GIBBONS

JENNIFER A. HRADIL
Director

Gibbons P.C.
One Gateway Center
Newark, New Jersey 07102-5310
Direct: (973) 596-4495 Fax: (973) 639-6487
jhradil@gibbonslaw.com

January 21, 2014

***VIA* ECF**

Honorable Esther Salas, U.S.D.J.
United States District Court
District of New Jersey
50 Walnut Street
Newark, New Jersey 07102

**Re: *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.***
**Civil Action No.: 13-cv-1887 (ES) (JAD)**

Dear Judge Salas:

Pursuant to the Court's Order of December 27, 2013, the parties in the above-captioned matter respectfully submit the attached supplemental letter brief.

Respectfully,

s/ Jennifer A. Hradil
Jennifer A. Hradil

cc: All counsel of record (*via* ECF)

January 21, 2014

**Via CM/ECF**

The Honorable Esther Salas
United States District Court
District of New Jersey
50 Walnut Street
Newark, NJ 07101

Re: *FTC v. Wyndham Worldwide Corp., et al.*, No. 2:13-cv-01887-ES-JAD

Dear Judge Salas:

Pursuant to the Court's order of December 27, 2013, the parties in the above-captioned matter respectfully submit the following supplemental letter brief.

## I. Defendants' Position

### A. The FTC Lacks Statutory Authority

The FTC, like any other federal agency, must show that Congress intended to delegate to it the specific authority it claims. *See La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374-75 (1986). The FTC has not done that. Nothing in Section 5 of the FTC Act gives the Commission all-encompassing authority to regulate the data-security practices of every company in America. And, by its own admission, the FTC cannot claim that authority by virtue of Congress's supposed acquiescence in the Commission's actions to date. *See* Mot. to Dismiss Oral Arg. Tr. ("Tr.") at 48:20-22 ("As [Defendants] pointed out in the reply brief, there is little point [in] trying to read tea leaves of Congressional inaction.").

Indeed, far from giving the FTC unfettered authority to regulate data-security in ***every*** sector of the economy, Congress has carefully circumscribed the FTC's data-security powers to certain narrow, well-defined subject matters. *See* Fair Credit Reporting Act ("FCRA"), Pub. L. 91-508, codified as amended at 15 U.S.C. § 1681 *et seq.* (consumer reporting agencies); Gramm-Leach-Bliley Act ("GLBA"), Pub. L. 106-102 (financial institutions); Children's Online Privacy Protection Act ("COPPA"), Pub. L. 105-277 (websites collecting information from children). Those targeted grants of authority would make no sense if Section 5 already gave the FTC authority to regulate data security in ***all*** circumstances. *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (explaining that statutes must be interpreted to avoid surplusage and "to give effect, if possible, to every clause and word"). Instead, the much more natural interpretation of Congressional intent is that Congress understood the FTC to possess no data-security powers at all, unless and until Congress enacted the FCRA, GLBA, and COPPA.

Faced with the plain conflict between its broad interpretation of Section 5 and the narrow grants of data-security authority that Congress has actually given the Commission, the FTC argues that Congress enacted the FCRA, GLBA, and COPPA merely to supplement the FTC's

existing general police power over data-security matters. That is revisionist history. Nothing in the text or legislative history of the FCRA, GLBA, or COPPA suggests that Congress has ever understood Section 5 of the FTC Act to give the FTC general police power to regulate data-security practices, and the FTC's attempts to argue otherwise are *post hoc* rationalizations intended to create out of whole cloth a statutory basis for the FTC's actions.

The FTC initially tried to square the FCRA, GLBA, and COPPA with the Commission's broad interpretation of Section 5 on the grounds that Congress enacted those statutes merely to grant the FTC "rulemaking and/or civil penalty authority" in certain specific contexts. *See* FTC Opp'n to WHR Mot. to Dismiss ("FTC Opp'n"), ECF No. 110, at 12. But far from being limited statutes that merely add civil-penalty and rulemaking authority to Section 5, the FCRA, GLBA, and COPPA each contain detailed provisions granting the FTC ***substantive*** authority over data-security practices, *see* 15 U.S.C. §§ 1681m(e)(1), 6804(a)(1)(C), 6502(b), and explicit authority to ***enforce*** those standards in limited contexts, *see id.* §§ 1681s(a), 6805(a)(7), 6505(d). The FCRA, for instance, directs the FTC to "prescribe regulations requiring [financial institutions] to establish reasonable policies and procedures . . . to identify possible risks to account holders." *Id.* § 1681m(e)(1)(B). And the GLBA instructs the FTC to "establish appropriate standards for the financial institutions subject to [its] jurisdiction relating to administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information." *Id.* § 6801(b). Those substantive grants of authority would have been entirely unnecessary if, as the FTC claims, the FCRA, GLBA, and COPPA did no more than merely add "rulemaking and/or civil penalty" powers to the FTC's existing Section 5 authority. FTC Opp'n at 12. The far more plausible interpretation is that Congress saw those substantive-authority provisions as necessary to give the FTC any authority at all over data-security matters, fundamentally undermining the FTC's belief that Section 5 already provided it that authority. *See, e.g.*, *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) ("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there."); *United States v. Ryan*, 350 U.S. 299, 305 (1956) ("If Congress intended to deal with that problem alone, it could have done so directly.").

For the first time at oral argument, the FTC advanced a second theory of how to reconcile the FCRA, GLBA, and COPPA with the Commission's novel interpretation of Section 5. According to the FTC, Congress always understood Section 5 to provide the FTC with general police power over data-security matters, but it enacted the FCRA, GLBA, and COPPA for the limited purpose of freeing the Commission from the need to prove substantial consumer injury in specific contexts. *See* Tr. at 45:8-12 ("[T]here is no injury requirement in those cases [under the FCRA, GLBA, and COPPA], so they are dramatically different than the FTC's authority under the FTC Act. Under the FTC Act we are limited to cases where we can prove substantial [in]jury.").

That is a far-fetched reconstruction of what Congress intended to accomplish in the FCRA, GLBA, and COPPA. The text of those statutes, to begin, does not support the FTC's understanding. If Congress really had intended to do no more than simply eliminate the substantial-consumer-injury requirement of Section 5, the data-security provisions of the FCRA, GLBA, and COPPA would have said little more than: "In enforcing Section 5 of the FTC Act in these circumstances, the FTC need not prove substantial injury to consumers." Needless to say, such language cannot be found in the text of these sector-specific statutes. To the contrary, the

FCRA, GLBA, and COPPA all contain detailed provisions granting the FTC ***substantive*** authority over data-security practices, something that would have been entirely unnecessary for Congress to do under the FTC's reconstruction of Congressional intent.

The context and legislative history of the FCRA, GLBA, and COPPA further undermine the FTC's argument that those sector-specific statutes were enacted merely to free the Commission from Section 5's consumer-injury requirement and not to provide the FTC with substantive authority it otherwise lacked. The legislative record shows that each statute was enacted in response to Congressional concerns over the collection and misuse of sensitive consumer data. *See, e.g.*, 149 Cong. Rec. H12198, H12214-15 (daily ed. Nov. 21, 2003) (conference report on the 2003 amendments to the FCRA, which granted the FTC data-security authority over the disposal of consumer credit information); H.R. Rep. 106-74(III) at 117-19 (1999) (committee report on the GLBA); 144 Cong. Rec. S8482, S8482-83 (daily ed. July 17, 1998) (statement of Sen. Bryan, drafter and co-sponsor of COPPA). Congress therefore enacted the FCRA, GLBA, and COPPA precisely because it believed that data security ***was not covered by existing statutory provisions***, including Section 5 of the FTC Act. Nothing in the legislative history supports the FTC's alternative theory that Congress already understood the FTC to have universal data-security authority under Section 5, but felt it necessary to enact three statutes to eliminate the consumer-injury requirement in certain circumstances.

Indeed, it is far from clear whether the FCRA, GLBA, and COPPA actually ***do*** eliminate the substantial-injury requirement in the first place. The FCRA and COPPA direct the FTC to enforce those statutes as though they included "***all applicable terms and provisions*** of the [FTC] Act." 15 U.S.C. § 6505(d) (emphasis added); *accord id.* § 1681s(a)(1) (directing the FTC to pursue violations of the FCRA and its underlying regulations "as though the applicable terms and conditions of the [FTC] Act were part of [the FCRA]"). That necessarily means the FTC must prove substantial, unavoidable consumer injury as a part of enforcing those statutes.* And although the statutes do alter ***some*** of the background requirements of the FTC Act, *see, e.g.*, § 1681s(a)(1), no provision of the FCRA, GLBA, or COPPA purports to relieve the FTC of its duty to prove substantial consumer injury. As a result, the FTC's asserted distinction between its sweeping understanding of Section 5 and the narrow delegations of the FCRA, GLBA, and COPPA is really not distinction at all—because both sets of statutes require substantial consumer injury, the FTC's understanding of Section 5 cannot be sustained without rendering the terms of the FCRA, GLBA, and COPPA entirely superfluous.

Finally, legislation recently proposed in Congress by Senator Patrick Leahy further confirms that the FTC lacks generalized data-security authority under Section 5. *See* Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. §§ 201-04. That legislation would require businesses with access to data on 10,000 or more individuals to establish "administrative, technical, or physical safeguards identified by the Federal Trade Commission." *Id.* § 202. The bill would also grant the FTC explicit enforcement authority over the data-security requirements

* The provisions in the FCRA, COPPA and GLBA providing that a violation of a regulation thereunder constitutes a violation of the FTC Act do nothing to alter this conclusion. See 15 U.S.C. § 1681s(a) (FCRA); *id.* §§ 6801(b), 6805(a)(7) (GLBA); *id.* § 6505(d) (COPPA). Rather than eliminating the substantial consumer injury requirement, those provisions implicitly acknowledge that these sector-specific statutes (and regulations validly enacted thereunder) already incorporate that requirement.

established thereunder. *See id.* § 203(b) ("Any business entity shall have the provisions of this subtitle enforced against it by the Federal Trade Commission."). Again, if the Commission already possessed plenary data security authority under Section 5, such comprehensive legislation would be unnecessary.

### B. The FTC Has Not Provided Fair Notice

In any event, even if the FTC were correct in its understanding of the relevant statutes, its amended complaint should still be dismissed because the FTC has not provided regulated entities with the fair notice that the Due Process Clause requires. The FTC has not published any rules, regulations, or guidelines explaining to businesses what data-security protections they must employ to comply with the FTC's interpretation of Section 5 of the FTC Act. Such a failure to publish any interpretive guidance whatsoever violates the "fundamental principle in our legal system" that "laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012). It also violates bedrock principles of administrative law, which make clear that when a statute such as Section 5 is "so vague that [its] ambiguity can only be resolved by deferring to the agency's own interpretation," the agency must at the very least state with "ascertainable certainty" what conduct is prohibited. Sec. of Labor v. Beverly Healthcare-Hillview, 541 F.3d 193, 202 (3d Cir. 2008).

The FTC's lack of guidance has not gone unnoticed. Congress has expressed concern over "the regulatory uncertainty many businesses feel already" because the FTC has failed to provide "a coherent statement of policy on how the Commission plans to enforce Section 5." See Hearing on FTC Review and Outlook before the Subcomm. on Commerce, Manuf. and Trade of the House Comm. on Energy and Commerce, 113th Cong., 2013 WL 6237638 at 3 (Dec. 3, 2013). Without such a "coherent statement," one member noted, "many businesses, large and small, are left to examining past decisions to see how they may fit into a certain set of facts." Id. Similarly, leading business organizations participating in this case have explained that current FTC enforcement practices give "no advance notice to businesses on what they are required to do to comply with the law in a rapidly changing technological environment." Br. of Amici Curiae Chamber of Commerce of the United States, et al. at 11.

Nor would it be particularly difficult for the FTC to promulgate the rules and regulations that due process requires. Although the FTC has previously claimed that it would be "impossible" to craft generalized data-security rules, at least two other federal agencies have managed to do just that—and both of those agencies did so for computer networks much more sophisticated than those involved in this litigation. See Department of Homeland Security ("DHS") Office of Inspector General, Evaluation of DHS' Information Security Program for Fiscal Year 2013 (Nov. 21, 2013), available at http://goo.gl/OC4CNx [hereinafter, "DHS Evaluation"]; National Institute of Standards and Technology ("NIST") Preliminary Cybersecurity Framework: Improving Critical Infrastructure Cybersecurity (Oct. 22, 2013), available at http://goo.gl/ivPLnq [hereinafter, "NIST Framework"]. NIST recently released for public comment a 44-page document explaining precisely what data-security protocols should be employed to protect computer networks at "critical infrastructure" locations, including facilities such as nuclear power plants. See NIST Framework at 13-27. And DHS has, since at least 2008,

assessed the state of its own internal data security using an "Information Security Scorecard" with a 0-100 rating on various, specific data-security metrics. See, e.g., DHS Evaluation at 42.

If NIST and DHS are readily able to compile a set of objective data-security standards for critical infrastructure and homeland security applications, the FTC can certainly do the same for consumer payment applications in order to satisfy constitutional fair notice requirements. Although the FTC claims it has not engaged in rulemaking because of the difficulty in crafting standards that would apply to businesses of all types and sizes, see Tr. at 77:6-9, 18-23, that variation among regulated entities is precisely why Congress and the courts require rulemaking in these types of situations — to ensure that the agency considers the views of all stakeholders and then fashions a policy or rule that remedies the problem at issue in a sensible manner, see, e.g., Hall v. EPA, 273 F.3d 1146, 1163 (9th Cir. 2001) ("[T]he point of notice-and-comment rulemaking is that public comment will be considered by an agency and the agency may alter its action in light of those comments."). The FTC's concession that different standards should apply to different businesses confirms the arbitrary nature of its current approach, which leaves businesses guessing as to what they must do to avoid running afoul of the Commission's ad hoc data security policy.

Although it concedes that it has published no rules or regulations on data-security requirements, Tr. at 69:24-70:2, the FTC argues that its prior consent decrees and an informal brochure provide all the notice that due process mandates. FTC Opp'n at 18-20. But it is well-established that third-party agency consent decrees do not constrain FTC discretion and thus cannot provide any meaningful notice to third parties. See, e.g., United States v. E.I. du Pont de Nemours & Co., 366 U.S. 316, 330 n.12 (1961); Integraph Corp. v. Intel Corp., 253 F.3d 695, 698 (Fed. Cir. 2001) ("[A] consent order does not establish illegal conduct."). And the informal brochure on which the FTC so heavily relies, see FTC Opp'n at 18-19 (citing Protecting Personal Information: A Guide for Business (2007)), is far too vague to provide meaningful guidance, particularly in the complex world of data security. For proof of that, one need look no further than the 44 pages of guidance that NIST has propounded on the same subject, much of which contains references to other, even more detailed protocols. See NIST Framework at 13-27.

For these reasons, Defendants' motions to dismiss should granted. Defendants also request leave from this Court to file a two-page reply letter after the FTC has set out its arguments below. Because the FTC raised its substantial-injury argument for the first time at oral argument, the response below is the first time Defendants will have been provided with a written articulation of the FTC's position on these issues. Defendants therefore request that the Court grant Defendants leave to file a short reply brief, so that Defendants can respond properly to the FTC's arguments.

## II. Plaintiff's Position

Section 5 of the FTC Act applies by its terms to *all* unfair commercial practices that violate the three-part statutory test of 15 U.S.C. § 45(n). The plain language of Section 5 is not susceptible to a "data security" exception. Wyndham thus resorts to an argument that Section 5 must not mean what it says because, if that plain-language interpretation were correct, Congress would not have needed to enact various subsequent statutes. *See supra* p. 2. That argument is wrong because, in at least three different respects, these statutes supplement the Commission's preexisting Section 5 authority. First, as discussed below, these statutes dispense with the "consumer injury" requirement that the FTC would otherwise face in any case it brings under Section 5. Second, these newer statutes grant the FTC additional powers, such as streamlined Administrative Procedure Act rulemaking authority and civil-penalty authority, each of which the FTC would otherwise lack. *See* Pl.'s Resp. in Opp'n to Mot. to Dismiss 12, ECF No. 110 ("Pl.'s Opp'n). Third, unlike the FTC Act itself, these newer statutes affirmatively compel (rather than merely authorize) the FTC to use its consumer-protection authority in specified ways. Those many differences alone undermine Wyndham's argument that, by enacting these statutes, Congress meant to carve out an atextual "data security" exception to the Commission's Section 5 authority.

We discuss the merits of these issues below, but we first note that any doubt about the FTC's statutory authority would be dispelled by two recent developments: (1) the FTC's recent decision in *LabMD*, which is entitled to full *Chevron* deference under *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863, 1871 (2013); and (2) the D.C. Circuit's decision in *Verizon v. FCC*, No. 11-1355, 2014 WL 113946, at *11-12 (D.C. Cir. Jan. 14, 2014), which rejects a very similar argument based on *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000).

**The FTC's *LabMD* order.** On January 16, 2014, the Federal Trade Commission entered an order in an administratively-pending Section 5 data security case against LabMD, in which the Commission addressed many of the arguments Wyndham makes in its Motions to Dismiss. *See LabMD, Inc.*, Order Den. Resp't Mot. to Dismiss 3-14, Docket No. 9357 (F.T.C. Jan. 16, 2014), ECF No. 151-1 ("LabMD Order"). In particular, in *LabMD*, the Commission explicitly, and thoroughly, rejected an identical statutory-authority argument, removing any doubt that Section 5 authorizes the FTC to enforce unfairness in the data security context. As the Supreme Court recently confirmed, under *Chevron*, courts "must defer to an agency's interpretation of statutory ambiguity that concerns the scope of the agency's statutory authority (that is, its jurisdiction)." *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863, 1868 (2013) (citing *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837 (1984)). *See also Nat'l Cable & Telecomms Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 985 (2005) ("Before a judicial construction of a statute . . . may trump an agency's, the court must hold that the statute unambiguously requires the court's construction.").

***The D.C. Circuit's Verizon decision.*** Wyndham's reliance on *Brown & Williamson* is untenable. *See* Pl.'s Opp'n 10-15; Mot. to Dismiss Hr'g Tr. 15-16, 45-46, ECF No. 139. The D.C. Circuit recently confirmed that point by rejecting a similar argument based on that decision for reasons that are instructive here. As the circuit court explained, the Supreme Court's

decision in *Brown & Williamson* turned on the fact "that the FDA had not only completely disclaimed any authority to regulate tobacco products, but had done so *for more than eighty years*." *Verizon*, 2014 WL 113946, at *11. Here, as previously explained, the FTC has never disclaimed its authority to enforce Section 5 unfairness in the data security context. *See* Pl.'s Opp'n 13-15, Mot. to Dismiss Hr'g Tr. 27-29; *accord* LabMD Order 7-10. Moreover, as the D.C. Circuit noted, the *Brown & Williamson* court deemed it significant "that the FDA's newly adopted conclusion that it did in fact have authority to regulate this industry would, given its findings regarding the effects of tobacco products and its authorizing statute, *logically require the agency to ban such products altogether, a result clearly contrary to congressional policy*." *Verizon*, 2014 WL 113946, at *11 (emphasis added). Like LabMD, Wyndham "can cite no similar congressional intent to preserve inadequate data security practices that unreasonably injure consumers." LabMD Order 6. Finally, none of the complementary statutes cited by Defendants conflict with the FTC's background Section 5 unfairness authority, let alone "logically require . . . a result clearly contrary to congressional policy." *Verizon,* 2014 WL 113946, at *11.

### A. The FTC Act and Complementary Statutes

The Court specifically asked for supplemental briefing concerning the relationship between the FTC Act's injury requirement set forth in 15 U.S.C. § 45(n), and three other statutes the FTC enforces, all of which have data security components: the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, *et seq*. (1970, amended 2003, 2010), the Gramm-Leach-Bliley Financial Modernization Act ("GLBA"), 15 U.S.C. § 6801, *et seq*. (1999), and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501, *et seq*. (1998).

Section 45(n) limits the definition of "unfair acts or practices" under the FTC Act to those which "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). For the FCRA, GLBA, and COPPA, Congress has in essence said that a violation of the terms of these statutes is itself a sufficient injury to permit the FTC to enforce the statute in federal court. "The passage of [a] statute is, in a sense, an implied finding that violations will harm the public and ought, if necessary, be restrained." *United States v. Diapulse Corp. of Am.*, 457 F.2d 25, 28 (2d Cir. 1972). *See also United States v. Cappetto*, 502 F.2d 1351, 1358-59 (7th Cir. 1974). For example, Congress has determined that when a credit reporting agency violates the FCRA by furnishing a consumer's financial data without a permissible purpose, that violation causes consumer injury. *See Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142 (D.C. Cir. 2001) ("*Trans Union I*") ("[T]he government cannot promote its interest (protection of personal financial data) except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent."). *See also Trans Union LLC v. FTC*, 295 F.3d 42, 53 (D.C. Cir. 2002) ("*Trans Union II*") (as in *Trans Union I*, in the GLBA context, the dissemination of financial data causes the very harm the government seeks to prevent).[1]

[1] Defendants suggest the language in the FCRA and COPPA stating the terms and provisions of the FTC Act are incorporated into those statutes requires the FTC to meet the Section 45(n) substantial injury requirement before it can enforce those statutes. *Supra* pp. 3-4. Section 45(n) places limitations on the Commission's authority to declare

These newer statutes also grant the FTC additional enforcement tools, further differentiating them from the FTC Act. Pl.'s Opp'n 10-12. As the Commission held in *LabMD*, Congress enacted the FCRA, GLBA, and COPPA to address specific concerns in particular sectors of the economy. LabMD Order 10. *See* FCRA, 15 U.S.C. § 1681a (consumer reporting agencies); GLBA, 15 U.S.C. § 6801(a) (financial institutions); COPPA, 15 U.S.C. §§ 6501-6508; 144 Cong. Rec. S12787 (daily ed. Oct. 21, 1998) (statement of Sen. Bryan, drafter and co-sponsor of COPPA) ("The goals of this legislation are: . . . to maintain the security of personally identifiable information of children collected online; and [] to protect children's privacy."). *See also* Mot. to Dismiss Hr'g Tr. 44:17-25; 45:1-22. As the Commission noted, these statutes not only impose specific regulatory requirements on companies in particular areas, but they provide the FTC with additional tools to protect consumers. *See* LabMD Order 10. One of those tools is Administrative Procedure Act rulemaking authority. *See* GLBA, 15 U.S.C. §§ 6801(b), 6805(b)(2); COPPA, 15 U.S.C. § 6502(b)(1)(D); FCRA, 15 U.S.C. § 1681w. Another tool is civil penalty authority, which is not available under Section 5. *See* FCRA, 15 U.S.C. § 1681s; COPPA, 15 U.S.C. § 6505(d). *See also* LabMD Order 10.

Moreover, as opposed to the FTC Act which merely authorizes, the FCRA, GLBA, and COPPA affirmatively compel the FTC to use its authority in particular ways. For example, COPPA instructs the FTC to promulgate rules addressing the specific duties of child-directed website operators to provide notices and obtain parental consent before collecting or disclosing children's personal information. 15 U.S.C. § 6502(b). *See also* FCRA, 15 U.S.C. § 1681w (requiring the FTC to issue regulations requiring proper disposal of consumer information); LabMD Order 10. "Of course, by *compelling* the Commission to take particular steps in those contexts, Congress did not somehow divest the Commission of its preexisting and much broader *authority* to protect consumers against 'unfair' practices." LabMD Order 13. *See also Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-06 (D.C. Cir. 2011).

Again, any question about the FTC's authority in the data security area is put to rest by the *LabMD* decision. In *LabMD*, the unanimous Commission specifically addressed the FCRA, GLBA, and COPPA, holding that "these laws *recognized* the Commission's *existing* enforcement authority, *expanded* that authority in particular respects, and affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts." LabMD Order 10. "To conclude otherwise," the Commission held, "would disregard Congress's instruction to the Commission to protect consumers from harmful practices in evolving technological and marketplace environments." *Id.* As the Commission noted, Section 5 of the FTC Act is an intentionally broad grant of power to the FTC to protect consumers from "unfair or deceptive acts or practices in or affecting commerce." *Id.* at 3-6. This grant of authority applies to *all* acts or practices in or affecting commerce. It is not limited to specific acts or practices, nor was it intended to be. *See* Pl.'s Opp'n 11. There is nothing unique about data security that exempts it from this broad authority. In fact, the Commission held, Congress intended the FTC to "ascertain, on a case-by-case basis, which specific practices should be condemned as 'unfair.'" LabMD Order 5. These findings all warrant substantial deference.

---

particular actions unfair under Section 5, either in litigation or rulemaking. It has no application where Congress itself has statutorily defined categories of actions to be unlawful and authorized the FTC to enforce those statues.

"Statutory ambiguities will be resolved, within the bounds of reasonable interpretation, not by the court but by the administering agency." *City of Arlington*, 133 S. Ct. at 1868, 1871.

**B. Fair Notice**

Although the Court did not request briefing on the topic, Defendants return to the untenable claim that the FTC has not satisfied due process fair notice requirements because it has not issued a comprehensive rule on data security. *Supra* pp. 4-5. This argument has no basis in the law. *See* Pl.'s Opp'n 17-25. Were Defendants correct, the FTC could never protect consumers from unfair practices without first issuing a regulation governing the specific practice at issue. Such a requirement would undermine 100 years of FTC precedent, and it would crash headlong into the Supreme Court's recognition that "the proscriptions in [Section] 5 are flexible, to be defined with particularity by the myriad of cases from the field of business," a fact that inherently requires the FTC to apply Section 5 'to the facts of particular cases arising out of unprecedented situations." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965). *See also FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (Congress delegated broad authority "to the Commission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply."). Indeed, such a requirement would be an exercise in futility because "[t]here is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *Sperry & Hutchinson Co.*, 405 U.S. at 241.

Section 45(n)'s three part test addressing when an act or practice is "unfair" adequately provides "a person of ordinary intelligence fair notice of what is prohibited" and constrains the FTC's authority to bring unfairness actions sufficiently so that the FTC may not enforce the FTC Act in a "seriously discriminatory" way. *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). *See also* LabMD Order 15-17. Agencies routinely bring enforcement actions where the governing statute or rules lack particularized prohibitions, and instead require compliance with a general reasonableness standard like that set forth in Section 45(n). *See* Pl.'s Opp'n 23-24 (discussing the National Labor Relations Board's "good faith" requirement, and the Occupational Safety and Health Act's "general duty clause."). In fact, this Circuit has rejected fair notice challenges to similar reasonableness standards. *See Voegele Co., Inc. v. Occupational Safety & Health Review Comm'n*, 625 F.2d 1075, 1078 (3d Cir. 1980).[2]

[2] Without acknowledging the discussion of the case at the Motion to Dismiss Hearing, Defendants cite to *Secretary of Labor v. Beverly Healthcare-Hillview* ("*Beverly*"), 541 F.3d 193 (3d Cir. 2008), in baldly asserting that to satisfy fair notice requirements the FTC must provide "ascertainable certainty" of how it will enforce Section 5 unfairness. *See supra* p. 4. As the FTC explained at the hearing, however, the ascertainable certainty test set forth in *Beverly* does not apply here. *Beverly*, 541 F.3d at 202. The FTC has not given "conflicting public interpretations" of how it will apply "unfairness." Rather, the FTC has repeatedly, and publicly, explained that it will enforce unfairness consistent with the unambiguous plain terms of the statute, which defines unfair acts or practices through the Section 45(n) balancing test. *See United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004); Mot. to Dismiss Hr'g Tr. 72-74; Pl.'s Opp'n 13-14, 17-20. In fact, the FTC's many public complaints and consent agreements, as well as public statements and business guidance, have provided further contour to the Section 45(n) test as it is applied in the data security context. Pl.'s Opp'n 18-20. Any doubt as to whether the FTC meets fair notice here is settled in this Circuit by *Voegele*, which noted that similar "reasonable person" standards survive fair notice challenges even though they provide no guidance other than to act as a reasonable person would. 625 F.2d at 1078 (citing *B&B Insulation, Inc. v. Occupational Safety & Health Review Comm'n*, 583 F.2d 1364 (5th Cir. 1978)). *See also* LabMD Order 18-19.

Moreover, the FTC's decision to enforce the FTC Act's prohibition of unfair practices through individual enforcement actions rather than rulemaking is well within the FTC's "informed discretion." *PBW Stock Exch., Inc. v. SEC*, 485 F.2d 718, 732 (3d Cir. 1973). *See also SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947); Pl.'s Opp'n 20-22; LabMD Order 14-15. "[A]gency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication[,] [and] [t]he Commission seems on especially solid ground in choosing an individualized process where important factors may vary radically from case to case." *Am. Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990).[3]

Accordingly, courts routinely uphold FTC unfairness actions despite the fact that there are no preexisting rules specifically governing the specific conduct at issue. In *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010), the Ninth Circuit affirmed the district court's holding that the defendants' acts or practices related to online check drafting and delivery were unfair even though there is no specific regulation addressing the practice. The Tenth Circuit reached the same conclusion in *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009), even though no regulation explicitly prohibited the conduct in question. *See also* Pl.'s Opp'n 11. In short, Defendants' claim that the FTC must issue regulations governing data security before it may enforce its unfairness authority is inconsistent with the FTC's long enforcement history.

Moreover, as the Commission held in *LabMD*, the claim that agencies can only satisfy due process through issuing specific regulations is "particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care," and when they "find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages." LabMD Order at 17. "There is simply no basis to conclude that the FTC's application of the Section [45](n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties." *Id.*[4]

For the reasons set forth above, and in prior briefing and argument, the Court should deny Defendants' Motions to Dismiss.

---

[3] Nor is that doctrine altered by the National Institute of Standards and Technology's ("NIST") critical infrastructure cyber security framework or the Department of Homeland Security's ("DHS") internal network assessment. *See supra* p. 5. The NIST framework is not an enforceable regulation requiring specific security measures. *See* Pl.'s Opp'n 16. Rather, it sets forth a voluntary *process* by which critical infrastructures can assess the threats they face and the protections they should reasonably take in response. *See, e.g.*, Exec. Order 13636, 78 FR 11737 (2013). The DHS Report is DHS's own internal assessment of its network security, and has no bearing on this case.

[4] In support of their claim that the FTC must make rules in the data security area, Defendants offer a single comment of a Congressman at a Subcommittee hearing (which in context appears actually to be about the FTC's competition-side efforts and not consumer protection unfairness actions), and an amicus brief from the U.S. Chamber of Commerce. *See supra* p. 5. Whatever weight should be accorded a single comment in a Subcommittee hearing, and an amicus brief, these statements cannot overcome the well-settled precedent holding that the FTC comports with due process even when proceeding through adjudication, rather than rulemaking. Pl.'s Opp'n 20-22.

Dated: January 21, 2014

/s/Jonathan E. Zimmerman
Lisa Weintraub Schifferle
Kristin Krause Cohen
Kevin H. Moriarty
John A. Krebs
Jonathan E. Zimmerman
Andrea V. Arias
Federal Trade Commission
600 Pennsylvania Ave., NW
Mail Stop NJ-8100
Washington, D.C. 20580

*Attorneys for Plaintiff*
*Federal Trade Commission*

*/s/ Jennifer A. Hradil*
Jennifer A. Hradil, Esq.
Justin T. Quinn, Esq.
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102-5310
(973) 596-4500

Eugene F. Assaf, P.C., DC Bar 449778
*Pro Hac Vice*
K. Winn Allen, DC Bar 1000590
*Pro Hac Vice*
KIRKLAND & ELLIS, LLP
655 Fifteenth St. N.W.
Washington, D.C. 20005
(202) 879-5078
eugene.assaf@kirkland.com
winn.allen@kirkland.com

Douglas H. Meal, MA Bar 340971
*Pro Hac Vice*
David T. Cohen, MA Bar 670153
Pro Hac Vice
ROPES & GRAY, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517
douglas.meal@ropesgray.com
david.cohen@ropesgray.com

*Attorneys for Defendants*

cc: Counsel via ECF