

United States Court of Appeals
for the
Eleventh Circuit

LABMD, INC.,

Petitioner,

v.

FEDERAL TRADE COMMISSION,

Respondent.

ON PETITION FOR REVIEW OF AN ORDER
OF THE FEDERAL TRADE COMMISSION
(FTC DOCKET No. 9357)

**BRIEF OF DR. DAVID BLACK, DR. BRUCE GREEN, DR. JOAN HADER,
DR. BRIAN HILL, DR. WARREN HITT, DR. WILLIAM NABORS, DR.
ROBERT ROSS, JR., DR. BRADLEY SECREST, AND DR. DAVID STOUT
AS AMICI CURIAE IN SUPPORT OF PETITIONER**

PATRICK J. MASSARI
MICHAEL PEPSON
CAUSE OF ACTION INSTITUTE
1875 EYE STREET N.W., SUITE 800
WASHINGTON, D.C. 20006
(202) 422-4332

Counsel for Amici Curiae

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Eleventh Circuit Rule 26.1-1, undersigned counsel for *amici curiae* practicing and retired physicians specializing in urology and Doctor David Lee Black, Founder and former CEO, President, and Director of Aegis Sciences Corporation, certifies that *amici curiae* are individual doctors participating in this action solely in that capacity, not corporate parties. In accordance with Federal Rule of Appellate Procedure 26.1 and Eleventh Circuit Rules 26.1-1 through 26.1-3, the undersigned further certifies that the Petitioner's Certificate of Interested Persons and Disclosure Statement, supplemented by *Amicus Curiae* National Federation of Independent Business Small Business Legal Center's Certificate of Interested Persons and *Amicus Curiae* National Technology Security Coalition's Certificate of Interested Persons, contains a complete list of interested persons and entities, with the exception of the following additional persons:

Black, David L., Ph.D., D-ABFT, FAIC, *Founder, Aegis Sciences Corp.*

Green, Bruce G., MD, FAC, *Doctor*

Hader, Joan E., MD, *Doctor*

Hill, Brian E., MD, *Doctor*

Hitt, Warren, MD, *Doctor*

Nabors, William L., MD, FACS, *Doctor*

Ross, Jr., Robert R., M.D., F.A.C.S., *Doctor*

Secrest, Bradley N., MD, *Doctor*

Stout, David C., MD, *Doctor*

Respectfully submitted,

/s/ Michael Pepson

Patrick J. Massari

Michael Pepson

CAUSE OF ACTION INSTITUTE

1875 Eye Street, NW, Suite 800

Washington, D.C. 20006

Phone: 202.499.6937

Fax: 202.330.5842

michael.pepson@causeofaction.org

Admitted only in Maryland.

Practice limited to federal matters.

January 3, 2017

Counsel for Amici Curiae

TABLE OF CONTENTS

Certificate of Interested Persons	C-1
Table of Contents	i
Table of Authorities	iii
Statement of Interest	viii
Statement of Issues.....	1
Summary of Argument	1
Argument and Citations of Authority	3
I. Congress Did Not Delegate To The FTC Authority To Regulate Medical Data Security	3
II. FTC’s General Section 5 “Unfairness” Powers Must Yield To HHS’s Healthcare-Industry-Specific HIPAA Authority.....	5
III. Application Of Billing Factors Confirms The FTC Lacks Medical Data-Security Jurisdiction.....	8
A. Congress Delegated to HHS, Not to the FTC, Authority to Regulate All Alleged Practices At Issue Here	8
B. HHS Actively Exercises Regulatory Authority to Supervise All Alleged Practices At Issue Here	12
C. The FTC’s Section 5 “Unfairness” Regulation Conflicts with HHS’s Regulatory Scheme	16
1. The FTC Lacks Healthcare-Industry Expertise.....	18
2. Section 5 “Unfairness” Regulation Is Inconsistent with HHS’s Regulatory Scheme.....	20

i.	Inconsistent Record-Retention Requirements.....	20
ii.	FTC Enforcement of Section 5 Undermines The Doctor-Patient Relationship.....	22
iii.	The FTC Has Brought Enforcement Actions for Alleged Failures to Use Practices Not Required by HIPAA	23
3.	FTC Regulation Damages the Healthcare Industry.....	24
4.	Potential Future Conflicts Between HIPAA and Section 5	26
5.	No Enforcement-Related Need for Section 5 “Unfairness.”	26
D.	The Possible and Actual Conflicts Affect Practices Squarely Within the Heartland of HIPAA.....	27
IV.	Because The FTC Has No Medical Expertise, The FTC’s Intrusion Into HHS’s Domain Deserves No Deference And Should Be Rejected	27
	Conclusion	29
	Certificate of Compliance	
	Certificate of Service	

TABLE OF AUTHORITIES

Cases

<i>ABA v. FTC</i> , 430 F.3d 457 (2005)	3, 4, 8
<i>ConArt, Inc. v. Hellmuth, Obata & Kassabaum, Inc.</i> , 504 F.3d 1208 (11th Cir. 2007)	6
<i>Credit Suisse Sec. LLC v. Billing</i> , 551 U.S. 265 (2007).....	passim
<i>Dep't of Treasury v. FLRA</i> , 837 F.2d 1163 (D.C. Cir. 1988).....	28
<i>EC Term of Years Tr. v. United States</i> , 550 U.S. 429 (2007).....	6
<i>Edward J. DeBartolo Corp. v. FGCBCTC</i> , 485 U.S. 568 (1988).....	28
<i>Emplr. Sols. Staffing Grp. II v. OCAHO</i> , 833 F.3d 480 (5th Cir. 2016)	29
<i>FDA v. Brown & Williamson Tobacco Corp.</i> , 529 U.S. 120 (2000).....	4, 5
<i>Gilbert v. United States</i> , 640 F.3d 1293 (11th Cir. 2011)	5
<i>Gordon v. N.Y. Stock Exch.</i> , 422 U.S. 659 (1975).....	19, 26
<i>King v. Burwell</i> , 135 S. Ct. 2480 (2015).....	28
<i>La. Pub. Serv. Comm'n. v. FCC</i> , 476 U.S. 355 (1986).....	3

Med. Soc. of N.Y. v. Cuomo,
976 F.2d 812 (2d Cir. 1992)4

Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.,
463 U.S. 29 (1983).....29

Moyle v. Dir., Office of Workers’ Comp. Programs,
147 F.3d 1116 (9th Cir. 1998)28

Nat’l Mining Ass’n v. Sec’y of Labor,
153 F.3d 1264 (11th Cir. 1998)28

S&H Riggers & Erectors, Inc. v. OSHRC,
659 F.2d 1273 (5th Cir. 1981)20

S.C. Med. Ass’n v. Thompson,
327 F.3d 346 (4th Cir. 2003)10

SEC v. Chenery Corp.,
318 U.S. 80 (1943).....29

United States v. Estate of Romani,
523 U.S. 517 (1998).....6

United States v. Fausto,
484 U.S. 439 (1988).....6

United States v. Louwsma,
970 F.2d 797 (11th Cir. 1992)6

Util. Air Regulatory Grp. (UARG) v. EPA,
134 S. Ct. 2427 (2014).....4

Webb v. Smart Document Sols., LLC,
499 F.3d 1078 (9th Cir. 2007)9, 18

Whitman v. Am. Trucking Ass’ns., Inc.,
531 U.S. 457 (2001).....5

Rules and Statutes

15 U.S.C. § 45.....x, 4

15 U.S.C. §57a(a)(1).....19

42 C.F.R. § 493.110520

42 U.S.C. § 263a 11, 20

42 U.S.C. § 13019

42 U.S.C. § 1320d..... passim

42 U.S.C. § 1793711

45 C.F.R. § 160.10312

45 C.F.R. § 164.306(d)(3).....23

45 C.F.R. § 164.308(a)..... 20, 23

45 C.F.R. §§ 164.50120

45 C.F.R. § 164.502 21, 22

64 Fed. Reg. 59,918, 59,922 (Nov. 3, 1999)13

65 Fed. Reg. 82,462 (Dec. 28, 2000).....12

65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000).....4

65 Fed. Reg. 82,46413

68 Fed. Reg. 8,33414

68 Fed. Reg. 8,33523

71 Fed. Reg. 8,390 (Feb. 16, 2006)12

74 Fed. Reg. 42,740 (Aug. 24, 2009).....12

74 Fed. Reg. 42,962, 42,964-65 (Aug. 25, 2009)14

74 Fed. Reg. 56,123, 56,124 (Oct. 30, 2009).....10

78 Fed. Reg. 5,63914

78 Fed. Reg. 5,566 (Jan. 25, 2013).....12

Ga. Comp. R. & Regs. 111-8-10-.26 11, 21

O.C.G.A. § 31-33-2(a)(1)(A)..... 11, 21

Other Authorities

H.R. Conf. Rep. No. 104-736, at 2639

H.R. Rep. No. 104-496(I) 10, 19

H.R. Rep. No. 104-497(I)9

Andrea Arias, “The NIST Cybersecurity Framework and the FTC” (Aug. 31, 2016), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>.....27

ANTONIN SCALIA & BRYAN GARNER, *READING LAW: THE INTERPRETATION OF LEGAL TEXTS*, 327 (2012)16

“Commission Statement Marking the FTC’s 50th Data Security Settlement” (January 31, 2014), <https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>.....9

David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 351-370 (2014)19

In the Matter of TRENDnet, Inc.,
 FTC No. C-4426 (Jan. 16, 2014).....24

Int'l Harvester Co.,
104 F.T.C. 949, 1984 FTC LEXIS 2 (1984)7

L. Holst, *Precision Medicine Initiative: Data-Driven Treatments as Unique as Your Own Body*, WHITE HOUSE (Jan. 30, 2015),
<https://www.whitehouse.gov/blog/2015/01/30/precision-medicine-initiative-data-driven-treatments-unique-your-own-body>21

INTEREST OF *AMICI CURIAE*¹

Amici curiae are doctors who used the cancer-diagnostic services provided by Petitioner LabMD, Inc. (“LabMD”) to better serve their patients and Doctor David Lee Black, founder and former Chairman, President, CEO, and Director of Aegis Sciences Corporation (“Aegis”).²

Amici doctors have real-world experience practicing medicine and take their obligation to protect patients’ medical records very seriously. In many cases, critical medical decisions depend upon the proper maintenance and accuracy of those records.

For many years, the U.S. Department of Health and Human Services (“HHS”) has comprehensively regulated medical data-security practices under the

¹ Undersigned counsel and Cause of Action previously represented Petitioner pro bono before the Commission and in related federal litigation. A party’s former counsel authored this brief in whole or in part; no party nor any party’s current counsel contributed money intended to fund the brief’s preparation or submission; and no person other than *amici*’s counsel contributed money intended to fund the brief’s preparation or submission. All parties have consented to the filing of this brief.

² *Amici* are as follows: Dr. David Lee Black, Ph.D., D-ABFT, FAIC, Aegis Sciences Corporation; Dr. Bruce G. Green, MD, FAC, Urology Specialists of Atlanta; Dr. Joan E. Hader, MD, Urology Specialists of Atlanta; Dr. Brian E. Hill, MD, Urology Specialists of Atlanta; Dr. Warren Hitt, MD, Gulf Coast Regional Medical Center; Dr. William L. Nabors, MD, FACS, Urology Specialists of Atlanta; Dr. Robert R. Ross, M.D., F.A.C.S., RTR Urology; Dr. Bradley N. Secrest, MD, Hattiesburg Clinic; and Dr. David C. Stout, MD, Hattiesburg Clinic. Institutional affiliations of the individual signatories are given for purposes of identification only and do not constitute endorsement by any institution listed with respect to the contents of this brief.

Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and other laws. *Amici* are familiar with such standards and have practical experience complying.

As former LabMD clients, *amici* doctors can also offer unique insight into the practical benefits of LabMD’s cancer-detection services to not only doctors and other healthcare professionals but also their patients. For instance, LabMD’s innovative years-ahead-of-its-time business model offered improved cancer-testing accuracy, reducing the potential for life-threatening errors; reduced patient costs and eliminated labor-intensive administrative burdens for nurses and other healthcare professionals; and improved turn-around time for returning test results and providing patient medical records, which helped alleviate stress and anxiety for patients awaiting cancer-test results and, at times, saved patients an unnecessary trip to the doctor.

Amici doctors can additionally address the concrete harms to doctors and their patients caused by government overreach and regulatory abuse that destroyed a small cancer-detection laboratory (at substantial taxpayer expense) for no reason. Particularly in the current healthcare environment, patients benefit from more competition and providers of specialized cancer-diagnostic services, not less. When the Federal Trade Commission (“FTC” or “Commission”) can take a provider, such as LabMD, out of the market, it harms the very “consumers” it is

supposed to help, providing no “help” to outweigh the harm. The healthcare system does not need to be regulated by the FTC.

As both the FTC and federal jurists have recognized, whether or not the FTC has jurisdiction under Section 5 of the FTC Act, 15 U.S.C. § 45 (“Section 5”), to regulate medical data security as an “unfair” trade practice is an important question with broad practical ramifications.³ This is particularly so for healthcare providers regulated by HHS under HIPAA for two decades. FTC “unfairness” regulation is foreign to doctors, in part for the common-sense reason explained to the FTC by a federal judge in 2014: “I have gone into enough doctors’ offices and nobody has ever had me sign a statement saying that whatever the obligations are, the rights that I have under the FTC are rights that I have to acknowledge and in some cases give up. It’s always HIPAA.”⁴

Doctor Black, founder and former CEO of Aegis, a HIPAA-Covered entity that performs numerous types of laboratory testing and analysis, including workplace drug testing, prenatal monitoring, and behavioral health testing, is intimately familiar with the regulatory structure under which providers like LabMD operate. He agrees with the views and perspectives of the doctor *amici* for

³ See, e.g., Doc. 48, 1; *LabMD v. FTC*, 14-cv-00810-WSD, 2014 U.S. Dist. LEXIS 65090, *16 n.6 (N.D. Ga. May 12, 2014).

⁴ PI Tr., *LabMD v. FTC*, No. 1:14-cv-810-WSD, 90:9-13 (May 7, 2014) (RX552), <https://www.ftc.gov/system/files/documents/cases/150612labmdmtn.pdf#page=126>

the reasons stated herein. From Doctor Black's vast experience in the same field as LabMD, it is his view that the FTC does not have authority within the regulatory space for healthcare. He contends that the market is thoroughly regulated via HIPAA and other laws and regulations directly and specifically governing healthcare and affiliated providers, and does not need another player inserting itself into the complex field of medicine.

All *amici* have a strong interest in ensuring that the FTC cannot abuse its "unfairness" authority to regulate the practice of medicine by imposing new, confusing, and burdensome patient-information data-security obligations inconsistent with federal healthcare law. *Amici* doctors are extremely concerned that, given its wholesale lack of healthcare expertise, the FTC's recent decision to layer conflicting medical data-security requirements on top of those already set by federal healthcare law will endanger their patients and have a deleterious effect both on the practice of medicine and the patients whose care is entrusted to these providers.

All *amici* also have an interest in preventing the FTC from further stifling technological innovation in how healthcare is provided through abusive, *ultra vires* enforcement actions, such as here.

STATEMENT OF ISSUES

Amici will address the following question only:⁵

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

SUMMARY OF ARGUMENT

Section 5 does not give the FTC "unfairness" authority to regulate medical data security. Therefore, the FTC's assault against LabMD is *ultra vires* and cannot stand.

Congress did not choose to regulate medical records and healthcare privacy via the FTC. Instead, Congress chose to regulate medical data security and privacy through healthcare-industry-specific statutes delegating rulemaking and enforcement authority to HHS, which has necessary specialized expertise. Most significantly, in 1996, Congress enacted HIPAA, giving HHS comprehensive authority to regulate patient Protected Health Information ("PHI") data security and privacy—that is, *all* alleged practices at issue here. HHS has exercised this authority to promulgate regulations setting medical data-security standards, which HHS's Office of Civil Rights ("OCR") actively enforces.

HIPAA's regulatory structure should not conflict with Section 5, for the text of Section 5 does not authorize the FTC to regulate HIPAA-Covered entities'

⁵ *Amici* also believe that the Order against LabMD is unlawful for the reasons set forth in Petitioner's brief.

medical data security. Notwithstanding this lack of authority, as this case illustrates, the FTC has fundamentally misconstrued Section 5 to trespass on HHS's exclusive jurisdiction under HIPAA. The FTC agrees that it does not and cannot enforce HIPAA, which is exclusively administered by HHS, and that LabMD was regulated by HHS as a Covered Entity under HIPAA. HHS did not join the FTC's in-house administrative prosecution of LabMD, even though FTC staff repeatedly reached out to HHS about a criminal third party's theft of a LabMD file as part of an extortion scheme. Yet the FTC, which does not recognize HIPAA compliance as a defense against Section 5, deemed LabMD's medical data security "unreasonable" and therefore an "unfair" trade practice banned by Section 5.

Because the *FTC's misinterpretation* of Section 5 is incompatible with the administrative structure Congress created to regulate medical data security, and contrary to Section 5's plain language and the U.S. Constitution, it should be rejected, based upon application of the preclusion factors articulated by the Supreme Court in *Credit Suisse Sec. LLC v. Billing*, 551 U.S. 265 (2007).

Unless this Court rejects the Commission overreach here, the FTC's lack of medical expertise will, as a practical matter, endanger patient welfare and stifle healthcare innovation. The FTC's position that it is allowed to dictate to doctors what medical data-security practices should be used beyond that which HIPAA

requires through *ad hoc* after-the-fact “we-know-‘unfair’-and-‘unreasonable’-data-security-when-we-see-it” enforcement actions concretely harms the practice of medicine.

This Court should vacate the Order against LabMD *in toto* and make pellucidly clear to the FTC that it lacks authority to “parachute in” without Congress’s permission or relevant expertise to interfere with how doctors treat patients.

ARGUMENT AND CITATIONS OF AUTHORITY

I. CONGRESS DID NOT DELEGATE TO THE FTC AUTHORITY TO REGULATE MEDICAL DATA SECURITY.

Because Congress has not conferred power upon the FTC to regulate medical data security, the FTC lacks authority to do so.⁶ *See La. Pub. Serv. Comm’n. v. FCC*, 476 U.S. 355, 374 (1986); *ABA v. FTC*, 430 F.3d 457, 468-69 (2005); *see also FTC v. LabMD*, No.1:12-cv-3005-WSD, Dkt. 23, at 14 (N.D. Ga. Nov. 26, 2012) (“[T]he Court finds there is significant merit to ... [LabMD’s] argument that Section 5 does not justify an investigation into data security practices[.]”).

⁶ The FTC’s lack of jurisdiction was repeatedly raised below. *See, e.g.*, Doc. 147, 9-10.

Section 5 says nothing about medical data security, silently refuting the FTC's newfound "unfairness" power claims,⁷ which should be greeted skeptically. *See Util. Air Regulatory Grp. (UARG) v. EPA*, 134 S. Ct. 2427, 2444 (2014); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 159-60 (2000). The 1938 Wheeler-Lea Amendments to the FTC Act, which added a prohibition against "unfair ... acts or practices" to Section 5(a),⁸ 15 U.S.C. § 45(a), do not implicitly delegate to the FTC authority to regulate healthcare privacy.⁹ Nor do the 1994 Amendments to the FTC Act, which added Section 5(n), 15 U.S.C. § 45(n), to "rein in" FTC's Section 5 "unfairness" abuse. *See* Doc. 326, 47-48.

If Congress wanted the FTC to regulate data security for the entire healthcare industry, it would have clearly and expressly assigned the FTC that economically and politically important task. *See UARG*, 134 S. Ct. at 2444. Congress, however, did the opposite, last amending Section 5 to *limit* the FTC's "unfairness" authority. *See* Doc. 326, 47-48. Congress did not give the FTC medical data-security authority through statutory amendments specifically intended

⁷ It is unclear when the FTC first purportedly "discovered" Section 5 "unfairness" authority to regulate HIPAA-Covered entities. The Commission linked this "discovery" to settlements occurring in 2009-2010. Doc. 48, 11 n.18.

⁸ Wheeler-Lea Act, Pub. L. 75-447, § 5, 52 Stat. 111 (1938).

⁹ Regulation of healthcare and privacy is traditionally a local matter. *See* 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000); *Med. Soc. of N.Y. v. Cuomo*, 976 F.2d 812, 816 (2d Cir. 1992). The FTC's overreach here without clear congressional permission violates federalism. *Cf. ABA v. FTC*, 430 F.3d at 471-72.

to narrow the FTC's powers.¹⁰ *Whitman v. Am. Trucking Ass'ns., Inc.*, 531 U.S. 457, 468 (2001). The FTC's blatant power grab should be rejected for this reason alone.

II. THE FTC'S GENERAL SECTION 5 "UNFAIRNESS" POWERS MUST YIELD TO HHS'S HEALTHCARE-INDUSTRY-SPECIFIC HIPAA AUTHORITY.

The FTC's *ultra vires* foray into healthcare should also be rejected for a more practical reason: Because Section 5 "unfairness," *as interpreted by the FTC*, is incompatible with more recent healthcare-sector-specific statutes like HIPAA, the FTC must yield.

More recent and specific statutes trump older and/or more general statutes.¹¹ *Gilbert v. United States*, 640 F.3d 1293, 1308 (11th Cir. 2011) (en banc) ("[G]eneral statutory provision enacted at an earlier time must yield to a specific and clear provision enacted at a later time."); *see, e.g., Credit Suisse Sec. LLC v. Billing*, 551 U.S. 265, 275-76, 279, 282 (2007) (preclusion even where mere "threat" that applying earlier-enacted statute would require certain parties to avoid actions later-enacted statute "permits or encourages"); *United States v. Louwsma*,

¹⁰ Instead, "Congress ... spoke[] subsequently and more specifically to the topic," *Brown & Williamson*, 529 U.S. at 133, through statutes like HIPAA. FTC "ignor[es] the plain implication of" this. *Id.* at 160.

¹¹ *Cf. Morton v. Mancari*, 417 U.S. 535, 550-51 (1974) (Generally, "specific statute will not be controlled or nullified by ... general one, regardless of the priority of enactment.").

970 F.2d 797, 799-800 (11th Cir. 1992) (illustrating principle); *see also EC Term of Years Tr. v. United States*, 550 U.S. 429, 433-36 (2007).

This principle has special force where, as here, the source of conflict is not the statutory language itself but a bizarre, sweeping misinterpretation of that language. *See, e.g., United States v. Fausto*, 484 U.S. 439, 453 (1988) (presumption against implied repeal inapplicable). Implied repeal will readily be found where the interpretation of the earlier-enacted statute creating the conflict with the later-enacted one does not appear in the “express statutory text.” *Id.* So too here.

The reason why Section 5, *as interpreted by the FTC*, irreconcilably conflicts with HIPAA and other law is that the FTC has misread its “unfairness” authority to somehow encompass practices regulated under HIPAA.¹² Here, the circumstances surrounding the FTC’s “discovery” of authority to overfile HHS illustrates how the FTC created irreconcilable conflict by (1) misreading Section 5 to extend to medical data security, and (2) compounding that error by layering on new, inconsistent, and ever-shifting compliance obligations.

Section 5, the older general statute, was last amended in 1994 to narrow the FTC’s “unfairness” powers through Section 5(n). *See* Doc. 326, 47-48. The FTC

¹² *Cf. United States v. Estate of Romani*, 523 U.S. 517, 530 (1998); *ConArt, Inc. v. Hellmuth, Obata & Kassabaum, Inc.*, 504 F.3d 1208, 1210 (11th Cir. 2007) (reading general statute not to extend to matters covered by specific statute, consistent with implied-repeals canon).

states that Section 5(n) is “derived from the Commission’s 1980 *Policy Statement on Unfairness*” and “codifies ... [its] analytical framework[.]” Doc. 355, Op. 9 (citing Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) (“Unfairness Statement”), appended to *Int’l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2, at *304 (1984)). In its “Unfairness Statement” the FTC told Congress that, “[o]f course, if matters involving health and safety are within the primary jurisdiction of some other agency, Commission action might not be appropriate.” Unfairness Statement, 1984 FTC LEXIS 2, at *308 n.15. Congress presumably took the FTC at its word.

HIPAA, the more recent and specific statute (dealing with “matters involving health”), was enacted two years later in 1996—but, importantly, *almost ten years before* the FTC first claimed Section 5 “unfairness” data-security authority in 2005.¹³

Consequently, the Congress that enacted HIPAA could not have anticipated, except through divination, that the FTC would ever claim “unfairness” medical data-security authority. There was no conflict then between Section 5 and HIPAA because the FTC had not asserted jurisdiction.

¹³ See FTC Opposition to Stay Motion, *LabMD v. FTC*, No. 16-16270, at 4 (Oct. 18, 2016) (dating the FTC’s discovery of “unfairness” data-security authority to 2005).

Therefore, it is unsurprising that Congress did not include language in HIPAA specifically exempting HIPAA-Covered entities from Section 5. But this does not suggest that the FTC has authority here, as it apparently assumes. Doc. 48 (“January 16 Order”), 12. *Cf. ABA v. FTC*, 430 F.3d at 468-69 (rejecting precisely such an FTC assumption).

III. APPLICATION OF *BILLING* FACTORS CONFIRMS THE FTC LACKS MEDICAL DATA-SECURITY JURISDICTION.

Application of the four preclusion factors articulated by the Supreme Court in *Credit Suisse Sec. LLC v. Billing* to the FTC’s overreach here confirms that the FTC currently lacks “unfairness” authority to regulate medical data security, even if there were an argument that such authority existed prior to Congress’s enactment of HIPAA.¹⁴ *See* 551 U.S. at 275-76 (listing factors for finding “clear repugnancy” between two regulatory regimes).

A. Congress Delegated to HHS, *Not to the FTC*, Authority to Regulate *All* Alleged Practices At Issue Here.

Congress intentionally and specifically gave a different agency, HHS, comprehensive statutory authority to regulate “all of the activities here in question.” *Id.* at 276. Therefore, the first *Billing* factor, “the existence of regulatory authority under ... [other] law to supervise the activities in question,” *id.* at 275, is met.

¹⁴ The Commission acknowledged *Billing* controls but misapplied *Billing* preclusion analysis. *See* Doc. 48, 12-13.

In 1996, Congress enacted HIPAA,¹⁵ tasking HHS with regulating medical data security. HIPAA addressed security, privacy, and various administrative-simplification issues through certain “Administrative Simplification” provisions.¹⁶ The purpose of those provisions is to improve “the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.” HIPAA, § 261, 110 Stat. at 2021 (codified at 42 U.S.C. § 1320d note); *see also* H.R. Rep. No. 104-497(I), at 98-100 (1996). *See generally* *Webb v. Smart Document Sols., LLC*, 499 F.3d 1078, 1083-84 (9th Cir. 2007).

In light of the FTC’s then-understood lack of Section 5 “unfairness” data-security authority,¹⁷ Congress recognized there was “no provision” in “present law” governing the matters addressed in HIPAA’s Administrative Simplification provisions. *See* H.R. Conf. Rep. No. 104-736, at 263; *see also* H.R. Rep. No. 104-

¹⁵ Pub. L. No. 104-191, 110 Stat. 1936 (1996); *see also* 45 C.F.R. Pts. 160-64 (implementing regulations).

¹⁶ Set forth in Subtitle F of Title II of HIPAA in sections 261 through 264. HIPAA § 262 amends Title XI of the Social Security Act, 42 U.S.C. § 1301 et seq., to add a Part C, entitled “Administrative Simplification,” with sections 1171-1179 codified at 42 U.S.C. §§ 1320d-1320d-8.

¹⁷ Even according to the “Commission Statement Marking the FTC’s 50th Data Security Settlement” (January 31, 2014), <https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>, FTC’s data-security activities “started in 2002 with a single case.”

496(I) at 97-98 (recognizing same and adoption of standards generally). Congress understood that HHS would be required to “establish” *for the first time* medical data-security and privacy standards. *See* H.R. Rep. No. 104-496(I) at 67 (referring to “establishment of standards and requirements for the electronic transmission of certain health information”), 100 (“The Secretary would be required to establish security standards[.]”). To this end, HIPAA authorized HHS to set such standards through regulations and to enforce those standards. *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1) (“Security standards for health information”); *see S.C. Med. Ass’n v. Thompson*, 327 F.3d 346, 348-49 (4th Cir. 2003) (HHS’s role in setting standards).

Congress buttressed HHS’s medical data-security authority in 2009 by passing the Health Information Technology for Economic and Clinical Health Act (“HITECH”),¹⁸ which expanded HIPAA’s reach and HHS’s role. *See, e.g.*, 42 U.S.C. § 1320d-2(i); *see* 74 Fed. Reg. 56,123, 56,124 (Oct. 30, 2009). In HITECH, Congress drew a bright line between *non*-HIPAA-Covered and HIPAA-Covered entities, carefully avoiding delegating to the FTC *any* authority to regulate HIPAA-Covered entities. For instance, § 13422(b)(1) directs HHS, in coordination with the FTC, to study data-security requirements only for *non*-HIPAA-Covered entities and determine “which Federal government agency is best equipped to enforce [any] such requirements.” Pub L. 111-5, § 13422(b)(1), 123 Stat. 260, 277

¹⁸ American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, Div. A, Title XIII, and Div. B, Title IV (HITECH) (codified at 42 U.S.C. §§ 1320d-5 *et seq.*).

(Feb. 17, 2009). Likewise, Congress only authorized the FTC to set and enforce data-breach notification requirements for *non*-HIPAA-Covered entities. *See* 42 U.S.C. § 17937; Doc. 48, 12 n.20. HITECH thus underscores Congress’s determination, codified in HIPAA, that medical data security is the exclusive purview of HHS.

With respect to clinical laboratories like LabMD, HIPAA supplemented the authority that Congress previously granted HHS to regulate medical-record retention and related matters through the Clinical Laboratory Improvement Amendments of 1988 (“CLIA”).¹⁹ CLIA directs HHS to set standards, 42 U.S.C. § 263a(f)(1), meeting certain specified requirements, *see* 42 U.S.C. § 263a(f)(1)(A)-(D), after considering certain factors, *see* 42 U.S.C. § 263a(f)(2)(A)-(G).

The FTC does not, and cannot, administer any of these laws. The FTC admits it does not, and cannot, enforce HIPAA, Doc. 48, 12 & n.19, which comprehensively regulates *all* alleged practices at issue here. The FTC also agrees that “LabMD ... is subject to HIPAA.” Doc. 355, Op. 12 n.22. Consequently, what the Commission Opinion refers to as “sensitive health or medical information,” *see* Doc. 355, Op. 19, 25, is PHI, exclusively subject to HIPAA medical data-security standards set by HHS’s Security and Privacy Rules, 45

¹⁹ Pub. L. 100-578, 102 Stat. 2903 (codified at 42 U.S.C. § 263a). State law imposes additional record-retention requirements. *See* O.C.G.A. § 31-33-2(a)(1)(A); Ga. Comp. R. & Regs. 111-8-10-.26.

C.F.R. § 160.103 (defining “PHI” and Electronic PHI (“ePHI”), the subset of PHI at issue here).

This factor favors preclusion.

B. HHS Actively Exercises Regulatory Authority to Supervise *All* Alleged Practices At Issue Here.

HHS comprehensively and actively regulates *all* medical data-security practices at issue here. HHS “has continuously exercised its legal authority to regulate conduct of the general kind now at issue” and “defined in detail” what medical data-security practices HIPAA-Covered entities like LabMD may use. *See Billing*, 551 U.S. at 277. The second *Billing* factor, “evidence that the responsible regulatory entities exercise that authority,” *id.* at 275, is therefore satisfied.

As instructed by Congress, 42 U.S.C. § 1320d-2(d)(1), HHS has exercised its authority under HIPAA to promulgate regulations establishing medical data-security standards. *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”), 65 Fed. Reg. 82,462 (Dec. 28, 2000); Health Insurance Reform: Security Standards (“Security Rule”), 68 Fed. Reg. 8,334 (Feb. 20, 2003); HIPAA Administrative Simplification: Enforcement (“Enforcement Rule”), 71 Fed. Reg. 8,390 (Feb. 16, 2006); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (“HIPAA Omnibus Final Rule”), 78 Fed. Reg. 5,566 (Jan. 25, 2013); *see also* HITECH Breach Notification Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009).

The preambles to HHS’s Security and Privacy Rules showcase the general understanding that the FTC lacks Section 5 “unfairness” data-security authority that prevailed until the FTC reversed course without explanation (or notice to the public).

For instance, the Privacy Rule preamble explains that it “establishes, for the first time, a set of basic national privacy standards and fair information practices....”²⁰ 65 Fed. Reg. at 82,464. Tellingly, the Privacy Rule’s extensive implied-repeal analysis omits mention of the FTC’s then-“undiscovered” Section 5 “unfairness” powers but addresses the FTC’s financial-sector-specific data-security regulatory authority under the Gramm-Leach-Bliley Act. *See id.* at 82,483-84 (no conflict because “health plans will not be subject to dual federal agency jurisdiction”). This omission is unsurprising given that the Privacy Rule was promulgated against the backdrop of the FTC’s then-public disavowal of Section 5 “unfairness” data-security authority—at the time, the two agencies were in agreement as to the FTC’s limitations.²¹

²⁰ Notably, in developing its proposed rule, HHS consulted with statutorily-specified groups and other key stakeholders (including various federal agencies), which did not include the FTC. *See* 64 Fed. Reg. 59,918, 59,922 (Nov. 3, 1999).

²¹ *See* Doc. 18, 16-17 & nn.12-14, <https://www.ftc.gov/sites/default/files/documents/cases/131112respondlabmdmodiscomplaintdatyadminproceed.pdf#page=18> (listing FTC statements).

The 2003 HIPAA Security Rule also predates the FTC’s “discovery” of medical data-security authority.²² “The purpose of” the Rule was “to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.” 68 Fed. Reg. at 8,334; *see also* HHS, Security 101 for Covered Entities, HIPAA Security Series, Vol. 2/Paper 1, 3 (2007) (“Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry.”). Significantly, the Security Rule also omits mention of Section 5.

Also consistent with Congress’s decision that HHS alone regulates HIPAA-Covered entities, “[b]oth HHS (pursuant to HIPAA and HITECH) and the FTC (pursuant to the American Recovery and Reinvestment Act of 2009) have promulgated [breach notification] regulations ... [that] are applicable to two different categories of firms.... [T]h[e] FTC rule does not apply to HIPAA-covered entities[.]”²³ Doc. 48, 12 n.20.

²² *See supra* note 7.

²³ The HIPAA Omnibus Rule notes that “HIPAA covered entities and business associates are subject to HHS,’ and not the FTC’s, breach notification rule.” 78 Fed. Reg. at 5,639; *accord* FTC Health Breach Notification Rule, 74 Fed. Reg. 42,962, 42,964-65 (Aug. 25, 2009) (same).

Honoring Congress's intent, HHS's OCR actively enforces HIPAA. *See generally* HHS, Enforcement Highlights (Nov. 30, 2016).²⁴ "OCR has received over 144,662 HIPAA complaints[]" and "ha[s] resolved ninety-seven percent of these cases (141,235)." *Id.* "OCR has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates noncompliance[.]" *Id.* OCR has referred 589 HIPAA-related matters to DOJ for criminal investigation, *see id.*, and increasingly coordinates with State Attorneys General to bring HIPAA civil enforcement actions.²⁵ OCR also initiates HIPAA compliance reviews²⁶ and audits,²⁷ routinely enters into resolution agreements, and has civil-penalty authority.²⁸

²⁴ *At* <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html?language=es>.

²⁵ *See generally* HHS, State Attorneys General, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html>.

²⁶ HHS, How OCR Enforces the HIPAA Privacy & Security Rules, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html>.

²⁷ *See, e.g.*, HHS, HIPAA Privacy, Security, and Breach Notification Audit Program, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html>.

²⁸ *See* HHS, Resolution Agreements, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>.

Put simply, all alleged practices at issue here are already comprehensively (and actively) regulated by HHS.²⁹ This *Billing* factor also favors preclusion.

C. The FTC’s Section 5 “Unfairness” Regulation Conflicts with HHS’s Regulatory Scheme.

The third *Billing* factor is whether there is “a resulting risk that” two different regulatory schemes enforced by different agencies, “if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct.”³⁰ 551 U.S. at 275-76. Notably, the *Billing* Court did not require inconsistent standards *as applied to the alleged underlying conduct* to conclude that this factor was met, instead assuming *arguendo* violations of both the specific securities laws and general antitrust laws.³¹ *See id.* at 279. The third *Billing* factor is therefore satisfied by a showing of *potential* (not necessarily *actual*) conflict. *See id.* at 280-84. Here, this test is more than met, as the FTC’s misinterpretation

²⁹ Commissioner McSweeney noted this at oral argument: “Aren’t we talking about HIPAA-covered documents, medical records, and hopefully state standards here as well?” Transcript Event (“TE”) 56, 46:19-23.

³⁰ The Commission misreads *Billing*, suggesting that preclusion obtains only where compliance with both laws is impossible. *See* Doc. 48, 12-13. Not so. For instance, under *Billing*, conflict may be found where one statute “forbid[s] the very thing that the [other statute] ... permit[s].” 551 U.S. at 273; *accord* ANTONIN SCALIA & BRYAN GARNER, *READING LAW: THE INTERPRETATION OF LEGAL TEXTS*, 327 (2012) (same).

³¹ The Commission misapplied *Billing*, erroneously finding that actual as-applied inconsistency is required. *See* Doc. 48, 12-13. Even (counterfactually) taking as true the FTC’s factually and legally inaccurate claims about LabMD, the third *Billing* factor is still met. Petitioner’s brief addresses such errors in detail.

of Section 5 has created numerous actual and potential conflicts between Section 5 and federal healthcare law.

The root of the repugnancy is the FTC's view that "the requirements imposed by HIPAA do not govern whether LabMD met its obligations under Section 5 of the FTC Act[.]" Doc. 355, Op. 12. Indeed, the Commission rejected the "legal argument" that "the Commission could not hold LabMD liable under Section 5 if its data security practices complied with HIPAA Standards." Doc. 147, 5. FTC does not recognize HIPAA compliance as a safe harbor or defense against Section 5. Doc. 48, 12-13.

Worse, the FTC does not claim that Section 5 *is consistent with* HIPAA, instead asserting that Section 5 is "*largely consistent*" with HIPAA. Doc. 48, 11 (emphasis added). "Largely consistent" is not the same as "consistent." And the FTC refuses to say how, precisely, its unstated "standards" diverge from HIPAA standards.

Here, the fact that the FTC acknowledges that LabMD "is subject to HIPAA," Doc. 355, Op. 12 n.22, but claimed that "this case has nothing to do with HIPAA," *see* Doc. 147, 5 (citation omitted), yet found LabMD liable under Section 5 showcases the risk (and reality) of regulatory conflict. Underscoring this, even though FTC staff repeatedly reached out to HHS about a third party's theft of

LabMD's 1718 File over a period of several years, HHS declined to join the FTC enforcement action against LabMD.³²

This risk (and reality) of conflict is further illuminated through the lens of five principles the *Billing* Court focused on to determine that the third factor was met, *see* 551 U.S. at 279-83 (illustrating principles), all of which apply here, as discussed below.

1. The FTC Lacks Healthcare-Industry Expertise.

Under *Billing*, a “need for [industry]-related expertise” to effectively regulate, *id.* at 283, 285, weighs in favor of preclusion.

Healthcare regulation is incredibly complex, and specialized expertise is necessary to further HIPAA's broad purpose. *See generally Webb*, 499 F.3d at 1083-84 (summarizing purpose). HIPAA “emphasizes privacy, efficiency, and modernization” and the broader “goals of improving the operation of the health care system and reducing administrative costs[.]”³³ *Id.* at 1084 (citations omitted).

Recognizing the need for healthcare-industry-specific expertise to achieve these

³² *See* Doc. 359, Ex.36, <https://www.ftc.gov/system/files/documents/cases/160830labmdstayapplication.pdf#page=1114>; Doc. 364, Ex.4, <https://www.ftc.gov/system/files/documents/cases/160915replyccoppstay.pdf#page=39>.

³³ LabMD's cancer-detection services furthered these goals. *See CX0225* (detailing how LabMD enhanced efficiency and modernization, improved operations, and reduced administrative costs); TE 40, 954-964 (benefits of LabMD services).

goals, Congress required HHS to consult with specified groups and engage with key stakeholders to implement HIPAA through notice-and-comment rulemaking. *See* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 351-370 (2014) (describing process); *see also* H.R. Rep. No. 104-496(I) at 99 (recognizing role of private sector in establishing standards). Through that public process, HHS established healthcare-industry-specific standards.

By contrast, the FTC, a generalist agency without industry-specific expertise, solely focuses on “reasonable” data security for its own sake *in vacuo*. *Cf. Gordon v. N.Y. Stock Exch.*, 422 U.S. 659, 688-90 (1975). Worse, unlike HHS, the FTC has eschewed using its formal rulemaking powers to set standards, *see* 15 U.S.C. §57a(a)(1), instead resorting to *ex post* enforcement actions. And unlike HHS, the FTC refuses even to tailor its expectations to particular industries. *See, e.g.*, Doc. 355, Op. 12 (referring to practices “IT practitioners commonly used”).

Thus, the FTC rejected HIPAA standards in this case. *See* Doc. 147, 5 (“[T]his case has nothing to do with HIPAA.”); Doc. 48, 12-13. Indeed, the FTC’s sole data-security expert witness admitted at trial that she “did not understand” HIPAA: “I can’t make a statement or—about the legal aspects of HIPAA and what it governs. I don’t understand the legal aspects of what it governs.” TE 36, 231 (Dr. Raquel Hill); *accord* RX525, 52:16-19 (FTC Bureau of Consumer Protection Deputy Director Daniel Kaufman: “I’m sorry, what is HITECH?”). Such

breathhtaking after-the-fact departures from industry-specific standards violate due process, *cf. S&H Riggers & Erectors, Inc. v. OSHRC*, 659 F.2d 1273, 1283-85 (5th Cir. 1981), and underscore the FTC’s lack of medical expertise.

2. Section 5 “Unfairness” Regulation Is Inconsistent with HHS’s Regulatory Scheme.

Where permitting two separate regulatory regimes—one expert and one non-expert—undermines consistency and creates a risk of arbitrary enforcement, *see Billing*, 551 U.S. at 281-82, conflict is more likely, and the non-expert regime must fall. So too here, as illustrated below.

i. Inconsistent Record-Retention Requirements.

FTC and HHS set different record-retention expectations.

For obvious reasons, HIPAA, CLIA, and state laws set minimum, as opposed to maximum, medical-record retention requirements.³⁴ For instance, HIPAA gives patients a six-year right of access to PHI in “Designated Record Sets,” which could be virtually all PHI collected by a Covered entity. *See* 45 C.F.R. §§ 164.501 (defining term), 164.524 (right of access), 164.530(j)(2) (six-year retention). CLIA and state laws set additional minimum record-retention requirements. *See* 42 U.S.C. § 263a; 42 C.F.R. § 493.1105 (CLIA record-retention

³⁴ The Security Rule also ensures patient-record accessibility, requiring maintenance of exact copies and emphasizing accessibility of records in emergencies. *See* 45 C.F.R. §§ 164.308(a)(7)(ii)(A)-(B) (required data-backup and disaster-recovery plans).

requirements); O.C.G.A. §31-33-2(a)(1)(A) (ten-year record-retention requirement); Ga. Comp. R. & Regs. 111-8-10-.26 (state law requirements). Indeed, the Privacy Rule requires compliance with respect to certain PHI for *fifty* years. *See* 45 C.F.R. § 164.502(f).

As this Court noted, LabMD is legally obligated to preserve patient files. Stay Order, *LabMD v. FTC*, No. 16-16270-D, at 12 (Nov. 10, 2016) (LabMD “only ... currently possesses” records “it is required by law to keep”). For good reason: preserving medical records benefits patients. To use LabMD’s field as an example, prostate cancer often develops slowly. TE 44, 1031:8-21 (explaining why LabMD retains slides and test results for physician access). Access to lab records from ten years previous in order to compare to current test results can provide life-saving information. Without that historical baseline, treatment decisions can be difficult or impossible. More generally, healthcare is moving toward a “precision” or “personalized” medicine model, which emphasizes long-term retention of patient information to provide customized, cost-effective healthcare.³⁵

Yet the FTC *faulted* LabMD for not destroying patient medical records. *See* Doc. 355, Op. 1, 15; *see also id.* at 4 (LabMD “continues to preserve tissue

³⁵ *See* L. Holst, *Precision Medicine Initiative: Data-Driven Treatments as Unique as Your Own Body*, WHITE HOUSE (Jan. 30, 2015), <https://www.whitehouse.gov/blog/2015/01/30/precision-medicine-initiative-data-driven-treatments-unique-your-own-body>.

samples and provide past test results to healthcare providers.”). The FTC’s medical-records-destruction mandate conflicts with federal law and defies logic.³⁶

FTC hubris in medical matters, vividly displayed here in its singular Javert-like obsession with destroying LabMD, should not be rewarded.

ii. FTC Enforcement of Section 5 Undermines The Doctor-Patient Relationship.

The Commission also criticized LabMD for possessing patient data even if no tests were performed. Doc. 355, Op. 26 n.74. This, too, is inconsistent with HIPAA, as well as HHS regulations and guidance—none of which limit PHI data collection.³⁷ FTC’s patient-information-minimization mandate is anathema to the healthcare industry, where patient health and family history, demographic information, payment information, social security information, and the like are all relevant.

³⁶ See also FTC, Start with Security: A Guide For Business (“Start with Security”), 2 (June 2015) (describing enforcement action where company allegedly wrongfully retained data for 30 days).

³⁷ Instead, the HIPAA “minimum necessary” concept only applies to “disclosure” or “use” of PHI. See 45 C.F.R. §164.502(b)(1). Notably, this does not apply to disclosures to or requests by a healthcare provider for treatment, see 45 C.F.R. §164.502(b)(2), because patients benefit when their doctors have *more access* to information, *not less*.

iii. The FTC Has Brought Enforcement Actions for Alleged Failures to Use Practices Not Required by HIPAA.

Because the FTC’s “unfairness” data-security regulation starts from a different premise than HIPAA, the FTC has brought enforcement actions for practices permitted by HIPAA.

HHS designed the Security Rule to be “scalable, so that it can be effectively implemented by covered entities of all types and sizes.”³⁸ 68 Fed. Reg. at 8,335. To this end, HHS created a unique, technologically-neutral information-security regulatory scheme that separates “implementation specifications” into two classes: “required” (i.e., mandatory) and “addressable” (i.e., *not* necessarily required). *See id.* at 8,336. Thus, the lodestar of HIPAA compliance is a good-faith “risk analysis,” 45 C.F.R. § 164.308(a)(1)(ii)(A), which allows Covered entities to determine for themselves which, if any, “addressable” implementation specifications should be used. *See* 45 C.F.R. § 164.306(d)(3) (describing process).

The FTC, however, apparently views “addressable” specifications under HIPAA as being “required” by Section 5, seemingly viewing use of certain specific technologies as mandatory under the FTC Act. The FTC’s enforcement approach is thus fundamentally incompatible with that of HHS, as the Commission was

³⁸ HIPAA directed HHS to consider, *inter alia*, “the costs of security measures” and “needs and capabilities of small ... and rural health care providers.” 42 U.S.C. §1320d-2(d)(1)(A).

made well aware of below but ignored.³⁹ For instance, the FTC has brought enforcement actions for *allegedly* not using practices that are neither “required” nor even specifically addressed by the HIPAA Security Rule,⁴⁰ such as “penetration testing,”⁴¹ “limiting administrator access,”⁴² and “guarding against brute force attacks.”⁴³ This list is illustrative, not exhaustive.⁴⁴

3. FTC Regulation Damages the Healthcare Industry.

Under *Billing*, “clear repugnancy” is more likely where, as here, overlapping regulation potentially damages a specialized industry. *See* 551 U.S. at 179.

FTC regulation of HIPAA-Covered entities harms doctors, other professionals and providers, and patients, as demonstrated by the FTC’s

³⁹ Healthcare data-security expert Cliff Baker has explained why Section 5 “unfairness” and HIPAA are incompatible. The Commission is well aware of Mr. Baker’s Expert Opinion Declaration and testimony, *see, e.g.*, Doc. 147, 7 (discussing Baker Declaration), which are posted on FTC’s website. *See* Doc. 96, Ex.12, <https://www.ftc.gov/system/files/documents/cases/140423labmdsummarymtn.pdf#page=163> (Declaration); Proposed RX552, 58:10-69:13, <https://www.ftc.gov/system/files/documents/cases/150612labmdmtn.pdf#page=94> (Testimony).

⁴⁰ None involved an admission or finding of liability, as all were resolved through settlements.

⁴¹ *See, e.g.*, Compl., ¶ 8.d.i.2, *In the Matter of TRENDnet, Inc.*, FTC No. C-4426 (Jan. 16, 2014).

⁴² *See* Start with Security at 4.

⁴³ *See id.* at 5.

⁴⁴ Healthcare expert Cliff Baker has documented additional examples of broad and specific conflicts. *See supra* note 39.

destruction of LabMD for no reason other than “because we can,” and as illustrated in Sections I.C.3.i-ii, above. More generally, as U.S. District Judge William S. Duffey, Jr., explained to the FTC:

[T]here are no security standards from the FTC....

[H]ow does any company ... operate when they are trying to focus on what HIPAA requires and to have some other agency parachute in and say, well, I know that’s what they require, but we require something different, and some company says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did....⁴⁵

Healthcare providers are already heavily regulated by HHS and subject to complex federal compliance requirements, as well as state law, which may have separate privacy and breach notification regimes. This is an onerous burden. Superimposing an additional layer of FTC *ad hoc*, standardless enforcement is unnecessary and counterproductive. HHS’s regulatory regime was developed with extensive stakeholder input and is applied consistently and predictably, creating a climate well-suited to emerging technological advances. Conversely, allowing the FTC to recklessly wield its unpredictable Section 5 Sword of Damocles chills healthcare innovation, hampering patient care.

⁴⁵ Doc. 132, Ex. 1, PI Hearing Tr., *LabMD v. FTC*, No. 1:14-cv-810-WSD, at 94:14-24 (May 7, 2014).

4. Potential Future Conflicts Between HIPAA and Section 5.

Since HHS has discretion to change HIPAA’s regulatory regime, *see, e.g.*, 42 U.S.C. §1320d-2(i)—and the FTC’s “unfairness” regulation is ever-shifting on a case-by-case basis—there will always be a risk of future conflict until the FTC is judicially barred from “parachuting in” to HHS’s domain. *Cf. Gordon*, 422 U.S. at 690-91 (finding preclusion based on risk of future conflict, regardless of current compatibility). The concrete risk of ongoing, even escalating, conflict is underscored by the reality that HHS’s healthcare-related policies may materially change under the new Administration, while the FTC is an “independent” Commission less accountable to the Executive. This also weighs in favor of preclusion. *Cf. Billing*, 551 U.S. at 273, 280-81; *Gordon*, 422 U.S. at 688.

5. No Enforcement-Related Need for Section 5 “Unfairness.”

Finally, preclusion is appropriate where, as here, “any enforcement-related need for” the general statute “is unusually small” because of active regulation by a different agency under industry-specific statutes. *See Billing*, 551 U.S. at 283. As discussed in Section III.B, “any enforcement-related need for” FTC regulation here “is unusually small” because of comprehensive HHS regulation and active, rigorous OCR enforcement. The FTC brings far fewer Section 5 “unfairness”

actions (“settling” no more than 60 so far)⁴⁶ than OCR (24,000-plus resolved with corrective action and/or technical assistance),⁴⁷ relying instead on an *in terrorem* approach.

D. The Possible and Actual Conflicts Affect Practices Squarely Within the Heartland of HIPAA.

The fourth *Billing* factor is whether “the possible conflict [between two regulatory regimes] affect[s] practices that lie squarely within an area of ... activity that the ... [specific] law seeks to regulate.” *Billing*, 551 U.S. at 276. Here, as explained above, the medical data-security practices the FTC seeks to regulate “lie squarely within” the area regulated by HHS under HIPAA, HITECH, and CLIA, and are “central to the proper functioning” of those statutory schemes. *Cf. id.* Therefore, this factor is met and thus all *Billing* factors favor preclusion.

IV. BECAUSE THE FTC HAS NO MEDICAL EXPERTISE, THE FTC’S INTRUSION INTO HHS’S DOMAIN DESERVES NO DEFERENCE AND SHOULD BE REJECTED.

Because the Commission admits that it does not, and cannot, enforce HIPAA or HITECH, Doc. 48, 12 & n.19, neither of which Congress entrusted the FTC to

⁴⁶ See Andrea Arias, “The NIST Cybersecurity Framework and the FTC” (Aug. 31, 2016), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>. The exact number of pure “unfairness” settlements is unclear; some such matters are primarily or exclusively brought under the FTC’s “deception” authority.

⁴⁷ See HHS, Enforcement Highlights (Nov. 30, 2016), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html?language=es>.

administer, this Court owes no deference to the FTC's recent "discovery" of "unfairness" authority to regulate HIPAA-Covered entities, *see Dep't of Treasury v. FLRA*, 837 F.2d 1163, 1167 (D.C. Cir. 1988). Courts "owe no deference to an agency's resolution of statutory conflicts that implicate legislation that is not administered by that agency." *Moyle v. Dir., Office of Workers' Comp. Programs*, 147 F.3d 1116, 1119 (9th Cir. 1998). Under this principle, courts "must independently resolve conflicts between statutes administered by one agency and regulations promulgated by another agency." *Id.* So too here.

Deference to agencies is based, in part, on perceived agency expertise. *But cf. Nat'l Mining Ass'n v. Sec'y of Labor*, 153 F.3d 1264, 1267 (11th Cir. 1998) ("[W]e need not defer to issues beyond the agency's expertise."). Here, however, the FTC lacks necessary medical expertise and thus no deference is due. *See, e.g., King v. Burwell*, 135 S. Ct. 2480, 2489 (2015) (denying deference because IRS "has no expertise in crafting health insurance policy").

The federal Constitution is also beyond the Commission's ken. Here, FTC's application of Section 5 to medical data security, at minimum, raises serious fair-notice due process concerns, as the ALJ correctly recognized.⁴⁸ *See* Doc. 326, 86-87. Therefore, no deference is owed. *See Edward J. DeBartolo Corp. v. FGCBCTC*, 485 U.S. 568, 573-75 (1988). *Cf. Emplr. Sols. Staffing Grp. II v.*

⁴⁸ *See* Pet'r's Br. 38-44.

OCAHO, 833 F.3d 480, 487-90 (5th Cir. 2016) (no deference “where ... agency’s interpretation of an ambiguous statute unfairly surprises ... party”).

Finally, this Court has already rebuffed the FTC’s deference demands for its January 16 Order—concocted (and used) to buttress the FTC’s litigating position in various federal courts. *See LabMD, Inc. v. FTC*, 776 F.3d 1275, 1278-79 & n.1 (11th Cir. 2015). The FTC’s power-grab must stand or fall based on the reasons given by the January 16 Order, which are without merit and thus should be rejected.⁴⁹

CONCLUSION

For these reasons, the Order should be vacated.

Respectfully submitted,

/s/ Michael Pepson

Patrick J. Massari

Michael Pepson

CAUSE OF ACTION INSTITUTE

1875 Eye Street, NW, Suite 800

Washington, D.C. 20006

Phone: 202.499.6937

Fax: 202.330.5842

Dated: January 3, 2017

Counsel for Amici Curiae

⁴⁹ FTC’s power grab can only be upheld “on the basis articulated” in *that* Order, *Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 50 (1983), and cannot stand if the FTC “misconceived the law.” *SEC v. Chenery Corp.*, 318 U.S. 80, 94 (1943).

CERTIFICATE OF COMPLIANCE

The undersigned counsel for *amici curiae* certifies that this brief:

- (i) complies with the word limit of Fed. R. App. P. 32(a)(7)(B)(i) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f) and/or 11th Cir. R. 32-4, this brief contains 6,140 words; and
- (ii) 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 it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in Times New Roman 14-point font.

/s/ Michael Pepson

Michael Pepson

CAUSE OF ACTION INSTITUTE

1875 Eye Street, NW, Suite 800

Washington, D.C. 20006

Phone: 202.499.6937

Fax: 202.330.5842

michael.pepson@causeofaction.org

Admitted only in Maryland.

Practice limited to federal matters.

Dated: January 3, 2016

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of January, 2017, a true and correct copy of the foregoing was filed with the Clerk of the United States Court of Appeals for the Eleventh Circuit via the Court's CM/ECF system, which will notify the following counsel:

Douglas H. Meal
ROPES & GRAY LLP
Douglas.Meal@ropesgray.com

Michelle L. Visser
ROPES & GRAY LLP
Michelle.Visser@ropesgray.com

David T. Cohen
ROPES & GRAY LLP
David.Cohen@ropesgray.com

Douglas Hallward-Driemeier
ROPES & GRAY LLP
Douglas.Hallward-Driemeier@ropesgray.com

Ashton R. Lattimore
ROPES & GRAY LLP
Ashton.Lattimore@ropesgray.com

Counsel for Petitioner LabMD, Inc.

Joel Marcus
jmarcuskurn@ftc.gov

Theodore Metzler
tmetzler@ftc.gov

Matthew Hoffman
mhoffman@ftc.gov

Counsel for Respondent Federal Trade Commission

Ronald L. Raider
KILPATRICK TOWNSEND & STOCKTON LLP
RRaider@kilpatricktownsend.com

Burleigh Lavisky Singleton
KILPATRICK TOWNSEND & STOCKTON LLP
BSingleton@kilpatricktownsend.com

*Counsel for Amicus Curiae National Federation of Independent Business
Small Business Legal Center*

Respectfully submitted,

/s/ Michael Pepson

Michael Pepson

CAUSE OF ACTION INSTITUTE

1875 Eye Street, NW, Suite 800

Washington, D.C. 20006

Phone: 202.499.6937

Fax: 202.330.5842

michael.pepson@causeofaction.org

Admitted only in Maryland.

Practice limited to federal matters.

Dated: January 3, 2016

Counsel for Amici Curiae