeded the FTC's unfairness authority. Specifically:

- The Opinion's contentions that "substantial" injury can include intangible injury and even purely conceptual injury, that "likely" injury can include improbable injury, and that a long-since discontinued practice nonetheless "is likely" to cause injury as long as it "was likely" to do so eight years earlier, each contravene the clear meaning of Section 5(n) (not to mention plain English and common sense).

- Additionally, the Commission misapplied the "countervailing benefits" prong of Section 5(n) by failing to conduct the cost-benefit test the FTC itself has acknowledged it must conduct.
- The Opinion also erroneously assessed LabMD's Section 5 culpability by using (a) the wrong legal standard, (b) the wrong sort of allegedly omitted security measures, and (c) the wrong methodology.
- The FTC further erred in bringing a data-security-based unfairness action against a medical facility like LabMD, because doing so creates clear repugnancy, as a matter of law, with federal healthcare legislation.
- The FTC in any event erred in enforcing against LabMD the interpretations that are the basis for its Section 5(n) and culpability analyses, because LabMD lacked fair notice of those interpretations as required by the Due Process Clause.

Section II below shows that the Order must be vacated for the independent reason that the Opinion lacked substantial evidence to support (1) its finding of "likely" consumer injury (even under the FTC's erroneous interpretation of that term), (2) its finding that LabMD's data security program omitted the Additional Security Measures, and (3) its finding that deployment of certain of the Additional

Security Measures would have reduced the likelihood of the 1718 File being stolen.

Section III below demonstrates that the Order's remedies are invalid even if the FTC properly found a Section 5 violation, because (1) the FTC did not (and could not have) concluded that there is a cognizable danger of LabMD committing the purported Section 5 violation again, (2) the Order consists entirely of affirmative relief that the FTC has no authority to impose, and (3) the Order is impermissibly vague.

Finally, as shown in Section IV below, this case raises serious questions of FTC misconduct on which LabMD was denied discovery below and that warrant vacating the Order so as to allow that discovery.

For all of these reasons, the Order must be vacated.

ARGUMENT

I. THE COMMISSION EXCEEDED ITS LEGAL AUTHORITY IN FINDING LABMD LIABLE FOR AN UNFAIR PRACTICE

It is well-established that "an agency literally has no power to act . . . unless and until Congress confers power upon it." *La. Pub. Serv. Comm'n v. F.C.C.*, 476 U.S. 355, 374 (1986). Moreover, "a fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *F.C.C. v. Fox Television Stations, Inc.*, 132 S. Ct. 2307,

2317 (2012). Here, the FTC violated both of these bedrock principles in finding LabMD liable for an unfair practice. The Order, accordingly, should be vacated.

A. The Opinion Sweeps Aside the Limits Congress Imposed on the Commission's Unfairness Authority By Means of Section 5(n)

In Section 5(n), Congress explicitly provided that the Commission "*shall have no authority*" to declare an act or practice "unfair" "*unless* the act or practice [1] causes or is likely to cause substantial injury to consumers[,] [2] which is not reasonably avoidable by consumers themselves[,] and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (emphasis added). The Commission's Opinion eviscerates several of these critical limits.

1. The Opinion Erred in Concluding that LabMD Caused "Substantial Injury"

In regard to Section 5(n)'s first prong, the Opinion did not find, nor could it have found, that the theft of the 1718 File caused any *tangible* consumer harm (meaning economic or physical injury). (Doc. 355, Op. 17.) To address this evidentiary gap, Part III.A.1 of the Opinion held that *intangible* harms, such as "embarrassment" and "reputational" harm, as well as the wholly conceptual "privacy harm" that the FTC found to be inherent in the mere theft of a consumer's personal information, are "substantial injury" under Section 5(n). (Doc. 355, Op. 17.) This holding was clear error.

First, the FTC's interpretation of "substantial injury" contravenes the term's plain meaning. As the Opinion concedes, the plain meaning of "substantial injury" as used by Congress when it enacted Section 5(n) in 1994 must be derived from the FTC's then-operative definition of "substantial injury" as set forth in the FTC's prior policy statements to Congress on this very question. (Doc. 355, Op. 9); *see United States v. Myers*, 972 F.2d 1566, 1572 (11th Cir. 1992) ("Congress is deemed to know the executive and judicial gloss given to certain language and thus adopts the existing interpretation unless it affirmatively acts to change the meaning."). And the FTC's pre-enactment policy statements make crystal clear that, as of the enactment of Section 5(n), the FTC defined "substantial injury" to require "tangible injury."

Specifically, the FTC's 1980 Policy Statement on Unfairness (the "Policy Statement"), Letter from FTC to Senators Ford and Danforth (Dec. 17, 1980), appended to *In re Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290, at *95 (1984), expressly stated in its discussion of the meaning of the term "substantial injury" that "[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair," Policy Statement, 1984 WL 565290, at *97, and then clarified that "emotional effects might possibly be considered as the basis for unfairness" *only* "where tangible injury could be clearly demonstrated." *Id.* at

*104 n.16.[7] Similarly, the FTC's 1982 policy letter clearly stated that, "as a general proposition"—*i.e.*, as a rule[8]—substantial injury "*does not cover* subjective examples of harm." Letter from FTC Chairman J.C. Miller, III to Senators Packwood and Kasten (March 5, 1982) ("Policy Letter"), reprinted in H.R. Rep. No. 156, pt. 1, 98th Cong., 1st Sess. 27, 32 (1983) (hereinafter cited by reference to H.R. Rep. No. 156).

Second, if the statute's plain meaning were not dispositive, the FTC's interpretation of "substantial injury" as including intangible injury is, as the ALJ recognized (Doc. 326, 69), directly at odds with Section 5(n)'s legislative history, which states in no uncertain terms that intangible injuries are not cognizable as "substantial injury" under Section 5(n). *See, e.g.*, S. Rep. 103-130, 1993 WL

[7] The Opinion's assertion that this footnote in the Policy Statement defines "substantial injury" to include "subjective types of harm" (Doc. 355, 10), thus represents a gross mischaracterization, as the footnote in fact says that some sort of "tangible" (meaning either economic or physical) consumer injury must *always* be present for the injury to be "substantial." The truth therefore is, as Commissioner Olhausen testified in 2012, that in the Policy Statement the Commission "specifically advised Congress that absent deception, it will not enforce Section 5 against alleged intangible harm." Stmt. of Commissioner Maureen K. Ohlhausen to Senate Committee on Commerce, Science & Transportation, 2012 WL 1612706 (May 9, 2012).

[8] A "general proposition" is a "universal proposition" or a "law of principle." Merriam-Webster Online Dictionary, 2016, http://www.merriam-webster.com/.

322671, at *13 (1993) ("Emotional impact and more subjective types of harm alone are not intended to make an injury unfair.").[9]

Even if intangible harm could be "substantial injury" under Section 5(n), moreover, the Opinion did not find LabMD caused any such harm here. While the Opinion suggested that a theft of personal information "*can* involve embarrassment or other negative outcomes, including reputational harm" (Doc. 355, Op. 17) (emphasis added), it makes no finding—and the FTC had no basis upon which to find—that any 1718 File Patient *actually* suffered any such intangible harm as a result of the 1718 File's theft. (Doc. 326, 52 ("Complaint Counsel presented no evidence of any consumer that has suffered . . . reputational injury, embarrassment, or any of the other injuries Complaint Counsel describes.").) Accordingly, even if intangible harm could qualify as substantial injury, which it cannot, the Opinion's conclusion that Tiversa's theft of the 1718 File caused substantial injury would still fail.

Finally, given that "substantial injury" does not even include intangible harm, it *a fortiori* cannot include the purely conceptual "privacy harm" the FTC

[9] Subsequent legislative enactments also make clear that "substantial injury" does not include intangible injury. *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015) (noting that the Gramm-Leach-Bliley Act, which the FTC enforces, "relieves some of the burdensome [Section 5(n)] requirements for declaring acts unfair" because it permits the FTC to establish standards protecting not only against "substantial harm," but also against "inconvenience" to consumers).

posited consumers suffer from the mere disclosure (and nothing more) of their personal information to an unauthorized third party. *See* Stay Opinion at 9 (agreeing that this alleged harm is "not even 'intangible'").

In opposing the Stay Motion, the FTC claimed its interpretation of "substantial injury" should be upheld based on "*Chevron* deference." (Dkt. 10/18/2016 ("Stay Opposition") at 11-12.)[10] The FTC is wrong.

The threshold *Chevron* deference question ("*Chevron* Step One") is "whether Congress has directly spoken to the precise question at issue." *Legal Envtl. Assistance Found., Inc. v. E.P.A.*, 276 F.3d 1253, 1257–58 (11th Cir. 2001) (quoting *Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842–43 (1984)). If "the intent of Congress is clear," no deference is due. *Id.* In determining whether congressional intent is clear, courts look to the statute's plain language, its legislative history, and prior agency interpretations. *PHH Corp. v. Consumer Fin. Prot. Bureau*, 839 F.3d 1, 41-49 (D.C. Cir. 2016) (relying on these factors to find statute unambiguous at *Chevron* Step One); *see also Miccosukee Tribe of Indians of Fla. v. United States*, 566 F.3d 1257, 1273 (11th Cir. 2009). Even if Congress's intent is not clear, moreover, a court only reaches *Chevron* Step

[10] In that briefing, the FTC did not claim to be owed deference as to any of its other Section 5 interpretations at issue on this appeal. *See* Stay Opposition at 11. Nor could the FTC claim (or prevail upon receiving) any such deference, as those interpretations are at odds with the plain language, the legislative history, and/or the FTC's prior interpretations of the statute, and in any event are unreasonable as shown in Sections I.A.2, I.A.3, I.B, and III below.

Two—determining whether an agency's interpretation is permissible—if Congress explicitly or implicitly demonstrated its intent to delegate authority to the agency to resolve the ambiguity. *See Josendis v. Wall to Wall Residence Repairs, Inc.*, 662 F.3d 1292, 1320 (11th Cir. 2011); *see also A.B.A. v. F.T.C.*, 430 F.3d 457, 469 (D.C. Cir. 2005) ("[A]mbiguity is not enough per se to warrant deference"). Upon reaching *Chevron* Step Two, a court finds the agency's interpretation permissible only if that interpretation is "reasonable" in light of the sources considered at *Chevron* Step One. *See PHH*, 839 F.3d at 50.

Applying these principles here, the FTC's interpretation of "substantial injury" is not entitled to *Chevron* deference. First, as set forth above, both the language and legislative history of Section 5(n) unambiguously convey Congress's intent that only tangible injuries can provide the basis for a finding of unfairness. And in any event, where Congress enacted Section 5(n) for the precise purpose of *limiting* the FTC's authority, *see* S. Rep. 103-130, 1993 WL 322671, at *12 (describing the 5(n) amendment as "limiting the FTC's authority"), Congress could not possibly have intended to authorize the FTC to adopt interpretations of Section 5(n) that write those limits out of existence.

Second, even if the Court reached *Chevron* Step Two, the FTC's interpretation of "substantial injury" is unreasonable, and hence impermissible, given the plain meaning and legislative history of the term. Stay Opinion at 8-9.

2. The Opinion Wrongly Holds that a Practice "Is Likely" to Cause Injury If the Injury "Was Possible" Eight Years Earlier

The Commission also acted contrary to law and beyond its jurisdiction in construing the "is likely" portion of Section 5(n)'s limitation that a practice may be found unfair only if it "causes or is likely to cause" the alleged substantial injury.

First, the Opinion concluded that a practice can be found "likely" to cause substantial injury where it merely creates "a significant risk of causing" that injury (*see* Doc. 355, Op. 21), and it then went even further by holding that a "significant risk" of injury can exist "even if the likelihood of the injury occurring is low," *id.* These holdings, which reduced beyond recognition Section 5(n)'s "is likely" limit on the FTC's authority, were in error.

"In interpreting the language of [a] statute, [the] Court must assume that Congress used the words of the statute as they are commonly and ordinarily understood[.]" *United States v. McLymont*, 45 F.3d 400, 401 (11th Cir. 1995) (per curiam). The plain meaning of "likely" is "having a high probability of occurring . . .[,] very probable," or "in all probability." Merriam-Webster Online Dictionary, 2016, http://www.merriam-webster.com/. Interpreting the term "likely" to include low probability events, as the Opinion does, thus contravenes its plain meaning. As the Court has already observed, one cannot "read the word 'likely' to include something that has a low likelihood." Stay Opinion at 10.

The Opinion sought to defend its interpretation by arguing that "the likelihood that harm will occur must be evaluated together with the severity or magnitude of the harm involved," and thus that even *unlikely* injury may be transformed into "likely" injury if "the magnitude of the potential injury is large." (Doc. 355, Op. 21.) While the FTC is correct that both likelihood and magnitude of injury must be considered, it fails to recognize that these are two *separate* requirements. As a matter of basic English grammar, the *severity* of a potential injury (while pertinent to Section 5(n)'s *separate* requirement that the injury at issue be "substantial") tells one nothing about whether the injury is *likely*.

The Opinion's interpretation that consumer injury is "likely" even where it has a "low" probability of occurring, as long as the magnitude of the injury would be "large," should be rejected not only because it flies in the face of the plain meaning of the word "likely," but also because it is incoherent and incapable of being objectively applied in practice. The Opinion provides no quantification of what magnitude of injury would be large enough to be "large" under the FTC's interpretation (as opposed to merely being "significant" or "medium" or something less than "large") or what the chances of an injury must be for the odds of its happening to be as least "low" under the FTC's interpretation (as opposed to its probability merely being "remote" or "a longshot" or something else less than "low"). In the absence of any such objective standard, the FTC's interpretation is

not a legal standard at all, but instead is an absurd "I-know-it-when-I-see-it" test that would allow the FTC to use the vacuous labels of "large" and "low" to justify whatever result it desires in any given case and make that result essentially unreviewable on appeal. *See In re Davis*, 565 F.3d 810, 823 (11th Cir. 2009) ("We cannot read statutory language in a way that renders it wholly meaningless or nonsensical."). Such an outcome would run directly counter to the congressional purpose of putting strict limitations on the FTC's Section 5 unfairness authority by means of Section 5(n). *See* S. Rep. 103-130, 1993 WL 322671, at *12 (describing Section 5(n) as "limiting the FTC's authority" and codifying "a statutory limitation on unfair acts and practices").

None of the sources cited in the Opinion supports its misreading of "likely." (*See* Doc. 355, Op. 21.) In *International Harvester*, a decision pre-dating Section 5(n), the FTC found conduct unfair based on *actual* injury, not *likely* injury—the product defect at issue had in several instances *already* resulted in "[s]erious injury and death" to consumers. 104 F.T.C. 949, 1984 WL 565290, at *83. In *Phillip Morris*, another pre-Section 5(n) case, there was no *adjudication* that any conduct was unfair. Instead, *Phillip Morris* involved a consent decree that did "not constitute an admission by respondents that the law has been violated." *In re Philip*

Morris, Inc., 82 F.T.C. 16, 1973 WL 165120, at *2 (1973).[11] The discussion of foreseeability in *Wyndham* is similarly unhelpful to the FTC's position, as it related solely to whether a business could commit an unfair act "when the business itself is victimized by criminals"—the court was not construing the statutory term "is likely." *Wyndham*, 799 F.3d at 246.

Second, the Opinion's interpretation of Section 5(n)'s "is likely" limitation is flawed for the independent reason that it focused on whether LabMD's conduct *was* likely (under the Opinion's erroneous interpretation of the term "likely"), at some distant point in the past, to cause consumer injury. (Doc. 355, Op. 20 ("LabMD's unauthorized exposure of the 1718 file *was* 'likely to cause substantial injury.'" (emphasis added)).) The Opinion never evaluated the *current* likelihood of LabMD's data security practices causing consumer harm. However, Section 5(n) plainly states that only a practice that causes or "*is* likely" to cause substantial injury may be declared unfair. The statute's use of the present tense makes clear that the FTC had no authority to declare LabMD's failure to employ the Additional Security Measures "unfair" on the basis of "likely" harm unless it could justifiably conclude *at the time it declared that failure unfair* (*i.e.*, the date of the Order) that LabMD *is* likely *at some point in the future* to cause substantial consumer injury

[11] In any event, *Philip Morris* did not involve a low probability harm of the sort the FTC found "likely" here: the company had been distributing unsolicited sample razor blades tucked into home-delivered newspapers, apparently without any warning of their presence. *Id.* at *3.

by failing to employ the Additional Security Measures. *See Medberry v. Butler*, 185 F.3d 1189, 1193 (11th Cir. 1999) (holding that "Congress' use of the present tense" in statute precluded prisoner from proceeding under "imminent danger" provision based on past danger).

Further, the remedial nature of Section 5 precludes the FTC's topsy-turvy "is"-means-"was" interpretation. Section 5 is a forward-looking provision concerned with remedying ongoing conduct that poses a *current* risk to consumers. *See New Standard Pub. Co. v. F.T.C.*, 194 F.2d 181, 183 (4th Cir. 1952) ("[Section 5] orders are entered, not as punishment for past offenses, but for the purpose of regulating present and future practices."). Where, as here, there is no evidence of substantial injury having occurred, and no evidence such injury *is* likely to occur going forward, there is nothing for the FTC to remediate by means of a cease-and-desist order, which is the *only* remedy available to the FTC in this type of case. Accordingly, it would be inconsistent with Section 5's remedial scope to read "is likely" to mean "was likely," even if basic English grammar permitted that reading.

3. The Commission Failed to Conduct the Cost-Benefit Analysis Required by Section 5(n)'s "Countervailing Benefits" Prong

By barring the FTC from declaring a practice "unfair" where any substantial consumer injury caused or likely to be caused by the practice is "outweighed by countervailing benefits to consumers or to competition," Section 5(n)'s

"countervailing benefits" prong "informs parties that the relevant inquiry [under that prong] is a cost-benefit analysis . . . that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." *Wyndham*, 799 F.3d at 255. In applying this prong, the FTC must also "take into account costs related to a prospective remedy, including but not limited to direct costs to the parties." Policy Letter at 32; *see* Policy Statement, 1984 WL 565290, at *97.

Here, then, Section 5(n) required the FTC to compare (1) the sum of (a) the costs of LabMD's implementing and maintaining the Additional Security Measures throughout the Relevant Period and (b) the additional costs associated with LabMD's compliance with the Order going forward (collectively, the "Relevant Costs"), with (2) the product of multiplying (a) the magnitude of any substantial consumer injury caused or likely to be caused by the 1718 File's being stolen during the Relevant Period by (b) the difference between (i) the probability of that injury occurring if LabMD had implemented the Additional Security Measures during that period and (ii) the probability of that injury occurring without those measures having then been implemented (the "Relevant Benefits").

The Commission made no attempt to undertake this required analysis, despite acknowledging that it was indeed required. (*See* Doc. 355, Op. 27 ("When

a case concerns the failure to provide adequate data security in particular, 'countervailing benefits' are the foregone costs of 'investment in stronger cybersecurity' by comparison with the cost of the firm's existing 'level of cybersecurity.'" (citing *Wyndham*, 799 F.3d at 255)).) For this reason alone the Order must be vacated. As to the Relevant Benefits, the FTC never quantified the *magnitude* of the substantial consumer injury caused or likely to be caused by a theft of the 1718 File during the Relevant Period, as required under *Wyndham*. The FTC also never quantified the *probability* of such a theft and consequent substantial consumer injury occurring first without, and then with, the Additional Security Measures being in place, as also required under *Wyndham*. 799 F.3d at 255 ("probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity" is "relevant factor" in Section 5(n) cost/benefit analysis).

Turning to the Relevant Costs, the Commission never quantified the total cost of implementing the Additional Security Measures throughout the Relevant Period. Instead, it cherry-picked a few of those costs—without totaling them—and declared without evidence or analysis that *all* of the Additional Security Measures could be implemented at "relatively low" cost. (Doc. 355, Op. 27-28.) "Relatively" compared to what is left unstated, and the Opinion conveniently side-stepped the most substantial costs the Additional Security Measures would have imposed upon

LabMD, namely the personnel costs of implementing, maintaining, and monitoring those measures on a day-in, day-out basis throughout the Relevant Period. (*See* Doc. 355, Op. 26-28.) Equally egregious, the FTC never quantified the costs LabMD would incur in complying with the Order, as the FTC previously conceded is required. *See* Policy Letter at 32; Policy Statement, 1984 WL 565290, at *97.

B. The Commission Evaluated LabMD's Section 5 Culpability Using the Wrong Culpability Standard, the Wrong Sort of Data Security Measures, and the Wrong Methodology

Beyond violating the specific limits of Section 5(n) in Part III of its Opinion, the Commission made independent errors in Parts I and II of the Opinion by impermissibly supplanting the culpability standard inherent in the "unfairness" prong of Section 5 with an "unreasonableness" test; by considering the wrong sort of data security measures in evaluating "unreasonableness"; and by using an inappropriate methodology to conclude that LabMD had "unreasonable" security measures in place to protect the 1718 File. For these independent reasons, the Order must be vacated.

First, the Commission applied the wrong culpability standard. By separately evaluating in Part II of the Opinion whether LabMD's data security practices were unreasonable, in addition to analyzing in Part III whether the three elements of Section 5(n) had been satisfied (*see* Doc. 355, Op. 11-16), the FTC tacitly conceded (indeed, it expressly stated at the end of Part I of the Opinion, *id.* at 11)

that the three prongs of Section 5(n) are insufficient on their own, and that an additional showing of culpability is required, for a practice to be declared "unfair." This concession is consistent with the text of the statute, its legislative history, the FTC's own prior interpretations of Section 5, and the Third Circuit's *Wynhdam* decision. By its express terms, Section 5(n) *limits* rather than defines the circumstances where the FTC may declare a practice "unfair," providing that "[t]he Commission shall have *no authority*" "*unless*" the stated prerequisites are met. (emphasis added). Indeed, imposing such a limitation was the express purpose of enacting Section 5(n). *See* H.R. Conf. Rep. 103-617, 11-12, 1994 WL 385368, at *11-12 (1994) (Section 5(n) was enacted "to *limit* unfair acts or practices to those that" satisfy the three prongs (emphasis added)); S. Rep. 103-130, 1993 WL 322671, at *13 (describing 5(n) as a "new subsection *limiting* the FTC's authority" (emphasis added)). Consistent with that history, the Commission itself has acknowledged that the consumer injury test is merely "*one of* the most crucial elements in finding an act or practice to be unfair." Policy Letter 32-33 (emphasis added).[12] *Wyndham* thus recognized that "[t]he three requirements in [Section] 45(n) may be necessary rather than sufficient conditions of an unfair practice." 799 F.3d at 259.

[12] The ALJ likewise recognized that Section 5(n) merely "establish[es] an outer limit to the Commission's authority to declare an act or practice unfair." Doc. 326, 89; *see also id.* at 48-49 (describing Section 5(n) as merely a "legal precondition to finding a respondent liable for unfair conduct").

While the FTC correctly recognized that something more than satisfaction of Section 5(n) is required, the Opinion erred in using "unreasonableness" as that something more. Instead, culpability under Section 5 requires a showing that the practice at issue was not merely negligent (*i.e.*, "unreasonable"), but instead involved more egregious conduct, such as deception or recklessness—namely, that the practice was "unfair." "The plain meaning of 'unfair' is 'marked by injustice, partiality, or deception.'" *LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1200 (11th Cir. 2010) (quoting Merriam-Webster Online Dictionary (2010)); *see Wyndham*, 799 F.3d at 245 (suggesting that, to the extent "these are requirements of an unfairness claim," such requirements were met based on defendant's allegedly deceptive statements); *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 496-97 (1st Cir. 2009) (analyzing unfairness under Massachusetts consumer protection statute, which incorporates "FTC criteria"; concluding that the statute covers only "egregious conduct"; and finding defendant's alleged "inexcusable and protracted reckless conduct" met the "egregious conduct" test). Here, the FTC made no finding that LabMD's failure to employ the Additional Security Measures was deceptive or reckless or otherwise involved conduct sufficiently culpable to be declared "unfair." The absence of any finding that LabMD's conduct fell within the definition of the term "unfair" rendered the FTC's Section 5 analysis fatally incomplete. This error alone requires that the Order be vacated.

Second, even if unreasonableness alone could satisfy Section 5's culpability requirement, the Commission's unreasonableness inquiry was fatally flawed because it considered the wrong sort of data security measures.

As an initial matter, LabMD's alleged failure to protect patient data related *only* to security for a single file on a single workstation, which file contained limited PHI as to barely 1% of the patients whose PHI LabMD was then protecting. Moreover, *no* data security risk was found as to any *other* portion of LabMD's network, or as to any of the nearly 750,000 *other* patients whose PHI LabMD was protecting, and as a result the Opinion nowhere claims that any of the Additional Security Measures would have ameliorated some such broader, network-wide data security risk. That being the case, *none* of the Additional Security Measures was or could have been found to address a "systemic" security deficiency. As a result, under the FTC's own articulated standards, *none* of them should have been taken into account in the FTC's reasonableness analysis. *See, e.g.*, *Identity Theft: Innovative Solutions For An Evolving Problem: Hearing Before the Subcomm. On Terrorism, Technology and Homeland Security of the S. Comm. on the Judiciary,* 110th Cong. 94 (2007) (statement of Lydia Parnes, Dir. Bureau of Consumer Protection, FTC) (noting that "multiple and *systemic*" deficiencies are the "common element[]" of FTC data breach actions).

Even if non-systemic deficiencies were relevant to the unreasonableness analysis, many of the Additional Security Measures nonetheless should have been excluded. Under the Commission's reading of Section 5, a company's failure to employ certain data security measures may be found "unfair" only if such failure both (1) was unreasonable and (2) causes or is likely to cause substantial consumer injury. (*See* Doc. 355, Op. 11 ("Thus, we evaluate [1] whether LabMD's data security practices, taken together, failed to provide reasonable and appropriate security for the sensitive personal information on its computer network, and [2] whether that failure caused or was likely to cause substantial consumer injury . . . .").) This necessarily means that in any given case the Commission's reasonableness inquiry must be strictly limited to those data security measures that, had they been employed, would have either prevented or made unlikely the consumer injury in question.

But the Commission did not so limit itself in this case. Here, the Opinion found that LabMD violated Section 5 *only* in regard to the 1718 File and *only* by supposedly failing to protect that file against the P2P vulnerability. The Opinion concedes, moreover, that 1718 File was only subject to the P2P vulnerability during the *eleven-month* period from June 2007 to May 2008. Yet the Opinion, unaccountably and without explanation, evaluates the "reasonableness" of LabMD's security based on whether LabMD lacked the Additional Security

Measures at any point during the *seventy-two-month* period from *January 2005 through December 2010*. (Doc. 355, Op. 12-16.) Moreover, this analytical flaw was no mere foot-fault, because as to many of the Additional Security Measures, including firewall deployment, anti-virus management, training, and network monitoring, the record evidence on which the Commission purported to make an out-of-place finding did not support a finding that the measure in question was lacking during the Relevant Period.

Timeframe issues notwithstanding, as to many of the Additional Security Measures (specifically, LabMD's alleged failure to appropriately deploy password controls, antivirus, firewalls, network monitoring, intrusion detection, and penetration testing systems (Doc. 355, Op. 2, 12-13)), even assuming the Opinion had a basis upon which to find that LabMD did not deploy the measure during the eleven months at issue, the Opinion never found, and could not have found, that LabMD's deployment of the measure during that period would have in turn enhanced the protection of the 1718 File against the P2P vulnerability.[13] This was fundamental error—akin to a court deciding a tort case by finding negligence

[13] Indeed, the Commission's own expert acknowledged that the P2P vulnerability would not have been prevented by the anti-virus measures the Opinion faults LabMD for failing to employ (CX0740, ¶ 65) and that alternatively configured firewalls would not have protected the 1718 File against the P2P vulnerability. (CX0737, 5 ¶13.)

based on acts that had not been shown to have caused or contributed to the injury being complained of.

It is, moreover, no answer for the Commission to argue that *some* of the Additional Security Measures *were* out of place during those eleven months, and *would* have enhanced the security of the 1718 File against the P2P vulnerability had they been in place at that time. The Opinion only found LabMD's data security to be unreasonable based on *all* of the Additional Security Measures, "taken together," allegedly having been out of place. (Doc. 355, Op. 11.) Its unreasonableness conclusion, therefore, necessarily falls apart when *even one* of those measures should have been excluded from the unreasonableness analysis as being temporally or causally irrelevant.

Third, the Commission applied the wrong methodology for evaluating "unreasonableness." Any regime that purports to hinge the *lawfulness* of an actor's conduct on the *reasonableness* of the actor's conduct must evaluate, at an absolute minimum, the costs and benefits of that conduct. *See Am. Petroleum Inst. v. O.S.H.A.*, 581 F.2d 493, 503 (5th Cir. 1978) ("The only way to tell whether the relationship between the benefits and costs of the [applicable] standard is reasonable is to estimate the extent of the expected benefits and costs,"), *aff'd sub nom. Indus. Union Dep't v. Am. Petroleum Inst.*, 448 U.S. 607 (1980); *Int'l Union, United Auto., Aerospace & Agr. Implement Workers of Am. v. O.S.H.A.*, 938 F.2d

1310, 1319 (D.C. Cir. 1991) ("'Reasonableness' has long been associated with the balancing of costs and benefits." (citing *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947))). Accordingly, numerous statutory regimes, including those in the consumer protection context, incorporate cost-benefit analysis into the evaluation of reasonableness. *See, e.g.*, *Aqua Slide 'N' Dive Corp. v. C.P.S.C.*, 569 F.2d 831, 839-40 (5th Cir. 1978) (Consumer Product Safety Act); *see also Felix v. N.Y. City Transit Auth.*, 324 F.3d 102, 110 (2d Cir. 2003) (Americans with Disabilities Act); *BNP Paribas Energy Trading GP v. F.E.R.C.*, 743 F.3d 264, 267–68 (D.C. Cir. 2014) (rates for the transportation and sale of natural gas); *Texas Indep. Ginners Ass'n v. Marshall*, 630 F.2d 398, 410–11 (5th Cir. 1980) (occupational health standards).

No exception exists here. Indeed, FTC Commissioners themselves have acknowledged that a cost-benefit analysis is integral to any analysis of reasonable data security. *See, e.g.*, Remarks of FTC Commissioner Maureen K. Ohlhausen Before the Congressional Bipartisan Privacy Caucus, 2014 WL 585465, at *2 (Feb. 3, 2014) (noting that in each investigation of reasonableness, the Commission "examines . . . the costs and benefits of implementing various protections"). And the Opinion itself echoed Commissioner Ohlhausen's acknowledgement, conceding that the "cost-benefit" approach to Section 5 described in *Wyndham* "dovetails with the analysis the Commission has consistently employed in its data

security actions, which is encapsulated in the concept of '*reasonable*' data security." (Doc. 355, Op. 11 (emphasis added).) Yet, despite recognizing that a cost-benefit analysis is required, Part II's analysis of the *legal* reasonableness of LabMD's data security measures, and its alleged failure to deploy the Additional Security Measures, conducted no such analysis. Moreover, as discussed above, the cost-benefit analysis the Commission conducted later in its Opinion was woefully deficient even for purposes of satisfying the third prong of Section 5(n) (*see supra* Section I.A.3), and hence did not approach the cost-benefit analysis required to establish the *legal* unreasonableness of a party's conduct.

Rather than conduct the required cost-benefit analysis, the Opinion relied on findings that certain (but by no means all) of the Additional Security Measures were available and used by IT practitioners. (Doc. 355, Op. 12-13 (referencing purportedly "common" practices among "IT practitioners").) An analysis of other companies' practices cannot substitute for a proper cost-benefit analysis, however. And even if such evidence were relevant in the context of a *legal* reasonableness inquiry, the issue would be not whether the evidence established that other entities employed the measures in question (which is what the FTC purported to show), but rather whether evidence established that those measures were *industry standard* or *industry custom* at the relevant time. *See, e.g.*, *Silverpop Sys., Inc. v. Leading Market Techs.*, 641 F. App'x 849, 852 (11th Cir. 2016) (industry custom); *S.E.C. v.*

Dain Rauscher, Inc., 254 F.3d 852, 856 (9th Cir. 2001) (industry standard); *Griggs v. Firestone Tire & Rubber Co.*, 513 F.2d 851, 862 (8th Cir. 1975) (industry custom). Here, no finding was made or could have been made that any of the Additional Security Measures was not merely "commonly used," but was in fact "industry standard" or "industry custom" (*i.e.*, conduct "generally accepted" as representing the expected level of conduct within the relevant industry), during the Relevant Period. *See, e.g., Johnson v. Manitowoc Boom Trucks, Inc.*, 484 F.3d 426, 434 (6th Cir. 2007).[14]

C. The Commission's Overreach Is Repugnant to Comprehensive Federal Healthcare Regulation

Even if Section 5 otherwise provided the Commission with authority to find LabMD's data security practices "unfair" (which it does not), the FTC still lacked authority to do so here if its assertion of such authority against LabMD is "repugnant" to Congress's grant to the U.S. Department of Health and Human Services ("HHS") of the authority to regulate the data security practices of medical laboratories like LabMD. *See Credit Suisse Sec. (USA) LLC v. Billing*, 551 U.S. 264, 271, 275 (2007). Whether the requisite "repugnancy" exists hinges on the

[14] Moreover, there is no evidence in the record regarding practices used, much less industry custom in the healthcare industry, let alone among small laboratories like LabMD. The Opinion's only references to practices in the healthcare industry is a National Research Council report (the "NRC Report") (Doc 355, Op. 12 n.23), which is not in the record. In any event, the NRC Report itself states that "it is not intended to serve as a benchmark for the industry." NRC Report at 168.

following factors: (1) the existence of regulatory authority to supervise the activities in question; (2) evidence that the responsible regulatory authority exercises that authority; (3) "a resulting risk" of "conflicting guidance, requirements, duties, privileges, or standards of conduct;" and (4) "the possible conflict affect[s] practices that lie squarely" within the area of conduct covered by the regulatory authority. *Id.* at 275-76. Each factor is satisfied here. The Order, accordingly, must be vacated under *Billing*.

First, similar to *Billing*, Congress has expressly granted HHS "considerable power to forbid, permit, encourage, discourage, tolerate, limit, and otherwise regulate virtually every aspect of the practices" employed by HIPAA-covered entities. *Id.* at 276. Congress enacted HIPAA in 1996 as a comprehensive overhaul of the healthcare system intended, among other things, to enhance the "efficiency and effectiveness of the health information system."[15] To accomplish Congress's objectives, HIPAA delegated HHS broad discretion to promulgate the first-ever comprehensive standards in the healthcare industry across a wide array of topics, including data security. 42 U.S.C. § 1320d-2.

Second, as in *Billing*, HHS has "continuously exercised its legal authority" under HIPAA, *see* 551 U.S. at 277, promulgating and actively enforcing the

[15] HIPAA § 261, Pub.L. 104–191, 110 Stat. 1936 (codified at 42 U.S.C. § 1320d notes).

required standards, including the Privacy Rule (45 C.F.R. §§ 164.500-534), Security Rule (§§ 164.302-318), and Breach Notification Rule (§§ 164.400-414).[16]

Regarding the third and fourth *Billing* factors, the FTC's use of Section 5 to impose data security obligations on LabMD creates both actual and potential "conflicting guidance, requirements, duties, privileges . . . or standards of conduct" that "lie squarely" within the healthcare field regulated by HIPAA, *Billing*, 551 U.S. at 275-76, as the Commission has conceded by repeatedly asserting that compliance with HIPAA is not sufficient to satisfy a company's data security obligations under Section 5.[17] The FTC's enforcement history underscores this acknowledged conflict. For example, the FTC's focus on imposing maximum retention periods for consumer information (Doc. 355, Op. 1, 15) ignores that both HIPAA and its implementing regulations contain only *minimum*—not *maximum*—retention requirements, *see* 45 C.F.R. § 164.530(j)(2) (providing that designated record sets must be retained for at least six years), and expressly contemplate

[16] Enforcement Results by Year, Department of Health & Human Services, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#resol2014 (last visited Dec. 21, 2016) (referencing more than 100,000 HIPAA-related investigations); HHS.gov Enforcement Highlights as of October 31, 2016, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (referencing collection of $48 million in civil penalties).

[17] Doc. 147, 5 (citing Doc. 48, 11, 13).

retention for as long as fifty years after a patient is deceased.[18] The FTC's objective of disincentivizing record retention is ill-suited for the healthcare industry, where the diagnostic utility of data accrues over time and can be the difference in life-saving treatment.

In short, the FTC's attempt to impose prescriptive data security obligations on companies like LabMD is repugnant to Congress's actual grant of that authority, in the healthcare area, to HHS, and the Order thus must be vacated.

D. Even if Otherwise Permissible, FTC Could Not Impose Its Novel Interpretations of Section 5 on LabMD, Which Lacked Fair Notice of Those Interpretations Under the Due Process Clause

Even if the FTC's interpretations of its Section 5 authority were otherwise permissible, the Commission could not apply them to LabMD based on its alleged failure to implement the Additional Security Measures, because back in June 2007 to May 2008—the only relevant time period in this case—LabMD did not have fair notice the FTC would adopt these interpretations over eight years later.

1. The Opinion's "Unreasonableness" Finding Violates Due Process

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *F.C.C. v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). The fair notice doctrine "prevents . . . deference from validating the application of a

[18] 45 C.F.R. §164.524(e); 45 C.F.R. §164.502(f); *see also* 42 C.F.R. § 493.1105.

regulation that fails to give fair warning of the conduct it prohibits or requires." *Gates & Fox Co., Inc. v. O.S.H.R.C.*, 790 F.2d 154, 156 (D.C. Cir. 1986). Moreover, where a court defers to an agency interpretation of its governing statute or its own regulation, and based on that interpretation the agency proposes to hold a party liable, the Due Process Clause requires that the agency's interpretation must have been knowable with "ascertainable certainty" at the time the party committed the alleged violation. *See Ga. Pac. Corp. v. O.S.H.R.C.*, 25 F.3d 999, 1005–06 (11th Cir. 1994). This means that, "by reviewing the regulations and other public statements issued by the agency, a regulated party acting in good faith would be able to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform." *Howmet Corp. v. E.P.A.*, 614 F.3d 544, 553–54 (D.C. Cir. 2010).

Here, were the Court to uphold the FTC's interpretation that Section 5 required LabMD to implement the Additional Security Measures in order to have data security "reasonably designed" to protect the 1718 File against the P2P vulnerability, it necessarily would be deferring to the FTC in doing so, given that the agency's "unreasonableness" analysis did not rely upon any existing legal standard beyond what the Commission itself had fashioned. Here, then, the Order must be vacated on fair notice grounds unless the FTC's public statements enabled LabMD, in June 2007, to know with ascertainable certainty that the FTC read

Section 5 as requiring LabMD to adopt the Additional Security Measures. *See Wyndham*, 799 F.3d at 251.

The Opinion asserts that certain Consent Decrees the FTC entered into in 2005 through 2008 gave LabMD "fair notice" that nearly 10 years later the FTC would interpret Section 5 as having required LabMD, back in June 2007, to deploy the Additional Security Measures to protect the 1718 File against the P2P vulnerability. (Doc. 355, Op. 30 n.81.) This assertion is patently absurd. To begin with, as a matter of law consent decrees cannot provide parties with fair notice, for Due Process Clause purposes, of an agency's interpretation of its governing statute or one of its regulations. As the Court in *Wyndham* recognized, "consent orders, which admit no liability and which focus on prospective requirements on the defendant, [would have been] of little use to [LabMD] in trying to understand the specific requirements imposed by § 45(a)," and it "may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees" in search of data security standards to illuminate the meaning of Section 5. *Wyndham*, 799 F.3d at 257 nn.22-23.

Moreover, even if consent decrees were legitimate sources of fair notice, many of the Additional Security Measures (specifically, anti-virus, file integrity monitoring, penetration testing, employee training, security-related manual inspections, and restricting employee downloads) are not mentioned in *any* of the

consent decrees cited in the Opinion (including the two decrees that post-dated the Relevant Period and hence are irrelevant in any event, *In re Reed Elsevier, Inc. & Seisint, Inc.*, No. C-4226, 2008 WL 3150420 (F.T.C. July 29, 2008) and *In re TJX Cos., Inc.*, No. C-4227, 2008 WL 3150421 (F.T.C. July 29, 2008)), and none of those consent decrees comes anywhere close to stating that a company like LabMD must employ each and every one of the Additional Security Measures to protect files like the 1718 File.

The fair notice deficiencies of the consent decrees are not cured by the "substantial public guidance" the FTC supposedly provided by means of a guidebook published in 2007 and a press release issued in 2004. (*See* Doc. 355, Op. 30 n.81.) As an initial matter, the FTC only relies on the guidebook *Protecting Personal Information: A Guide for Business* (2007) as a source of notice for a select few of the Additional Security Measures, while ignoring that the guidebook never mentions several of the very same Additional Security Measures that are absent from the consent decrees (file integrity monitoring, security-related manual inspections, and penetration testing) and describes others (such as intrusion detection systems and additional firewalls) merely as measures a company may want to "consider" (*see id.* at 14-15). More importantly, the whole tenor of the guidebook, as it states on its first page, is that companies should safeguard personal information not because Section 5 requires them to, but rather because it "is just

plain good business" to do so. (*Id.* at 1.) Thus, the guidebook merely says that Section 5 "*may require* [businesses] to provide reasonable security for sensitive information" (*id*. at 7)—it never says reasonable security for such information, or any particular security practice or combination thereof, *is required*. As the *Wyndham* court noted when analyzing this same document, because "the guidebook does not state that any particular security practice is required by [Section 5]," 799 F.3d at 256, "the guidebook could not, on its own, provide 'ascertainable certainty' of the FTC's interpretation of what specific cybersecurity practices fail" the unfairness test. *Id.* at 256 n.21.

Turning to the press release, this document cannot conceivably be viewed as a legitimate source of fair notice because—even more than the consent decrees the *Wyndham* court suggested were illegitimate sources, *see Wyndham*, 799 F.3d at 257 n.23—it would be unfair to expect parties to have looked to press releases, which are not legal documents, in search of guidance about the FTC's expectations as to the data security measures required to comply with Section 5. In any event, the press release, which the FTC relies upon only as a source of notice regarding installation of file-sharing programs, merely recommends that companies "consider" prohibiting employees from installing file-sharing programs on their computers—it nowhere states that Section 5 *legally obliges* that prohibition.

(CX0771.) And, in point of fact, LabMD *did* prohibit employees from doing that. (CX0001-02.)

2. The Opinion's Other Novel Interpretations of Section 5 Also Violate Due Process

In its Stay Opposition, the FTC claimed to be entitled to deference on only one of its interpretations of Section 5 at issue in this appeal: namely, its interpretation of the Section 5(n) term "substantial injury." And as shown above in Section I.A.1, no deference to the FTC is warranted on this interpretation, and deference would not save this interpretation even were it granted. But should the Court defer to the FTC's interpretation of this term and uphold that interpretation based on having accorded it such deference, the Court must in that event hold that the FTC failed to provide LabMD with fair notice of that interpretation in violation of the Due Process Clause, because prior to the beginning of the Relevant Period in 2007 the FTC had never provided LabMD with any ability to know with "ascertainable certainty" of the FTC's interpretation that intangible and even purported conceptual consumer injuries can constitute "substantial injury." *See Ga. Pac.*, 25 F.3d at 1005–06; *Gen. Elec. Co. v. E.P.A.*, 53 F.3d 1324, 1330 (D.C. Cir. 1995); *PMD Produce Brokerage Corp. v. U.S.D.A.*, 234 F.3d 48, 54 (D.C. Cir. 2000). Indeed, as shown in Section I.A.1, as of 2007, the FTC had consistently publicly stated *the exact opposite*.

Similarly, if the FTC were to request, and this Court were to grant, deference on any of the other FTC Section 5 interpretations at issue in this appeal, and were the Court to uphold any such FTC interpretation based on having accorded it such deference, the Court must in that event hold that the FTC failed to provide LabMD with fair notice of that interpretation prior to June 2007, in violation of the Due Process Clause, because prior to the beginning of the Relevant Period in June 2007 the FTC had *never* provided LabMD with the ability to know with "ascertainable certainty" any of the other FTC interpretations of Section 5 at issue on this appeal.

II. THE OPINION IS UNSUPPORTED BY SUBSTANTIAL EVIDENCE

The Order should be vacated for the additional reason that the Opinion is unsupported by substantial evidence, because many of its findings do not rely on "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Consolidated Edison Co. v. N.L.R.B.*, 305 U.S. 197, 229 (1938).

First, even if the Court accepts the FTC's incorrect interpretation that "likely" injury includes injury that has a "low" probability but a "large" magnitude (*see* Section I.A.2 *supra*), the FTC did not establish, and there is nothing in the record that would have provided a basis for it to have established, (1) the percentage probability of any claimed potential substantial injury (whether tangible or intangible)—leaving no basis upon which the FTC could find that probability high enough to be at least "low"—or (2) the dollar magnitude of any such injury—

leaving no basis upon which the FTC could find that magnitude high enough to be "large." *See Gulf S. Insulation v. C.P.S.C.*, 701 F.2d 1137, 1148 (5th Cir. 1983) ("The failure to quantify the risk . . . actually associated with [a practice] is the finding's Achilles heel.").

Second, the FTC's finding that LabMD failed to employ the Additional Security Measures was unsupported by substantial evidence. Specifically, as to many of the Additional Security Measures, the Opinion's not-in-place finding ignored, without explanation, a host of evidence establishing that LabMD in fact did have the measure in place. In particular, the FTC ignored (1) LabMD's letters to the FTC explaining its network architecture and security measures generally,[19] (2) evidence regarding LabMD's security policies and training practices,[20] (3) testimony and documents regarding LabMD's antivirus tools,[21] (4) expert testimony regarding LabMD's network security measures,[22] (5) evidence that LabMD's access practices were necessary for LabMD employees to perform their job functions,[23] (6) LabMD's network configuration, including the ZyWALL

[19] CX0443-44; CX0446-47.
[20] CX0001; CX0733, 79:17-24, 230:9-15; CX0536, 9-17.
[21] CX0733, 89:2-90:6, 113:5-22, 143:1-10, 166:5-20; Tr. 15, 127:6-14; CX0395.
[22] RX0533, 16-26.
[23] Tr. 10, 101:7-9; Tr. 11, 73:23-74:9; RX0533, 22-23.

IPSec 5 firewall and the Cisco router/firewall,[24] and (7) LabMD's security-related walk-arounds and manual inspections.[25] *See Schering-Plough*, 402 F.3d at 1070 (substantial evidence review "most certainly includes . . . the overwhelming evidence that contradicts the Commission's conclusion."); *McCruter v. Bowen*, 791 F.2d 1544, 1548 (11th Cir. 1986) ("It is not enough to discover a piece of evidence which supports that decision, but to disregard other contrary evidence."); *Cinderella Career & Finishing Schools, Inc. v. F.T.C.*, 425 F.2d 583, 585 (D.C. Cir. 1970) (The Commission "may not choose to ignore completely the testimony adduced at the hearing.").

The FTC's unexplained decision to ignore all this contrary, directly-on-point evidence is made all the more egregious by the Commission's concomitant decision, instead, to base its not-in-place findings on testimony from employees who were not employed by LabMD during the Relevant Period[26] (and therefore could not testify as to LabMD's practices at that time) and others who were deposed without LabMD's counsel being present (which testimony in one case the

[24] CX0034; CX0603 (depicting firewall blocking rules); Tr. 8, 129:15-17 ("[LabMD's firewall] appeared to be a commercial grade."); CX0630; CX0626; CX0733, 155: 6-12 (logs monitored daily).
[25] CX0004; CX0447; CX0482.
[26] The Commission extensively relies on testimony from Brandon Bradley, Jeremy Dooley, Matthew Bureau, Robert Hyer, and Patrick Howard (*see, e.g.*, Doc. 355, 12-13 nn.30, 36, 40), none of whom were employed during the Relevant Period. (Doc. 124, Ex. 2, 1-5 ¶¶ 2, 4, 6, 11, 13.)

ALJ expressly and correctly found deserved little weight).[27] *Brown v. Barnhart*, 390 F.3d 535, 540 (8th Cir. 2004) (discounting deposition testimony taken without opposing counsel); *Parker v. Bowen*, 788 F.2d 1512, 1521 (11th Cir. 1986) ("The notion that special deference is owed to a credibility finding by a trier of fact is deeply imbedded in our law.").

Third, even as to the limited sub-set of Additional Security Measures as to which the FTC found that the measure both was not deployed during the Relevant Period and would have enhanced the security of the 1718 File against the P2P vulnerability had it been deployed (*see* Section I.B *supra*), the FTC's findings are unsupported by substantial evidence. In particular, the FTC's findings that additional employee training and employee access controls would have enhanced the security of the 1718 File (Doc. 355, Op. 14, 16) are not supported by *any* reference to the record, and the FTC's assertion that file integrity monitoring would have done so (Doc. 355, Op. 13-14) references an expert who merely opines that file integrity monitoring "might have" aided detection of the application containing the P2P vulnerability. (CX0740, 45 ¶ 105b.) "[C]onjecture is not a substitute for substantial evidence." *Vera-Villegas v. I.N.S.*, 330 F. 3d 1222, 1231 (9th Cir. 2003).

[27] Curt Kaloustian (CX0735) and Alison Simmons (CX0734) were both deposed without LabMD counsel present. *See also* Tr. 32, 9:8-10:8.

III. THE ORDER'S REMEDIES AND RELIEF ARE INVALID EVEN ASSUMING THE OPINION VALIDLY FOUND A SECTION 5 VIOLATION

Even if the Opinion properly found that LabMD violated Section 5, this Court must set aside the Order if its remedies and relief are "in excess of statutory . . . authority, or limitations." 5 U.S.C. § 706(2)(C). They are.

A. There Was No Basis for Entry of *Any* Order

In administrative proceedings, the FTC is only authorized to order that a party "cease and desist from . . . [the] act or practice" found to be "prohibited by" Section 5. 15 U.S.C. § 45(b); *see Heater v. F.T.C.*, 503 F.2d 321, 324 (9th Cir. 1974) ("Congress limited the consequences of violation[s] of the Act to a cease and desist order."). Moreover, "[t]he commission is not [even] authorized to issue a cease and desist order as to practices long discontinued, and as to which there is no reason to apprehend renewal." *F.T.C. v. Civil Serv. Training Bureau, Inc.*, 79 F.2d 113, 115-16 (6th Cir. 1935). Such orders are thus unjustified when there is no "cognizable danger" of a recurrent violation, and "cognizable danger" requires more than a "mere possibility" of recurrence. *United States v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953); *see also TRW, Inc. v. F.T.C.*, 647 F.2d 942, 954 (9th Cir. 1981) ("[W]hile we cannot say that it is 'absolutely clear' that repetition will not occur, we can and must say there is simply nothing to suggest a 'cognizable

danger' of repetition[.]"); *Borg-Warner Corp. v. F.T.C.*, 746 F.2d 108, 110-12 (2d Cir. 1984) (same).

Here, at most, the Commission showed a theoretical possibility that LabMD may—one day in the future—resume business operations and, if it does, resume the practices the Commission found to be unfair. (*See* Doc. 355, Op. 36.) Such a theoretical possibility, standing alone, does not come anywhere near establishing the necessary "cognizable danger" of recurrence, especially where LabMD had fully remediated the single workstation at the core of the Commission's unfairness finding long before the FTC even began its investigation (*see* Doc. 326, 25-26 ¶¶ 88-99 (P2P vulnerability eliminated from workstation in May 2008)) and in any event had ceased operations entirely two years before the Order entered. The FTC thus abused its discretion in entering *any* order in this case. *See TRW*, 647 F.2d at 954 (setting aside orders where violations were neither egregious nor blatant, and the unlawful practice was discontinued before notice of FTC investigation).

B. The Order's Affirmative Relief Is Inappropriate

In administrative proceedings, a cease-and-desist order may include ancillary affirmative relief[28] only in unique situations, *e.g.* deceptive advertising, where some affirmative action must *necessarily* be taken in order for the party to

[28] Here, of course, the Order includes no cease-and-desist order at all and thus no relief as to which the Order's affirmative relief might be thought to be "ancillary." Indeed, LabMD is unaware of any court ever upholding an FTC order that—like the Order—consists *exclusively* of affirmative relief.

cease and desist from the relevant practice. *See Warner-Lambert Co. v. F.T.C.*, 562 F.2d 749, 759-761 (D.C. Cir. 1977); *see also Heater*, 503 F.2d at 323 n.7 (noting affirmative relief in cases involving corrective advertising for deceptive practices, divestiture for antitrust violations, and patent licensing agreements for monopolistic behavior). Here, LabMD could cease and desist its purported failure to employ the Additional Security Measures to protect the 1718 File against the P2P vulnerability by eliminating the P2P vulnerability from the one workstation at issue (which it did over eight years ago, in May 2008, Doc. 326, 25-26 ¶¶ 92-99) or for that matter by disconnecting its network and going out of business (which it did nearly three years ago, in January 2014, *id.* at 19-20 ¶¶ 36-41). LabMD thus did not *necessarily* have to take any affirmative action to cease and desist from the practice the FTC found unlawful here. That being the case, the Order is invalid in its entirety, because it consists entirely of impermissible affirmative relief.

Moreover, because the FTC is only authorized to issue cease-and-desist orders, and hence is not authorized to order consumer redress, the FTC may not issue consumer notification orders in cases where only unfairness is alleged. *See Barrett Carpet Mills, Inc. v. C.P.S.C.*, 635 F.2d 299, 301-02 (4th Cir. 1980); *Congoleum Indus., Inc. v. C.P.S.C.*, 602 F.2d 220, 225-26 (9th Cir. 1979) (citing *Heater* and finding no authority under Section 5 to order consumer notification).

The notification requirement in Part III of the Order is therefore invalid for the separate reason that it constitutes impermissible consumer redress.

C. The Order Is Impermissibly Vague

FTC orders must be, "at the outset, sufficiently clear and precise to avoid raising serious questions as to their meaning and application" by those against whom they are directed. *F.T.C. v. Henry Broch & Co.*, 368 U.S. 360, 367-68 (1962); *see also F.T.C. v. Colgate-Palmolive Co.*, 380 U.S. 374, 392 (1965). The crucial terms of the order should be "as specific as the circumstances will permit." *Colgate-Palmolive*, 380 U.S. at 393. Thus, the FTC's own Operating Manual states that orders "must set forth specific standards so that the proscribed conduct can be readily demonstrated to secure enforcement." FTC Operating Manual, Ch. 5 § .1.

The Order's instruction in Part I that LabMD establish a "reasonably designed" information security program does not specify the data security measures that constitute a "reasonably designed" information security program. The Commission itself has admitted as much; specifically, in touting the inherent "flexibility" in the Order, the FTC agreed that the Order does *not* specify "how precisely to meet [its] requirements." (Doc. 370, 6.) Nor has the FTC separately specified how to meet those requirements. Because the Order is by the FTC's own admission not "sufficiently clear and precise to avoid raising serious questions as to [its] meaning and application," *see Henry Broch*, 368 U.S. at 367-68, it is

impermissibly vague. *See Asheville Tobacco Bd. of Trade, Inc. v. F.T.C.*, 294 F.2d 619, 627-29 (4th Cir. 1961) (FTC order requiring "reasonable" practices is unenforceable because it is too vague and indefinite to enable the subject to prospectively determine the correct course of action); *see also Belle Maer Harbor v. Charter Twp. of Harrison*, 170 F.3d 553, 558 (6th Cir. 1999) (same in context of city ordinance); *In re Metro-East Mfg. Co.*, 655 F.2d 805, 810-11 (7th Cir. 1981) (same in context of OSHA regulation).

IV. THIS ACTION RAISES SERIOUS ISSUES OF FTC MISCONDUCT THAT, AT A MINIMUM, REQUIRE FURTHER DISCOVERY

Section 5(c) permits this Court to order the taking of additional evidence where "such additional evidence is material and . . . there were reasonable grounds for the failure to adduce such evidence in the proceeding before the Commission." 15 U.S.C. § 45(c); *Texaco, Inc. v. F.T.C.*, 301 F.2d 662, 663 (5th Cir. 1962) (per curiam). In the proceedings below, LabMD sought evidence regarding the FTC's investigation, its relationship with Tiversa, and its receipt of the 1718 File, that could have materially supported LabMD's defenses based on the Fourth and First Amendments—but the ALJ denied those requests. (Doc. 49, 2, 5-7; Doc. 62, 2, 4-5; Doc. 65, 2-5.) In so doing, however, the ALJ explicitly stated that "limiting [LabMD's] discovery . . . does not prejudice [its] ability to pursue its claim at a later phase of the case" because "the FTC Act expressly authorizes *a court of appeals* to order that the Commission take additional evidence." (Doc. 62, 4 n.3

(emphasis added); *see also* Doc. 65, 7 n.4.) LabMD now seeks from this Court that very discovery. Given LabMD's prior efforts to obtain that discovery and the ALJ's reasoning in denying that discovery, LabMD's inability to adduce the evidence in the proceedings below is clearly reasonable. *See, e.g.*, *Swinick v. N.L.R.B.*, 528 F.2d 796, 800-01 (3d Cir. 1975). And, as described below, the discovery is highly material to LabMD's constitutional defenses.

Late in the proceedings, through the whistleblower testimony of a former Tiversa employee provided with immunity by the Justice Department, LabMD was able to develop a limited record regarding the FTC's relationship with Tiversa prior to the early 2008 theft of the 1718 File. Even this limited record strongly suggests a level of collaboration that may have violated the Fourth Amendment. The record states that the FTC and Tiversa began communicating with some frequency around September 2007 regarding Tiversa's business model of using the P2P vulnerability to steal personal information from unsuspecting companies. (Doc. 326, 30-31 ¶¶ 133-138.) During in-person meetings, "[Tiversa] would present [its] technology to . . . the representatives from the FTC, and they would evaluate whether or not they could use it." (Tr. 51, 1435:3-5; *see also id.*, 1434:8-1436:11.) Shortly after those meetings began, Tiversa stole the 1718 File, and it

subsequently provided the file to the FTC.[29] Accordingly, the record indicates the FTC may have had a hand in Tiversa's theft of the 1718 File.

Documents stolen by a private party for use by the government, or where the government otherwise "had a hand" in the theft, are obtained through the equivalent of an unreasonable search and seizure within the meaning of the Fourth Amendment and are, therefore, subject to the exclusionary rule. *United States v. Mekjian*, 505 F.2d 1320, 1328 (5th Cir. 1975) ("[T]he question [is] whether or not there was such participation by the federal authorities as to require a holding that they had a hand in it."); *see also Knoll Assocs., Inc. v. F.T.C.*, 397 F.2d 530 (7th Cir. 1968) (excluding evidence stolen for use by the government); *F.T.C. v. Page*, 378 F. Supp. 1052 (N.D. Ga. 1974) (holding that respondents were entitled to discovery from FTC officials to determine if exclusionary rule was triggered). Accordingly, if the discovery sought by LabMD confirmed that the FTC "had a hand" in Tiversa's theft of the 1718 File, the exclusionary rule would apply to the

[29] Following the whistleblower's testimony, the U.S. House Oversight & Government Reform Committee published a 100-page report on Tiversa, criticizing it for myriad criminal and unethical behaviors. (RX644.) The report includes a 24-page section regarding Tiversa's relationship with the FTC, which it found to have been a "cooperative relationship" and a "mutually-beneficial collaboration" of questionable "propriety" that began in the fall of 2007 and pursuant to which Tiversa received "advanced knowledge of FTC regulatory actions" and provided documents to the FTC as early as December 2007. (*Id.* 54-58.)

FTC's keystone piece of evidence, the 1718 File, and its fruits. *Atl. Richfield Co. v. F.T.C.*, 546 F.2d 646, 651 (5th Cir. 1977).

Moreover, the Commission's conduct in this matter strongly suggests the FTC may have retaliated against LabMD for its CEO's having exercised his First Amendment right to publish a book sharply criticizing the FTC's investigatory overreach in this matter. *See Bennett v. Hendrix*, 423 F.3d 1247, 1250, 1254-56 (11th Cir. 2005) (government action in retaliation for protected speech violates First Amendment). The timing of the FTC's announcement of its decision to issue the Complaint just three days after LabMD's CEO announced his book, *see LabMD, Inc. v. F.T.C.*, 776 F.3d 1275, 1277 (11th Cir. 2015), alone creates a strong suspicion of retaliation. The Commission's retaliatory motive is also suggested by the Opinion's manifold strained statutory interpretations and unsupported evidentiary findings. Because this is a paradigmatic case where "it would seem as though the Commission clearly made its decision before it considered any contrary conclusion," *Schering-Plough*, 402 F.3d at 1065, the Court should have heightened concern about the possibility of the Commission's action having had an improper retaliatory motive.

Accordingly, whether or not the Court vacates the Order on one or more of the grounds set forth in Sections I-III *supra*, it should vacate the Order with directions that the FTC allow discovery into the FTC-Tiversa relationship prior to

the issuance of the Complaint and into the FTC's possibly unconstitutional retaliatory motive in filing the Complaint.

CONCLUSION

For the foregoing reasons, the Order should be vacated.

Dated: December 27, 2016

Respectfully submitted,
Counsel for LabMD, Inc.

/s/ Douglas H. Meal

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

Michelle L. Visser
ROPES & GRAY LLP
Three Embarcadero Center
San Francisco, CA 94111-006
(415) 315-6300

Douglas Hallward-Driemeier
ROPES & GRAY LLP
2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
(202) 508-4600

David T. Cohen
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
(212) 841-9000

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT, TYPEFACE REQUIREMENTS, AND TYPE-STYLE EQUIREMENTS

The undersigned counsel for Appellant hereby certifies that:

1. This brief complies with the type-volume limit of FED. R. APP. P. 32(a)(7)(B)(i) because, excluding the parts of the brief exempted by FED. R. APP. P. 32(f) and 11th Cir. R. 32-4, this brief contains 13,000 words.

2. This brief complies with the typeface requirements of FED. R. APP. P. 32(a)(5) and the type-style requirements of FED. R. APP. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font.

Dated: December 27, 2016

By: */s/ David T. Cohen*

David Cohen
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
(212) 841-9000

Counsel for Appellant

CERTIFICATE OF SERVICE

I hereby certify that, on December 27, 2016, I filed the foregoing document in the United States Court of Appeals for the Eleventh Circuit using the Court's Electronic Case Files ("ECF") system, which generates a notice that is emailed to attorneys of record registered to use the ECF system, including the following attorneys for Respondent Federal Trade Commission:

Joel Marcus
jmarcuskurn@ftc.gov

Theodore Metzler, Jr.
tmetzler@ftc.gov

Matthew Hoffman
mhoffman@ftc.gov

Under 11th Cir. R. 25-3(a), no independent service by other means is required.

Dated: December 27, 2016

By: */s/ Douglas H. Meal*

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000