No. 16-16270

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

LabMD, Inc.,

***Petitioner*,**

v.

Federal Trade Commission,

***Respondent*.**

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

AMICUS CURIAE BRIEF OF INTERNATIONAL CENTER FOR LAW & ECONOMICS AND TECHFREEDOM IN SUPPORT OF PETITIONER, LABMD, INC.

Geoffrey A. Manne
Kristian Stout
INTERNATIONAL CENTER
FOR LAW & ECONOMICS
3333 NE Sandy Blvd., Suite 207
Portland, OR 97232
503-770-0076
gmanne@laweconcenter.org

Berin M. Szóka
Thomas W. Struble
TECHFREEDOM
110 Maryland Avenue, Suite 409
Washington, DC 20002
202-803-2867
bszoka@techfreedom.org

John P. Hutchins*
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com

* *Counsel of Record*

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

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT (CIP)

Pursuant to Fed. R. App. P. 26.1 and 11th Cir. R. 26.1-1(a), International Center for Law & Economics and TechFreedom, by and through their undersigned counsel, hereby state that neither entity has a parent corporation and that no publicly held corporation owns ten percent or more of either entity's stock. A listing of all known trial judges, attorneys, persons, associations of persons, firms, partnerships, or corporations that have an interest in the outcome of this case or appeal, including subsidiaries, conglomerates, affiliates, parent corporations, any publicly held corporation that owns 10% or more of the party's stock, and other identifiable legal entities related to a party follows:

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

International Center for Law & Economics

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

Manne, Geoffrey A., Attorney, International Center for Law & Economics

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

Stout, Kristian, Attorney, International Center for Law & Economics

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

No publicly traded company or corporation has an interest in the outcome of the case or appeal.

Dated: January 3, 2017

Respectfully submitted,

/s/ John P. Hutchins
John P. Hutchins
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com

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

STATEMENT OF AUTHORSHIP & FINANCIAL CONTRIBUTIONS

Under Federal Rule of Appellate Procedure 29(c), *amici* state that no party's counsel authored this brief in whole or in part, and no party or its counsel made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amici curiae or their counsel contributed money that was intended to fund preparing or submitting the brief.

STATEMENT OF INTEREST

ICLE is a non-profit, non-partisan global research and policy center. ICLE works with more than fifty affiliated scholars and research centers around the world to promote the use of evidence-based methodologies in de-

veloping sensible, economically grounded policies that will enable businesses and innovation to flourish.

TechFreedom is a non-profit, non-partisan 501(c)(3) tax-exempt think tank dedicated to educating policymakers, the media and the public about technology policy. TechFreedom advocates regulatory approaches that balance the need for flexibility with analytical rigor to constrain regulatory discretion.

TechFreedom and ICLE have convened the FTC: Technology & Reform Project, dedicated to studying the details of the agency's operations and proposing reforms to help the agency achieve its mission of maximizing consumer welfare. *See, e.g.*, CONSUMER PROTECTION & COMPETITION REGULATION IN A HIGH-TECH WORLD: DISCUSSING THE FUTURE OF THE FEDERAL TRADE COMMISSION (Dec. 2013), *available at* http://goo.gl/52G4nL.

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Statutes

Other Authorities

Rules

SUMMARY OF THE ARGUMENT

Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ["Section 5"], is a consumer protection statute, not a data security rule. *See* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, United States Senate (Dec. 17, 1980) ["Unfairness Statement"], reprinted in *International Harvester Co.*, 104 FTC 949, 1073 (1984) ["*International Harvester*"]

(quoting 83 Cong. Rec. 3255 (1938) (remarks of Senator Wheeler)) ("Unjustified consumer injury is the primary focus of the FTC Act….'").

This fundamental point has been lost in the Commission's approach to data security. The touchstone for Section 5 actions is not "reasonableness," but consumer welfare: Does this enforcement action deter a preventable "unfair" act or practice that, on net, harms consumer welfare, and do the benefits to consumers from this action outweigh its costs? Section 5's purpose is neither fundamentally remedial nor prescriptive. Concern for consumer welfare means deterring bad conduct, avoiding over-deterrence of pro-consumer conduct, minimizing compliance costs, and minimizing administrative costs (by focusing only on substantial harms) — *not* preventing every possible harm. Instead of weighing such factors carefully, or even performing a proper analysis of negligence, as it purports to do, the Commission has effectively created a strict liability standard unmoored from Section 5.

Across the Commission's purported guidance on data security, it has likewise failed to articulate a standard by which companies themselves should weigh costs and benefits to determine which risks are sufficiently foreseeable that they can be mitigated cost-effectively. Thus, in addition to violating the intent of Congress, the FTC has also violated the Constitution by failing to

provide companies like LabMD with "fair notice" of the agency's interpretation of what Section 5 requires.

For the following reasons, the FTC's Order should be vacated.

ARGUMENT

I. THE FTC PROVIDED INSUFFICIENT NOTICE OF THE DATA SECURITY REQUIREMENTS UNDER SECTION 5 OF THE FTC ACT TO COMPORT WITH DUE PROCESS.

The FTC alleges that, between June 2007 and May 2008, LabMD violated Section 5 of the FTC Act by failing to provide "reasonable" data security. *In re LabMD, Inc.*, Administrative Complaint, F.T.C. Docket No. 9357 (Aug. 29, 2013) ["Complaint"]. Contrary to the view of the FTC, but in keeping with that of its Chief Administrative Law Judge, *In re LabMD, Inc.*, Initial Decision, F.T.C. Docket No. 9357 (Nov. 13, 2015) ["Initial Decision"], the FTC failed to provide, *during this period*, the fair notice required by the Constitution to LabMD that its data security could be deemed unfair. As a plainly exasperated district court judge said to FTC's counsel during a hearing on the FTC's denial of LabMD's motion to dismiss:

> I think that you will admit that there are no security standards from the FTC. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…. [H]ow does any company in the United States operate when… [it] says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are

> not supposed to do what you did.… [Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.

Transcript of Proceedings at 91, 94–95, *LabMD, Inc. v. Fed. Trade Comm'n*, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014) ["Oral Argument Transcript"]. Thus, lacking such notice, the FTC's Order finding LabMD's data security violated Section 5 of the Act was in violation of LabMD's due process rights, and should be vacated. *In re LabMD, Inc.*, Final Order, F.T.C. Docket No. 9357 (July 29, 2016) ["Order"].

A. **The FTC Misreads the Case Law on Fair Notice**

The FTC relies heavily upon *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 (3d Cir. 2015) ["*Wyndham*"], but fundamentally misunderstands the case. The FTC claims that the agency has

> provided ample notice to the public of our expectations regarding reasonable and appropriate data security practices by issuing numerous administrative decisions finding specific companies liable for unreasonable data security practices. Our complaints, as well as our decisions and orders accepting consent decrees…make clear that the failure to take reasonable data security measures may constitute an unfair practice. Those complaints, decisions, and orders also flesh out the specific types of security lapses that may be deemed unreasonable.… And even though they "are neither regulations nor 'adjudications on the merits,'" they are sufficient to afford fair notice of what was needed to satisfy Section 5(n). *See Wyndham*, 799 F.3d at 257 (citing *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004) ["*Lachman*"]; *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008) ["*Beverly*"];

> and *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) ["*General Electric*"]).

In re LabMD, Inc., Opinion of the Commission, F.T.C. Docket No. 9357, at 30–31 (July 29, 2016) ["FTC Opinion"]. This misreads *Wyndham*: as an interlocutory appeal from the denial of a 12(b)(6) motion, the decision did not determine whether the FTC's informal data security guidance had provided fair notice. *Wyndham*, 799 F.3d at 240.

The Third Circuit merely noted that "courts regularly *consider* materials that are neither regulations nor 'adjudications on the merits.'" *Id.* at 257 (emphasis added). Whether such agency guidance affords fair notice depends on the circumstances. *See, e.g.*, Gerard M. Stegmaier & Wendell Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MAS. L. REV. 673, 704–05 (2013).

Crucially, the sufficiency of such materials to confer fair notice in each of the three cases cited by *Wyndham* (and relied upon by the FTC) turns on the reasonableness of expecting the defendant to create an adequate internal compliance regime based on (i) monitoring the agency's interpretations and pronouncements, and (ii) effectively predicting how the agency would apply its authority. Each analysis also hinged on the company's experience as a special-

ly regulated enterprise vis-à-vis a particular agency — in a way that is not true of LabMD and the FTC:

- *Lachman*: Manufacturer of "carbon/carbon material…suitable for use in rocket components, including ballistic missiles with nuclear capability" could not claim it lacked fair notice that its product would require an export license; it had a duty to consult counsel regarding how the Commerce Department would apply the term "specially designed" to its product. 387 F.3d at 45, 57.

- *Beverly*: Nursing home had fair notice of an advice letter issued by OSHA fifteen years earlier declaring that employers of healthcare professionals must reimburse employees exposed to blood-borne pathogens not only for direct medical costs, but also for travel costs, and compensation for time spent recovering. 541 F.3d. at 202.

- *General Electric*: Manufacturer of large electric transformers lacked fair notice of the EPA's interpretation of its regulation on disposing of a dangerous chemical because the agency's "policy statements [were] unclear…the [company's] interpretation [was] rea-

> sonable, and … the agency itself struggle[d] to provide a definitive reading of the regulatory requirements." 53 F.3d at 1334.

All three cases involved regulations "addressed to sophisticated businessmen and corporations which, because of the complexity of the regulatory regime, necessarily consult counsel in planning their activities." *Lachman*, 387 F.3d at 57.

The FTC effectively imputes this burden to any company in America that holds personal data. But the FTC differs fundamentally from the Commerce Department enforcing export control regulations or the EPA policing toxic substances — or even HHS regulating the data practices of healthcare companies. The FTC is America's catch-all consumer protection regulator; it polices nearly every company in America under the most general possible standards. This case is readily distinguishable from *Beverly*: yes, the FTC and OSHA both enjoy broad jurisdiction ("trade" and "workplaces") but OSHA enforced a statute explicitly focused on the topic at issue (*i.e.*, "wage loss" and "medical expenses"), 29 U.S.C. § 651(a). The only question was the precise application of those terms, a question that OSHA answered with a clear statement including the very issues in dispute (time spent receiving treatment and travel expenses). *Beverly*, 541 F.3d. at 197. The FTC, by contrast, is enforcing a vague statutory standard (unfairness) with a vague regulatory standard (unrea-

sonableness) and offering guidance whose applicability is unclear — and is not the regulator assigned by Congress to the issue.

The implication from this line of cases is clear: entities, like LabMD, comprehensively regulated under industry-specific regimes, have a duty to be aware of the requirements of those specialized regimes. But, to the extent that other federal regulatory regimes purport to impose *differing* requirements on those companies, fair notice of those different requirements cannot be presumed. This is particularly true where the specialized regulatory regime enforces detailed regulations relating to the issue under consideration.

The FTC occasionally brings actions against HHS-regulated companies and has sporadically opined on health-related data security issues, *see, e.g.*, *In the Matter of CVS/Caremark Corp.*, Dkt. No. C-4259, FTC File No. 0723119 (2009), http://bit.ly/2hMjDNH (2009); *In the Matter of Rite-Aid Corp.*, Dkt. No. C-4308, FTC File No. 0723121 (2010), http://bit.ly/2hMcU6z; Medical Identity Theft Guidance: FAQ'S for Health Care Providers and Health Plans, FTC (2011), *available at* https://goo.gl/6S61SH. But not only does this not suffice to establish the FTC as a sectoral regulator commanding the close attention of industry actors, the first of these actions and guidance documents long postdated the conduct at issue here.

Meanwhile, HHS energetically enforces its own data security rules, and yet, during the time period relevant here, never offered guidance directing its covered entities or business associates to look to the FTC, nor referred to FTC guidance or enforcement actions relating to data security and privacy. *See* "Security," hhs.gov (last visited Jan. 2, 2017), http://bit.ly/2hJhDWC (referring only to FTC guidelines promulgated in 2010 and later, and not referring to enforcement at all). In fact, HHS and FTC have often been at loggerheads over data enforcement.[1]

The Supreme Court has repeatedly that, where they diverge, specialized, comprehensive regulatory regimes supersede more generalized regimes that address overlapping issues. See, e.g., *Credit Suisse Securities v. Billing*, 551 U.S. 264 (2007); *Verizon Comm. Inc. v. Law Offices of Curtis V. Trinko*, 540 U.S. 398 (2004); *United States v. Citizens Southern Nat. Bank*, 422 U.S. 86 (1975).

B. The FTC Misreads *Wyndham* More Generally.

The FTC generally misreads the *Wyndham* opinion. The Third Circuit repeatedly expressed skepticism of the FTC's notice arguments. Most funda-

[1] Not until October 2016 did the FTC and HHS declare that covered entities and business associates should look to both agencies for guidance regarding certain PHI practices. *See* "Sharing Consumer Health Information? Look to HIPAA and the FTC Act," FTC and HHS, *available at* http://bit.ly/2hJfKcw.

mentally, the court dismissed the relevance of the FTC's enforcement actions and focused instead on the statute itself. *Wyndham*, 799 F.3d at 255–59.

The relevant question is not merely whether LabMD had fair notice that Section 5 might apply to data security, *id.* at 255 ("We do not read Wyndham's briefs as arguing [it] lacked fair notice that cybersecurity practices can … form the basis of an unfair practice"), but whether LabMD had fair notice as to *how* the FTC would apply the cost-benefit analysis test in Section 5 to its data security. *Id.* ("Wyndham argues instead that it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability.") (emphasis in original). This is the difference, between saying that General Electric had a special duty to monitor to the EPA's pronouncements and that General Electric had fair notice of *how* the EPA would interpret a particular rule. *See Gen. Elec. Co.*, 53 F.3d at 1334.

On that question, the *Wyndham* court implied strongly that the FTC's guidance was insufficient to qualify as fair notice. *See Wyndham*, 799 F.3d at 256 n.21 ("we agree with Wyndham that the guidebook could not, on its own, provide 'ascertainable certainty' of the FTC's interpretation of what specific cybersecurity practices fail § 45(n). But as we have already explained, this is not the relevant question."); *id.* at 257 n.22 ("We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective

requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).").

C. The FTC's *Guidance* Did Not Provide LabMD *Fair* Notice, and the Order Thus Violates Due Process.

The FTC points to various guidance it had produced contemporaneous with the LabMD data theft. But such guidance was insufficient to afford LabMD fair notice.

The FTC's first document on the topic, *Protecting Personal Information: A Guide For Business*, FTC (2007), *available at* https://goo.gl/w9fSfW, issued in March 2007 — very shortly before the LabMD data theft — suggested at least some of the data security practices the FTC alleges LabMD should have provided. Previously, the FTC had issued only one press release (2004) and workshop report (2005, geared towards developers of peer-to-peer networking software) to point to for guidance. FTC Opinion, at 30 n.81 (citing Press Release, Press Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, offer Businesses Tips For Keeping Their Computer Systems Secure (Apr. 2, 2004), and *Protecting Personal Information*, FTC (2005)). And the FTC also cited evidence of common industry practice, but that evidence was from 2010, a full two years *after* the relevant time period. But, given the timing of its guide, the size and sophistication of LabMD, and

the nature of the allegedly unreasonable behavior, the FTC's guidance did not provide *fair* notice.

In claiming that its press releases and workshop reports qualify as sufficient guidance to provide fair notice, the FTC is treating these highly informal statements as triggers of legally enforceable duties — *i.e.*, *de facto* rulemakings. For example, the FTC routinely cites its 2012 Privacy Report, Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) ["FTC Privacy Report"], *available at* http://bit.ly/2hMz7RX, as if it were a rulemaking, incorporating its "recommendations" as boilerplate, welding them onto every data security settlement, regardless of the circumstances. *See, e.g.*, Gus Hurwitz, *FTC's Efforts in* LabMD *Lack Required Due Process and Don't Actually Improve Security*, TECHPOLICYDAILY.COM (Aug. 2, 2016), http://bit.ly/2hNZtTu.

Thus has the Commission circumvented the rulemaking safeguards established by Congress in the Magnuson-Moss Act of 1975, 15 U.S.C. § 57b-3, and tightened by Congress in 1980, Federal Trade Commission Improvements Act of 1980, Pub. L. 96-252, 94 Stat. 374 (1980) — the same Congress that forced the FTC to issue the Unfairness Statement. Whatever discretion administrative agencies enjoy in choosing to use either rulemakings or case-by-case

adjudication, the FTC's attempt to shoehorn these quasi-regulatory soft guidance materials into fair notice raises profound due process concerns.

II. THE FTC'S "REASONABLENESS" STANDARD EXCEEDS ITS AUTHORITY UNDER SECTION 5

Consumer welfare is the lodestar of Section 5. Like the consumer welfare-oriented antitrust laws, Section 5 does not proscribe specific acts but is a general standard, designed to penalize and deter "unfair" conduct that harms consumers on net – *without* sweeping in pro-consumer conduct that does not cause demonstrable harm (or that is "reasonably avoidable" by consumers themselves). *See* FTC Opinion at 26 (quoting Unfairness Statement, at 1073) ("A 'benefit' can be in the form of lower costs and… lower prices for consumers, and the Commission 'will not find that a practice unfairly injures consumers unless it is injurious in its net effects.'").

Thus, Section 5(n) incorporates a negligence-like standard, rather than a strict-liability rule, and thus concepts from the common law, such as foreseeability and duty of care. Thus, the FTC may prohibit only conduct whose costs outweigh benefits, and where harm isn't more efficiently avoided by consumers themselves. *See, e.g.*, Letter from Joel Winston, Associate Director of Fed. Trade Comm'n to Michael E. Burke, Esq., Counsel to Dollar Tree Stores, Inc. (Jun. 5, 2001), *available at* https://goo.gl/0LPP5w (emphasizing these ele-

ments of the FTC's unfairness inquiry and finding no responsibility for unforeseeable risks).

Establishing that conduct was unfair/unreasonable thus requires establishing (i) a clear baseline of conduct, (ii) a company's deviation from that baseline, and (iii) proof that its deviation caused, or was significantly likely to cause, harm. Both the statute and the constitutional doctrine of Fair Notice require *some* limits on the FTC's discretion to decide what, beyond the existence of a breach, indicates inadequate data security.

The FTC's rhetoric on data security appears to reflect the fundamental negligence-like analysis and economic balancing required by Section 5(n):

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities…. [T]he Commission… does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

Commission Statement Marking the FTC's 50th Data Security Settlement at 1 (Jan. 31, 2014) ["FTC 50th Settlement Statement"], *available at* http://bit.ly/2hubiwv*; see also* FTC Opinion at 11. Yet, by eliding the distinct elements of a Section 5(n) analysis, the FTC's "reasonableness" approach ends

up ignoring Congress's plain requirement that the Commission demonstrate causality and substantiality, and perform a cost-benefit analysis — clearly rejecting a strict liability approach. Congress plainly intended to constrain the FTC's discretion to avoid the hasty assumption that imposing *any* costs on consumers is "unfair."[2]

The FTC claims it has weighed the relevant facts, but has failed to adduce how specific facts affect its analysis, demonstrate causation, or evaluate the relative costs and benefits of challenged practices and its own remedies. The Commission asserts that the exposed data were sensitive, but said nothing, for example, about (i) whether any of it (*e.g.*, medical test codes) could actually reveal sensitive information; (ii) what proportion of LabMD's sensitive data was exposed on LimeWire; (iii) the complexity or size of the business; (iv) the indirect costs of compliance, such as the opportunity costs of implementation of the FTC's required remedies; and (v) the deterrent effect of the enforcement action.

The FTC's inappropriately *post hoc* assessment considers only those remedial measures it claims would address the specific breach at issue. This ignores the overall compliance burden to avoid liability without knowing, *ex*

[2] No market interaction is *ever* without costs: paying any price, waiting in line, or putting up with advertising are all "costs" to a consumer.

ante, which specific harm might occur. Actual compliance costs are far more substantial, and require a firm to evaluate which of the universe of possible harms it should avoid, and which standards the FTC has and would enforce. This is a far more substantial, costlier undertaking than the FTC admits.

A. The FTC Failed to Establish that LabMD Breached Its Duty of Care

Section 5(n) plainly requires a demonstrable connection between conduct and injury. While the anticompetitive harm requirement that now defines Sherman Act jurisprudence was a judicial construct, *see, e.g., Continental T.V., Inc. v. GTE Sylvania, Inc.*, 433 U.S. 36 (1977), Section 5(n) itself demands proof that an "act or practice causes or is likely to cause substantial injury" before it may be declared unfair. But the FTC's reasonableness approach, as noted, is not directed by the statute, which nowhere defines actionable conduct as "unreasonable;" rather, the statute requires considerably more. But even taking the FTC at face value and assuming "reasonableness" is meant as shorthand for the full range of elements required by Section 5(n), the FTC's approach to reasonableness is fatally wanting.

1. The FTC Has Not Established a Benchmark Standard for Duty of Care

Although reasonableness is a fuzzy concept, courts have developed consistent criteria for establishing it. Under negligence standards, an actor must

have, and breach, a duty of care before its conduct will be deemed unreasonable. *See* STUART M. SPEISER ET AL., 2A AMERICAN LAW OF TORTS, § 9:3 (2016). This requires that the actor's duty be defined with enough specificity to make it clear when her conduct breaches it — which is not true here, reasons that parallel why LabMD lacked fair notice of how the FTC would apply Section 5 to it.

In most jurisdictions, "care" is defined by reference to standard industry practices, specific legislative requirements, contractual obligations, or a judicial determination of what prudence dictates. Restatement (Second) of Torts § 285 (1965). Moreover, in most jurisdictions, the appropriate standard of care reflects the foreseeability of harm: there is no duty to protect against unforeseeable risks. *Id.* § 302.

The FTC has established no concrete benchmark for due care, however. The Commission cites in passing to some possible sources, *see, e.g.,* FTC Opinion at 12 (referring to HIPAA as "a useful benchmark for reasonable behavior"), but fails to distinguish among such documents, to explain how much weight to give any of them, or to distill these references into an operationalizable standard. Not only was this true at the time of LabMD's alleged conduct, but it remained the case six to seven years *later*, and arguably still holds true today:

> the standard language that the FTC uses is terse and offers little in the way of specifics about the components of a compliance program. Consequently, anyone seeking to design a program that complies with FTC expectations would have to return to the complaints to parse out what the FTC views as "*un*reasonable" — and, by negation, reasonable — privacy and data security procedures.

Patricia Bailin, *What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, IAPP/Westin Research Center Study, at 1 (Oct. 30, 2014), *available at* http://bit.ly/2hJkIWR.

Moreover, because of the amorphousness of the FTC's data security "standards", and the fact that they are developed through one-sided consent decrees with limited application and little, if any, legal analysis,

> *we don't know what we don't know*, that is, whether other practices that have not yet been addressed by the FTC are "reasonable" or not. (In fact, we don't even know whether there is … a comprehensive FTC data security standard). Even in those cases that have been pursued, we don't know how high the reasonableness bar is set. Would it be enough for a company to elevate its game by just an increment to clear the reasonableness standard? Or does it have to climb several steps to clear the bar?

Omer Tene, *The Blind Men, the Elephant and the FTC's Data Security Standards*, PRIVACY PERSPECTIVES BLOG (Oct. 20, 2014), *available at* http://bit.ly/2hJwlwI (emphasis in original). Again, this was only *more* true at the time of LabMD's conduct, when the FTC's unfairness approach to data security was in its infancy.

Not only does this defect cause the action against LabMD to fail for lack of fair notice, as discussed above, it also causes the action to exceed the Commission's statutory authority.

2. The FTC Failed to Establish that LabMD's Conduct Deviated from its Duty of Care

Because "perfect" data security is impossible, not all data security practices that "increase" risk of breach are unfair. *See* FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement", (Jan. 31, 2014) ("the Commission has made clear that it does not require perfect security"). *Some* amount of harm (to say nothing of breaches) is fully consistent with the exercise of due care — of "reasonable" data security practices. For the statute to be meaningful, data security practices must be shown to fall outside of customary practice — *i.e.*, to increase the risk of unauthorized exposure (and the resulting harm) above some "customary" level — before they are deemed unreasonable.

The FTC asserts that this standard is sufficiently well-defined, that LabMD's failure to engage in certain, specific actions enabled the data breach to occur, and thus that LabMD must have deviated from what was required of it. But a company cannot be faulted for engaging in conduct (or for failing to engage in conduct) that it does not know, or could not know, violates its duty of care. It is not the case that LabMD had *no* data security program. "LabMD

employed a comprehensive security program that included a compliance program, training, firewalls, network monitoring, password controls, access controls, antivirus, and security-related inspections." Brief for Petitioner at 2, *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. Dec. 27, 2016) (citations to the record omitted). The Commission disputes some of these. But for every practice the FTC claims LabMD did *not* engage in, there were other practices in which it *did* engage.

The FTC simply has not established that LabMD's practices were insufficient to meet its duty of care. At best, the Commission has argued that LabMD failed to engage in *some* conduct that *could* be part of the duty of care. But even if LabMD failed to engage in every practice derived from FTC consent decrees (most of which post-date the relevant time period here), or some of the practices described in one or more of the industry standard documents that the FTC refers to, *see* FTC Opinion at 12 & n. 23, the FTC has failed to establish that LabMD's practices. *as a whole*, were insufficient to meet a reasonable standard of care. Even if LabMD failed to engage in *some* of the wide range of possible practices that comprise the FTC's (undefined) standard, the FTC still has not established that such a failure causes the overall data security regime to become insufficient.

Where, as here, the FTC focuses on the sufficiency of precautions relating to the specific harm that occurred, it fails to establish the requirements for an overall data protection scheme — the relevant consideration. The general security obligations under which any company operates prior to a specific incident are not necessarily tied to that incident. *Ex ante*, in implementing its security practices, LabMD would not have focused particularly on the P2P risk, which was, at the time, not particularly well understood. Before Tiversa's incursion, LabMD surely faced different security risks, and undertook to adopt measures to protect against them. Given this, the existence of P2P software on one computer in its billing department was hardly unreasonable, in light of the protections LabMD *did* adopt. Despite suffering no no security breaches, the Commission would invalidate all of LabMD's data protection measures because of the single (unlikely) breach that *did* occur.

The fundamental problem with the FTC's argument is that, by arguing backward solely from what eventually *did* occur, and failing to assess the *ex ante* risk that it *as well as all other possible security problems* would occur, the FTC puts the cart before the horse and effectively converts a negligence-like regime into one of strict liability. The duty of care that must be violated for a "reasonableness" standard is meaningless if it is defined solely by such a narrow, post hoc analysis. By effectively defining "reasonableness" in terms of a company's

failure to thwart only the breach that *did* occur (and not the ones that *could* have but did *not*), the analysis becomes one of effective strict liability.

B. The FTC Misinterprets the Plain Meaning of "Substantial Injury."

When establishing causality, Section 5(n) is not focused on the "substantial[ity]" of the injury; the *likelihood* that conduct caused substantial injury and the *substantiality* of the injury itself are distinct concepts. Conduct does not become more likely to *cause* harm in the first place just because the resulting harm may be relatively more *substantial.*

This is clear from the statute: "Substantial" modifies "injury," not "likely." Either conduct *causes* substantial injury, or it is *likely* to cause substantial injury, meaning it creates a heightened risk of substantial injury. To reimport the risk component into the word "substantial" following the word "likely" makes no syntactic sense: "Likely to cause" already encompasses the class of injuries comprising increased risk of harm. The FTC's interpretation would amount to creating liability for conduct that creates *a risk of a risk* of harm.

Although the Unfairness Statement does note that "[a]n injury may be sufficiently substantial… *if it raises a significant risk of concrete harm,*" FTC Opinion at 21 (quoting Unfairness Statement at 1073 n. 12) (emphasis added), "raises" clearly does not mean "increases the degree of" here, but rather "stirs up" or

"gives rise to." *Raise*, Merriam-Webster.com (last visited Jan. 2, 2017), *available at* https://goo.gl/R2sVhm. And the relevant risk in footnote 12 is deemed to be "significant," not "substantial," suggesting it was intended to be of a different character. Moreover, that passage conveys the Commission's intention to address inchoate harms under Section 5 — conduct "likely" to cause harm: In effect, footnote 12 was incorporated into Section 5(n) by inserting the words "or is likely to cause" in the phrase "causes… substantial harm." Importing it *again* into the determination of substantiality is a patently unreasonable reading of the statute and risks writing the substantial injury requirement out of the statute.

At first blush, the FTC's proposed multiplication function ("[A] practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low." FTC Opinion at 21) may sound like the first half of Footnote 12 ("An injury may be sufficiently substantial, however, if it does a small harm to a large number of people." Unfairness Statement at n.21), but these are two very different things. Indeed, the fact that the Footnote proposes a multiplication function for interpersonal aggregation of harms, but then, in the next breath, says no such thing about multiplying small risks times large harms, can have only one meaning: The Policy Statement requires the FTC to prove the substantiality of harm, independent of its risk. Had Congress

intended for the rather straightforward strictures of 5(n) to accommodate the large loophole proposed by the FTC, it surely would have spoken affirmatively. It did not. Instead, as is evident from the plain text of the statute, Congress structured Section 5(n) as a meaningful limitation on the FTC's potentially boundless Unfairness authority.

The Commission claims that "[t]he Third Circuit interpreted Section 5(n) in a similar way in *Wyndham*. It explained that defendants may be liable for practices that are likely to cause substantial injury if the harm was 'foreseeable,' … focusing on both the 'probability and expected size' of consumer harm." FTC Opinion at 21 (internal citations omitted). But the *Wyndham* court did *not* declare that the first prong of Section 5(n) requires that the magnitude of harm be multiplied by the probability of harm when evaluating its foreseeability. Instead, the court includes the magnitude of harm as one consideration in cost-benefit analysis:

> [T]his standard informs parties that the relevant inquiry here 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 (internal citations omitted). This is not the same as the Commission's proffered approach. The Third Circuit essentially recited the

elements of a complete evaluation of Section 5(n), *not* the requirements for evaluating the first prong of the test.

C. The FTC Failed to Demonstrate that LabMD's Conduct Caused or Was Likely to Cause Substantial Harm

Even with respect to causation, the Commission failed to adequately show that the actual and likely harm of which it complained was a foreseeable result of LabMD's conduct, given the standards (or lack thereof) of reasonable conduct in 2007.

There is some question whether the Act contemplates conduct at all that merely facilitates (or fails to prevent) harm by third parties, rather than causes harm to consumers directly. *See generally* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008). But even if the FTC does have authority to police data breaches and data security problems, *see, e.g.*, *Wyndham*, 799 F.3d at 248–49, the fit between such conduct and Section 5 remains uneasy.

The FTC has traditionally used its unfairness power to police coercive sales and marketing tactics, unsubstantiated advertising, and other mirepresentations to consumers; in such cases, there is a more direct line between conduct and harm. *See generally* Richard Craswell, *Identification of Unfair Acts and Practices by the Federal Trade Commission*, 1981 WISC. L. REV 107 (1981). In data secu-

rity cases, however, the alleged unfairness is a function of a company's failure to take precautions sufficient to *prevent* a third party's intervening, harmful action (*i.e.*, hacking).

This creates far more significant problems of causation and proof. While a company's security *may* have facilitated a breach, it is difficult to *know* whether this is true. The FTC simply infers causation from the existence of a breach. *See* Transcript of Closing Arguments (Rough Draft) at 48*, In re LabMD, Inc.,* F.T.C. Docket No. 9357 (Sep. 16, 2015) (on file with the authors) ("[Y]ou haven't cited any Court of Appeals case… [finds]… evidence of… a single breach, is sufficient to sustain a violation of *Section* 5"). But, as noted (and as the Commission recognizes elsewhere), no security can be perfect, and thus the fact of a breach cannot, *per se,* prove that a company's data security practices violated Section 5. Indeed, by the same token, even if a company *had* done everything the FTC asserts is required, there could *still* have been a breach. Instead the statute demands demonstration that the failure to prevent a breach violated the duty of care and that it *resulted in* — *i.e.*, was not *itself* — "substantial injury."

The FTC has failed to establish either that LabMD "cause[d] or [was] likely to cause substantial injury to consumers," or that its conduct was "not outweighed by countervailing benefits to consumers or to competition."

The Commission "does not know," FTC Opinion at 17, whether any patient encountered a single problem related to the breach, and thus has not articulated any injury caused by LabMD's conduct.[3] The Commission asserts that mere exposure of information suffices to establish harm. *See* FTC Opinion at 18 ("Indeed, the Commission has long recognized that the unauthorized release of sensitive medical information harms consumers"). But this amounts to saying that any conduct that causes breach causes harm. That not only violates the FTC's own claims that breach alone is not enough, it is patently insufficient to meet the substantial injury requirement of Section 5(n). The examples it adduces to support this point all entail not merely exposure, but actual dissemination of personal information to large numbers of unauthorized recipients who *actually read* the exposed data. *See generally In the Matter of MTS, Inc.* Dkt. No C-4110, 137 F.T.C. (2004), *available at* https://goo.gl/4emzhY (Tower Records liable for software error that allowed 5,225 consumers' billing information to be read by anyone, which actually occurred). Even if it is reasonable to assert in such circumstances that "embarrassment or other negative

[3] And although the Commission effectively blames LabMD for its (the FTC's) lack of knowledge of harm, that burden does not rest with LabMD. Moreover, the Commission had ample opportunity to collect such evidence if it existed, *e.g.*, by actually asking at least a sample of patients whose data was in the 1718 file or subpoenaing insurance companies to investigate possible fraud. That the Commission still cannot produce any evidence suggests, in the strongest possible terms, that none exists.

outcomes, including reputational harm" result from that sort of public disclosure, FTC Opinion at 17, no such disclosure occurred here. That the third-party responsible for exposure of data itself viewed the data — which is effectively all that happened here — cannot be the basis for injury without simply transforming the breach itself into the injury.

Moreover, instead of establishing a causal link between LabMD's conduct and even the breach itself (let alone the alleged harm), the FTC offers a series of *non sequiturs*, unsupported by evidence. The Order cites allegedly deficient practices, *see, e.g.*, FTC Opinion at 2, but establishes no causal link between these and Tiversa's theft of the 1718 file — nor *could* it, because the theft had nothing to do with passwords or operating system updates, or firewalls, and because things like integrity monitoring and penetration testing, at best, "'might have' aided detection of the application containing the P2P vulnerability," Pet. Br. at 47 (citations to the record omitted); *see also id.* at 31 & n. 13, LabMD's alleged failure to do these things cannot be said to have caused the (alleged) harm. Even with respect to other security practices that *might* have a more logical connection to the breach (*e.g.*, better employee training), the Commission offers no actual evidence demonstrating that these actually caused, or even were likely to cause, any harm.

Whatever the standard for "unreasonableness," there must be a causal connection between the acts (or omissions) and the alleged injury. Even for likely harms this requires not mere possibility but *probability* at the time the conduct was undertaken. *See* Initial Decision at 54. Instead, the Commission merely asserts that harm was sufficiently "likely" based on its own *ex post* assessment, in either 2012 or 2016, of the risks of P2P software in 2007.

The FTC's Chief Administrative Law Judge found this assertion wanting, ruling that the Commission had failed to establish likely harm. *Id.* at 53. But the Commission, in its turn, disagreed:

> The ALJ's reasoning comes perilously close to reading the term "likely" out of the statute. When evaluating a practice, we judge the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes.

FTC Opinion at 23. This is true, as far as it goes, but the FTC's only evidence on the likelihood of harm in 2007 is… evidence of the likelihood of such harm in 2013 and today. *Id.* at 24. Moreover, judgments about the likelihood that past conduct will cause harm must be informed by what has actually occurred. By the time the FTC filed its complaint, and surely by the time the FTC rendered its opinion, facts about what actually happened up to that point should have informed the Commission about what was likely to occur. That the only

available facts point to the complete absence of injury suggests injury was not likely caused by any of LabMD's conduct.

It is thus the Commission that is in danger of reading "likely" out of the statute — and "substantial" for that matter. Under the FTC's interpretation the statute could have been written as "The Commission shall have no authority under this section… to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or [could conceivably have] cause[d]… [any] injury."

CONCLUSION

For the foregoing reasons, the FTC's Order should be vacated.

Respectfully submitted,

Geoffrey A. Manne
Kristian Stout
INTERNATIONAL CENTER
FOR LAW & ECONOMICS
3333 NE Sandy Blvd., Suite 207
Portland, OR 97232
503-770-0076
gmanne@laweconcenter.org

Berin M. Szóka
Thomas W. Struble
TECHFREEDOM
110 Maryland Avenue, Suite 409
Washington, DC 20002
202-803-2867
bszoka@techfreedom.org

John P. Hutchins*
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
(404) 267-2733 Direct
(404) 267-2750 Fax
(404) 644-9325 Mobile
John.Hutchins@leclairryan.com
https://www.leclairryan.com

* Counsel of Record

January 3, 2017

CERTIFICATE OF COMPLIANCE

The undersigned counsel hereby certifies that this brief complies with Fed. R. App. P. 32(a) because, excluding the parts exempted by Fed. R. App. P. 32(f) and 11th Cir. R. 32-4, this brief contains 6,478 words and has been prepared in a 14-point proportionally spaced typeface.

Dated: January 3, 2017

Respectfully submitted,

/s/ John P. Hutchins
John P. Hutchins
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com

CERTIFICATE OF SERVICE

I hereby certify that, on January 3, 2017, 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.

Dated: January 3, 2017

Respectfully submitted,

/s/ John P. Hutchins
John P. Hutchins
Georgia Bar No. 380692
LECLAIRRYAN
1170 Peachtree Street, NE, Suite 2350
Atlanta, Georgia 30309
404-267-2733
John.Hutchins@leclairryan.com