UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. 9357**
	)	
LabMD, Inc.,	)	**PUBLIC**
a corporation.	)	
	)	

RESPONDENT LabMD, INC.'S REPLY TO COMPLAINT COUNSEL'S RESPONSE IN OPPOSITION TO RESPONDENT'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Senior Vice President for Litigation and Counsel to Cause of Action.

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

INTRODUCTION

FTC's Opposition to LabMD's Motion is remarkable in only two respects. First, it demonstrates FTC has discarded rule-of-law and constitutional values for boundless bureaucratic power and discretion. Second, it shows FTC will distort the law and even re-write history to justify its power-grab.

FTC's Opposition's admissions and arguments demonstrate only that FTC lacks Section 5 authority over patient-information data-security, and that its standardless, blame-the-victim *ex post* enforcement tactics violate due process and fail to provide LabMD with constitutionally-adequate fair warning of the data-security standards FTC believes Section 5 forbids or requires.

STANDARD OF REVIEW

FTC does not respond to many arguments made in LabMD's Motion to Dismiss (Mot.). "[F]ailure to respond to an argument…acts as a concession" and thus an admission. *CREW v. Cheney*, 593 F. Supp. 2d 194, 229 (D.D.C. 2009).

FTC admits it must prove Congress intended to delegate it specific authority to regulate patient-information data-security. *La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). FTC also admits the FRCP 12(b)(6) standard controls here under *In re S.C. State. Bd. of Dentistry*, 138 F.T.C. 229, 232 (F.T.C. 2004). *See* FTC Opp. to Mot. (Opp.) 3. Yet FTC claims without citing any controlling (or on-point) authority that the *Iqbal/Twombly* standard for 12(b)(6) motions does not apply. Opp. 25. Because FRCP 12(b)(6) applies here, as FTC admits, *Iqbal*/*Twombly* apply as well. *See Jones v. Horne*, 634 F.3d 588, 595-96 & n.4 (D.C. Cir. 2011)(*Iqbal/Twombly* sets standard for 12(b)(6) motions).

ARGUMENT

I. FTC LACKS SECTION 5 "UNFAIRNESS" AUTHORITY OVER DATA-SECURITY.

A. HIPAA/HITECH Control, And FTC May Not Over-File.

Citing no controlling authority or explicit statutory command, FTC wrongly claims "concurrent" jurisdiction over HIPAA/HITECH patient-information data-security.

FTC admits LabMD is and always has been a HIPAA-covered entity regulated exclusively by HHS under HIPAA/HITECH.[1] It also admits LabMD is specifically exempted from FTC's HITECH rule. *Cf.* Mot. 12 & n.9. It offers no explanation why HITECH, Pub. L. 111-5 §13424(b)(1), directs HHS and FTC to determine *which* agency is best equipped to enforce HITECH against non-HIPAA-covered entities (FTC agrees that HHS exclusively regulates HIPAA-covered entities like LabMD). It also ignores HIPAA's directive to HHS—not FTC—to "adopt [data-]security standards" for "health information." 42 U.S.C. §1320d-2(d)(1); 42 U.S.C. §1320d(4)(defining "health information").

Even if Section 5 covered data-security, HIPAA/HITECH are "precisely drawn, detailed statute[s that] pre-empt" Section 5's "more general remedies." *EC Term of Years Trust v. U.S.*, 550 U.S. 429, 433 (2007). Through HIPAA/HITECH, Congress deliberately targeted specific data-security problems with specific solutions, and these specific statutes govern over whatever "general" Section 5 authority FTC might have. *See RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-72 (2012). Otherwise, HIPAA-covered companies like LabMD lack data-security safe-harbor and certainty, contrary to HHS's regulatory intent.

[1] FTC incorrectly claims LabMD only cites one HITECH provision to support its argument. But LabMD cites multiple HIPAA provisions. Mot. 11-13 & nn.4,9.

See 78 Fed. Reg. 5,566, 5,644 (Jan. 25, 2013)(encouraging covered entities to use encryption safe-harbor); 65 Fed. Reg. 82,462, 82,543 (Dec. 28, 2000)(discussing safe-harbor).

FTC says "Congress's intent to preempt or repeal…FTC's unfairness authority" must be clear-and-manifest. Opp. 6. This distorts the law, for implied repeal may be found even "absent 'a clearly expressed congressional intention'" where, as here, two statutes irreconcilably conflict. *Carcieri v. Salazar*, 555 U.S. 379, 395 (2009).

FTC attempts to avoid *Credit Suisse v. Billing,* 551 U.S. 264 (2007), with the specious argument that the Court explicitly limited the rule there to conflicts between antitrust and securities laws. Opp. 7. But nowhere in *Billing* does it say this.[2] Instead, *Billing* fleshes out the analysis for determining a "clear repugnancy." *Billing* confirms that HIPAA/HITECH irreconcilably conflict with Section 5, and, being more recent and more specific than Section 5, control. *See Billing*, 551 U.S. at 276, 285. Even if the canon against implied repeal is applied here, Section 5 is displaced by HIPAA/HITECH. *See EC Trust*, 550 U.S. at 434-36.

FTC claims that because HITECH was enacted "*after*…[FTC] had brought a half-dozen unfairness cases relating to data security," Congress has blessed its power-grab. Opp. 7 n.4. That, too, distorts the law. Congress's failure to express any opinion is not probative of legislative intent. *Rapanos v. U.S.*, 547 U.S. 715, 749-50 (2006).

Finally, FTC's reliance on *two recent consent orders* in cases also involving allegations of Section 5 "deception" and HIPAA violations is another irrelevant distraction.[3] Here, the question is not whether Section 5 and HIPAA/HITECH authorities might be "complementary"

---

[2] *See* Jesse Markham, *The Supreme Court's New Implied Repeal Doctrine*, 45 GONZ. L. REV. 437,475 (2009)(*Billing* "not limited to…interplay between antitrust law and economic regulation.").

[3] *In re CVS Caremark* "is the first instance in which [HHS] OCR…coordinated …with…FTC." http://www.hhs.gov/news/press/2009pres/02/20090218a.html.

under some circumstances. Instead, it is whether FTC's "unfairness" authority allows FTC to over-file HHS and punish a company FTC admits *complied* with HIPAA/HITECH in all respects. FTC's interpretation of Section 5 wrongly eviscerates Congress's HIPAA/HITECH enactments and HHS's regulatory scheme.

B. FTC Lacks "Unfairness" Authority Over Data-Security.

FTC says its position that "companies *should* engage in 'reasonable' [data-security] practices…is premised on Congress's mandate" in 15 U.S.C. §45(n). Opp. 2 (emphasis added). This claim, yet again, distorts the law. Congress's subsection (n) mandate was to rein in FTC's abuse of its "unfairness" authority by, *inter alia*, prohibiting FTC from using public-policy considerations "as a primary basis for…determin[ing]" that a practice is "unfair." 15 U.S.C. §45(n).

1. Distorted History And Law Cannot Give FTC Data-Security Authority.

FTC distorts the legislative history to serve its power-grab. *See* Opp. 9. It cites "unfair-*competition*" materials from 1914 predating by twenty-four years the 1938 Wheeler-Lea Amendments to the FTC Act, which added "unfair or deceptive acts or practices" to Section 5, and predating by eighty years the 1994 Amendments, which added 15 U.S.C. §45(n). Therefore, FTC's alleged "legislative history" is irrelevant to its Section 5 "unfairness" authority here.[4]

FTC's case authority illustrates only that FTC lacks jurisdiction here. First, none of their cases are legally controlling. FTC admits that no court has ever affirmed its Section 5 authority

[4] FTC cites dicta from *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972), interpreting legislative history from the 1914 pre-Wheeler-Lea Amendments version of Section 5. But Congress was aware of this when it limited FTC's "unfairness" authority in 1994 in 15 U.S.C. §45(n) and overruled FTC's "unfairness" authority claims. *See Miles v. Apex Marine,* 498 U.S. 19, 32 (1990)("Congress…aware of existing law when it passes legislation"). Because *Sperry* was decided over twenty years before §45(n) was enacted, it is irrelevant.

to regulate patient-information or any other data-security. *Cf.* Mot. 1. Second, none of the cases cited are even factually analogous.

Unlike this case, where LabMD's property was taken by a third party without its knowledge or permission, in *FTC v. Neovi*, the defendant affirmatively participated in fraudulent creation and delivery of unverified checks. *See* 604 F.3d 1150, 1155-57 (9th Cir. 2010). Similarly, in *FTC v. Accusearch*, Accusearch was held liable for maintaining a website selling GPS locations of individual cell phones and other confidential, personal information, where every time Accusearch ordered phone records, they caused use of false pretenses and other fraudulent means to obtain this information. *See* 2007 U.S. Dist. LEXIS 74905, at *17-18 (D.Wyo. Sept. 28, 2007).

Unlike this case, where FTC admits LabMD has always complied with all applicable data-security regulations, *cf.* Mot. at 4,8,13, *Orkin Exterminating Co. v. FTC*—decided years *before* 15 U.S.C. §45(n)'s enactment limiting FTC's "unfairness" authority—involved unilateral breaches of unambiguous contracts through which Orkin wrongfully obtained money from consumers. *See* 849 F.2d 1354, 1363-66 (11th Cir. 1988).

Unlike this case, where FTC admits LabMD has not engaged in any deception, *cf.* Mot. 6, in *FTC v. Verity Int'l, Ltd.*, the defendant not only told its customers they were liable for payments for services they did not use or agree to but "misrepresented…services provided." 335 F. Supp. 2d 479, 484 (S.D.N.Y. 2004).

In re Int'l Harvester Co., 104 F.T.C. 949, 1984 FTC LEXIS 2 (1984), is a Commission decision predating Congress's attempt to rein in FTC via 15 U.S.C. §45(n). It is also factually inapposite. The "unfair" trade practice in that case was a deceptive material omission, i.e., the

company's failure to warn its customers about serious safety risks associated with its products. *Int'l Harvester*, 1984 FTC LEXIS at *255-62.

2. Congress's Preference for Sector-Specific Data-Security Statutes Trumps the Commission's Data-Security Power-Grab.

FTC again distorts the law, arguing FCRA, GLBA, and COPPA simply provide new "tools," such as "APA rulemaking authority…." Opp. 10. But Section 5 already gives FTC authority to promulgate rules. 15 U.S.C. §57a(a)(1). It just refuses to do so.

FTC also says LabMD "does not grasp the significance of civil penalties" and that under Section 5 FTC can seek only equitable relief. Opp. 11 (citing 15 U.S.C. §45(b)). Yet Section 5 authorizes civil penalties for cease-and-desist order violations of up to $10,000-per-violation, 15 U.S.C. §45(l), *and* authorizes substantial civil penalties for violations of "rules" respecting unfair acts or practices,[5] 15 U.S.C. §45(m).

Finally, FTC says FCRA, GLBA, and COPPA "enhance" FTC's general data-security authority because it need not prove a likelihood of substantial injury thereunder. Opp. 11. But if FTC actually issued data-security rules, as it is both authorized and constitutionally-required to do if Section 5 covered data-security, *see* 15 U.S.C. §57a(a), it would not need to prove substantial injury, 15 U.S.C. §45(m), and would have the same enforcement powers as it does under FCRA, GLBA, and COPPA, thereby rendering these statutes nullities. However, Congress recognized that FTC has no general Section 5 "unfairness" data-security authority and thus enacted these sector-specific statutes. FTC's "enhancement" argument therefore fails.

[5] Civil penalties under subsections (l) and (m) are *four times* higher than those available under the FCRA, 15 U.S.C. §1681s(a)(2)(A); COPPA incorporates FTC Act penalties, 15 U.S.C. §6505(d); and GLBA is enforced under the FTC Act, 15 U.S.C. §6805(a)(7). Thus, the monetary penalty in *U.S. v. Choicepoint*, No. 06-0198 (N.D.Ga. Feb. 15, 2006), was issued "pursuant to…Section(m)(1)(A) of the FTC Act." Stip. Final Judgment 4. Likewise, the Consent Decree in *U.S. v. Path,* No. 13-0448, ¶18 (N.D.Cal. Feb. 8, 2013), expressly states that the civil penalties are imposed "pursuant to Section 5(m)(1)(A) of the FTC Act…."

C. FTC Disclaimed Authority to Regulate.

Complaint Counsel says "FTC has consistently maintained its ["unfairness" data-security] authority" and that "[a] contrary conclusion requires…tortured application" of a Supreme Court case involving a different agency. Opp. 12. As a matter of fact, this claim straddles the line between distortion and outright deception. As a matter of law, this is breathtakingly wrong.

1. Against the Backdrop of FTC's Admitted Lack of Authority, Congress Enacted Numerous Targeted Data-Security Statutes.

FTC claims that "[s]ince 2000, the FTC has brought nearly fifty data-security cases, more than eighteen of which alleged…unreasonable security is an unfair…practice," citing a string of consent orders. Opp. 12 & n.9. But the *earliest* consent order they cite is dated "Sept. 20, 2005." Opp. 12 n.9. The earliest Commission statements they cite are dated "Mar. 21, 2007" and "Sept. 22, 2004," respectively. Opp. 13 & n.10. Even taking FTC's citations at face value, their world seemingly was created in late 2004.

Furthermore, FTC's out-of-context cherry-picked statement from a footnote in Orson Swindle's testimony must be addressed. *See* Opp. 13 n.10. He never suggested that the Commission has general substantive data-security authority under Section 5, for the very next sentence in footnote 24 states: "[FTC] has used this ["unfairness"] authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing'" and cites two "phishing" cases.

Complaint Counsel does not mention FTC's statement in *Privacy Online: A Report to Congress*, 41 (1998), that FTC generally "lacks authority to require firms to adopt information practice policies," or its statement in *Privacy Online: Fair Information Practices in the Electronic Marketplace,* 34 (2000), that FTC "lacks authority to require firms to adopt

information practice policies or…abide by…fair information practice principles on their Websites" not directed to children. *Cf.* Mot. 16 n.12. They do not deny that Chairman Pitofsky told Congress the FTC's data-security authority is "limited…to ensuring…Websites follow their stated information practices." Mot. 16 n.12. They offer no response to a FTC official's 2001 statement that "'[t]he agency's jurisdiction is (over) deception….If a practice isn't deceptive,…[FTC] can't prohibit…collecting information." Mot. 16 n.12. They also concede that even FTC's 2008 Resolution did not claim authority to regulate data-security under a pure "unfairness" theory. *Cf.* Mot. 17 n.14.

FTC admits it pestered Congress to confer data-security authority, Opp. 14; *cf.* Mot. 15-16 nn.12-15, but argues that "FTC's requests for additional [data-security] authority showcase…FTC's unfairness authority," Opp. 13. This non-sequitur fails. Asking Congress for the authority to regulate data-security "showcases" only that FTC lacked this authority, for there would be no need to ask for power FTC already had.

FTC's recent statements claiming general Section 5 "unfairness" data-security authority cannot erase FTC's many prior statements disavowing Section 5 data-security jurisdiction or cloud the fact that Congress enacted many targeted data-security statutes against that backdrop.

FTC's reliance on *Smiley v. Citibank*, 517 U.S. 735 (1996), fails. First, here FTC's newfound Section 5 authority is a "[s]udden and unexplained change…." *Id.* at 742. Second, *Smiley* involved an agency regulation entitled to *Chevron* deference. *See id.* at 740-41. No deference is owed to FTC here, because it has not engaged in formal adjudication or rulemaking. *U.S. v. Mead Corp.*, 533 U.S. 218, 227 (2001).

2. Rejected Legislation Confirms FTC Lacks Authority.

FTC says "savings clauses" in four of *ten* or more bills Congress has rejected that would have given FTC general data-security authority supports its claimed authority. Opp. 14. This is bizarre.

First, all four cited bills were proposed in 2011, Opp. 14, *after* Congress had given FTC sector-specific data-security authority through GLBA, FRCA, and COPPA, Mot. 14 & n.10. Of course, these "[p]reservation clauses would be unnecessary if…FTC lacked existing authority," Opp. 14, under GLBA, FCRA, COPPA, and other targeted statutes. But the "savings clauses" are general, do not refer to Section 5, and protect FTC's data-security authority under these other statutes. *See* S. 1207, §6(d)(protecting "Commission's authority under any other provision of law"); H.R. 2577, §6(d)(same); H.R. 1841, §6(d)(same); H.R. 1707, §6(d)(same). None of these bills address, much less endorse, FTC's claimed Section 5 authority.[6] Indeed, H.R. 2577, §4(d)(1), would have *exempted* HIPAA-covered entities like LabMD from compliance.

Second, FTC ignores *six other* 2011 cybersecurity bills that included no language "preserving" FTC data-security authority. *See* S. 1151, S. 1408, S. 1434, S. 1535, S. 2105, H.R. 624.

D. *Massachusetts v. EPA* Supports LabMD's Arguments.

FTC's reliance on *Massachusetts v. EPA*, 549 U.S. 497 (2007), is misplaced. Unlike Section 5, the Clean Air Act unambiguously defined "air pollutant" to embrace "all airborne compounds of whatever stripe…." *Id.* at 528-29. Moreover, the Court noted two "critical" considerations absent from that case but present in *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), and present here. *See Massachusetts*, 549 U.S. at 530-31. First, Section 5

[6] A single Senator's remark during a hearing has no weight, even if it did support FTC.

data-security jurisdiction for the *entire private economy* is not only "counterintuitive" but leads to "extreme measures," because it would require *substantive* data-security standards for the entire economy to be classified as "unfair" practices and eviscerate Congress's longstanding, deliberate policy of regulating data-security through narrow, targeted statutes. *Cf. id.*

Second, like *Brown & Williamson*, there is "an unbroken series of congressional enactments that ma[k]e sense only if adopted 'against the backdrop of…[FTC's] consistent and repeated statements that it lacked authority'" to regulate data-security. *Cf. id.* For FTC to prevail, Congress's many specific, narrow delegations of data-security regulatory authority enacted against the backdrop of FTC's repeated disavowal of general regulatory authority must be deemed superfluous nullities.[7] Furthermore, unlike *Massachusetts*, many of these statutes, including HIPAA/HITECH, directly conflict with FTC's claimed authority.

E. *ABA v. FTC* Illustrates Why Dismissal Is Required.

FTC dismisses *ABA v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), claiming "there is no debate about the meaning of the term 'unfairness.'" Opp. 16 (citing 15 U.S.C. §45(n)). Given that the one court that actually considered FTC's claimed Section 5 authority to regulate patient-information data-security said "there is significant merit" to LabMD's argument against FTC's power-grab, *see* Mot. 1, and 15 U.S.C. §45(n) does not define "unfairness" but rather cabins FTC's authority,[8] that argument fails.

In truth, FTC concedes that nothing in Section 5 explicitly authorizes it to regulate patient-information data-security practices. Instead, as in *ABA*, FTC is simply grabbing power to "fill in" what it perceives as a regulatory gap. But Congress has already filled that "gap" through

[7] *See* Mot. 11-16 & nn.10-11 (listing and discussing specific statutes).

[8] Statutory language always trumps section titles. *R.R. Trainmen v. Balt.&Ohio R.R.*, 331 U.S. 519, 529 (1947).

HIPAA/HITECH, and FTC cannot second-guess Congress. FTC's assault on LabMD is contrary to the administrative structure Congress has constructed for patient-information data-security and entirely illegitimate. *See ABA*, 430 F.3d at 469-71.

Furthermore, FTC concedes Congress has generally left patient-information data-security to the states, and where Congress has found federal regulation of patient-information data-security practices appropriate, it has explicitly said so. *Cf.* Mot. 21; 42 U.S.C. §1320d-2(d)(1). Because Section 5 does not clearly authorize FTC's conduct here, its brazen power-grab must be denied. *See ABA*, 430 F.3d at 472.

II. FTC'S LACK OF STANDARDS VIOLATES DUE PROCESS.

A. FTC's Admitted Lack of Standards.

FTC admits LabMD has not violated any data-security statutes, rules, or regulations and concedes LabMD has not engaged in a "deceptive" trade practice. *Cf.* Mot. 6,8. It admits LabMD's data-security practices are regulated under HIPAA/HITECH and that HHS exclusively implements and enforces these statutes as applied to LabMD. *Cf.* Mot. 4,13. FTC's sole claim against LabMD is unspecified "unfair" acts or practices. *Cf.* Mot. 7-8.

FTC also admits that Section 5 statutorily bars FTC from enforcing consent orders against non-parties and that its consent orders do not establish illegal conduct and only bind the parties thereto. *Cf.* Mot. 23,26. It has not alleged LabMD had actual notice of the business guides, consumer alerts, links to Sans Institute/NIST publications, and other Internet postings. *Cf.* Mot. 24-28 & nn.19-21. It admits that none of these materials were published in the Federal Register and that *none* of their alleged sources of data-security standards create *any* legally binding duties and obligations. *Cf.* Mot. 7-8. Instead, FTC says Section 5 alone provides

constitutionally and statutorily adequate *ex ante* notice of what data-security practices are forbidden or required. Opp. 16-17.

B. Section 5 Does Not Establish Proper Standards.

FTC does not acknowledge, much less address, the authorities cited by LabMD holding that FTC was required to provide fair notice of prohibited or required conduct. FTC has never alleged that LabMD's patient-information data-security practices did not meet objective medical-industry standards in effect and applicable to businesses of its size and nature at the time of the alleged violation. *Cf. S&H Riggers & Erectors v. OSHRC*, 659 F.2d 1273, 1280-83 (5th Cir. 1981)(reasonable-person standard divorced from industry standards or regulations violates due process). Instead, FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations. *Cf.* Mot. 4,8,13.

No case has ever held, and no plausible argument can be made, that Section 5 provides constitutionally-adequate data-security fair notice. *See* Stegmaier & Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 706 (2013)("[S]tatutory language does not provide notice of required data-security safeguards."). Section 5's broad "unfairness" prohibition, which does not even refer to "data security," let alone prescribe or proscribe data-security practices, is far more offensive than the statutes at issue in cases like *Connally v. General Constr. Co.*, 269 U.S. 385 (1926)(cited by LabMD but ignored by FTC) finding fair-notice due-process violations. And even if data-security "reasonableness" standards could provide regulated entities with constitutionally-adequate notice if codified in a regulation or statute, FTC says it has not done so and will not do so.

To claim fair notice, FTC again distorts the law. It cites *U.S. v. Merrill*, 513 F.3d 1293, 1306 (11th Cir. 2008), but this is not a fair-notice case. The cherry-picked portion of *Merrill* it cites discusses *a jury instruction*, not statutory fair notice. Opp. 18. Unlike Section 5, the *Merrill* statute (Controlled Substance Act, 21 U.S.C. §841) is quite detailed and hence provides fair notice.

FTC claims OSHA's General Duty Clause is the best analogy to their standardless *ex post* data-security regime. Opp. 19 n.12. It is a poor fit. Cases interpreting OSHA's General Duty Clause prove LabMD's point and confirm why FTC's actions violate due process, particularly because FTC admits LabMD has always complied with HIPAA/HITECH's specific data-security requirements.

The General Duty Clause is a regulatory tool of last resort—a stop-gap—which "was not meant…[as] 'a general substitute for reliance on standards'" and only applies to "'special circumstances for which no standard has yet been adopted.'" *Ramsey Winch v. Henry*, 555 F.3d 1199, 1205 (10th Cir. 2009). It only controls where there are no other standards, because "standards preempt the [G]eneral [D]uty [C]lause…." *In re Samsonite Corp.*, 756 F. Supp. 498, 500 (D.Colo. 1991). FTC claims that even though LabMD has always complied with HIPAA/HITECH *data-security standards*, it remains liable under Section 5 for compliance with FTC's unstated data-security standards. This is the antithesis of how the General Duty Clause works.[9] *See Teal v. E. I. du Pont*, 728 F.2d 799, 804 (6th Cir. 1984)(Congress "enacted…general duty clause to cover serious hazards…not otherwise covered by specific regulations.").

[9] *See* OSHA's Field Operations Manual, CPL02-00-148, pp.4-14-4-30 (2009)(detailed elements of General-Duty-Clause violation and strict limits). Unlike Section 5, there are 30-plus years of concrete agency guidelines specifying General-Duty-Clause-imposed obligations. *E.g., ConAgra, Inc.*, 1983-84 O.S.H. Dec. (CCH) ¶26,420, 33,523 (1983)(formal agency interpretation).

The "objective" industry-specific reasonableness standard at issue in *Voegle v. OSHA*, 625 F.2d 1075 (3d Cir. 1980), is fundamentally different from what FTC is doing here. *Voegle* involved a fair-notice challenge to a construction-industry-specific *regulation* (not the General Duty Clause), *see id.* at 1077, far more specific than Section 5's text. Furthermore, *numerous* agency enforcement actions applying occupational-safety regulations far more specific than Section 5 have been dismissed on fair-notice grounds. *E.g., Fabi Const. Co. v. SOL*, 508 F.3d 1077, 1088 (D.C. Cir. 2007); *Gates & Fox v. OSHRC*, 790 F.2d 154,156-57 (D.C. Cir. 1986).

FTC enforcement actions are fundamentally different from garden-variety tort suits, and common-law negligence cases do not displace the APA's and Fifth Amendment's due-process fair-notice requirements. *See Satellite Broadcasting v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987). Also, given FTC admits LabMD has not engaged in "deception," *cf.* Mot. 4, their reliance on dicta from *In re Zappos.com*, No. 12-00325, 2013 U.S. Dist. LEXIS 128155 (D.Nev. 2013), is badly misplaced, for they omit mention of the court's decision to treat the data-security claims as "negligent misrepresentation claims" based on false website statements,[10] *id.* at *15-16.

FTC v. National Urological Group (NUG), 645 F. Supp. 2d 1167 (N.D.Ga. 2008), also deals with "deceptive" advertising allegations not at issue here. FTC itself has explained why "deception" actions do not raise the same fair-notice concerns as "unfairness" actions: "[U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset." *Int'l Harvester*, 1984 FTC LEXIS at *246. Further, the *NUG* court found it critical that, unlike here, FTC had at least expressly defined "competent and reliable scientific evidence" (this definition is omitted from FTC's block-quote) and articulated a definite

[10] *Loschiavo v. City of Dearborn* (overruled) is also not a fair-notice case; inapposite dicta FTC cites refers to the test for whether a private-right-of-action-against-the-government exists under Section 1983. *See* 33 F.3d 548, 551 (6th Cir. 1994).

standard. *See* 645 F.Supp.2d at 1186. That standard is exponentially more detailed than FTC's proposed "reasonableness" standard here.

Unlike FTC's nebulous, standardless concept of data-security "unfairness," "deception" has a well-established, clear meaning in Section 5 and elsewhere in the law and does not raise the same fair-notice concerns. *E.g.,* FTC Policy Statement on Deception, appended to *Cliffdale Assoc., Inc.*, 103 F.T.C. 110, 174 (1984)(*detailed* explication of deception elements). Thus, "deception" cases cited by FTC do not support its fair-notice argument.

Tellingly, FTC's discussion of the "reasonableness" analysis they believe Section 5 requires contains no citations whatsoever and appears to be cut from whole cloth—the only citation on the page is *In re Zappos.com*, addressed above. Opp. 21.

FTC dismissively argues that "ascertainable certainty does not require agencies to provide…guidance at the level of detail…[LabMD] seems to think appropriate." Opp. 20. They brazenly admit that neither the Complaint nor the notice order prescribe *any* specific data-security practices LabMD *should* (let alone must) implement going forward. *Cf.* Mot. 8. Elsewhere, FTC has boldly stated that the argument that a regulated entity "did not know which standard it was supposed to follow…misses the point." Mot. 27 n.21. They blithely explain that they "do[] not endorse any [industry] standards"—"[they] don't say…how you should set up your router…[they] don't say you should have…white…and black lists for IP addresses"—because "[they] are not tech support." Hearing Transcript, *FTC v. Wyndham*, 53:2-10 (Nov. 7, 2012).

The cases they cite—like the cases LabMD cites to which they do not bother to respond, *see* Mot. 22-28 & nn.19-21—make clear that this violates due process. For example, *U.S. v. Lachman*, 387 F.3d 42 (1st Cir. 2004), which, unlike here, involved a detailed technical

regulation and interpreted the phrase "specially designed," *id.* at 50-53, notes that the line of D.C. Circuit cases LabMD cites (and FTC ignores) invalidate agency *ex post* enforcement actions where, as here, the statute "is so ambiguous that a regulated party cannot be expected to arrive at the correct interpretation using standard [interpretive] tools…, must therefore look to the agency for guidance, and the agency failed to articulate its interpretation before imposing a penalty," *id.* at 57. Indeed, even FTC's patchwork-quilt of consent orders is inconsistent. *See* Stegmaier & Bartnick, *supra*, at 700 ("FTC has not explained why data-security practices in one [fact-specific consent-order] case may violate Section 5 while those same practices may not violate Section 5 in another case…apparently expect[ing] entities to piece together…complaints and consent orders in thirty-six cases, without any authoritative commentary, to arrive at…[FTC's] interpretation of adequate data-security practices….").

Finally, again without responding to LabMD's arguments and thereby conceding the points, *cf.* Mot. 25-26 & n.19, FTC—incredibly—suggests that NIST and HIPAA publications supply standards LabMD should have followed. Opp. 22 n.15. The NIST Handbook they cite is from 1995, does "not…specify requirements," and only "provides a broad overview of computer security." NIST, Special Publication, 800-12, §1.1 (1995). Section 1.1 of NIST Special Publication 800-30 states: "The guidelines herein are not mandatory and binding standards." With respect to HIPAA Guidance they cite, even if LabMD was required to follow it, FTC has admitted that LabMD *has always complied with all data-security obligations under HIPAA/HITECH.*

C. FTC Cannot Announce New Rules Through Adjudication Punishing Past Conduct.

The fact that, subject to fair notice, FTC may fill in Section 5's interstices through adjudication does not allow FTC to deliberately evade its constitutional and statutory fair-notice

obligations. FTC cannot regulate through intimidation by bullying companies into signing consent decrees. Yet FTC brags about the myriad consent decrees secured from 2005 to present, Opp. 12-13 n.9, and says they are "not obligated to engage in a rulemaking…," Opp. 23. *SEC v. Chenery*, 332 U.S. 194 (1947), where, unlike here, the agency "had not previously been confronted with the problem," *id.* at 203, explains that "[t]he function of filling in…[statutory] interstices…should be performed, as much as possible, through…quasi-legislative promulgation of rules to be applied in the future," *id.* at 202. *Chenery* is not a fair-notice case; unlike here, SEC did not seek liability for past conduct, *see id.* at 203-04. *PBW Stock Exch. v. SEC*, 485 F.2d 718 (3d Cir. 1973), also not a fair-notice case, involved *a challenged regulation,* not adjudication, *id.* at 721; dicta FTC cites is inapposite.

In *Beazer v. EPA*, 963 F.2d 603 (3d Cir. 1992), EPA had actually promulgated regulations through normal notice-and-comment rulemaking and the statute and regulations prescribed detailed requirements, *see id.* at 604-05. In that context, the court found adjudication permissible. *Cf. id.* at 609 (APA "expressly prohibit[s]…agency from retroactively imposing…interpretive rule upon…regulated party."). Unlike *Beazer*, here FTC brazenly admits that they do not have legislative or even interpretive rules explaining what data-security practices they believe Section 5 forbids or requires. *Cf. id.* at 606.

NLRB v. Bell Aerospace, 416 U.S. 267 (1974), is not a fair-notice due-process case and thus inapposite. Rather, the issue was Bell Aerospace's *future* collective-bargaining obligations. *See id.* at 269. Even in that very different context, the Court recognized situations where NLRB reliance on adjudication would be unlawful, noting that "this is not a case in which some new liability is sought to be imposed…for past actions" and that "fines or damages" were not involved. *Id.* at 294-95. Due-process-based fair-notice requirements are heightened where, as

here, the agency alleges violation of law based on *past* conduct. *See PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51-52 (D.C. Cir. 2000).

III. FTC'S FAILURE TO STATE PLAUSIBLE SECTION 5 VIOLATION.

FTC concedes it lacks even *one* complaining witness who has suffered *any* injuries because of LabMD's alleged patient-information data-security failures. FTC admits LabMD complied with HIPAA/HITECH—the only applicable patient-information data-security requirements. FTC does not allege what the objective medical-industry-standard data-security practices are or were or that LabMD's data-security practices fell short of meeting them. As explained above, the *Iqbal/Twombly* standard applies here. The Complaint fails to meet that standard and must be dismissed.

IV. STAY NECESSARY TO STOP DISCOVERY ABUSE.

FTC does not deny that its discovery tactics are barred in federal courts and does not substantively respond to LabMD's arguments or deny LabMD's assertions. At minimum, the Commission should stay the proceedings.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion in full.

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Senior Vice President for Litigation and
Counsel to Cause of Action

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and
administrative proceedings before federal agencies.

Dated: December 2, 2013

CERTIFICATE OF SERVICE

I hereby certify that on December 2, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

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

I certify that I delivered via first-class mail twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

I also certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: December 2, 2013 By: /s/ Michael D. Pepson