No. 14-3514

In the United States Court of Appeals for the Third Circuit

FEDERAL TRADE COMMISSION

v.

WYNDHAM WORLDWIDE CORP., a Delaware corporation,
WYNDHAM HOTEL GROUP, LLC, a Delaware limited liability company,
WYNDHAM HOTELS & RESORTS, LLC, a Delaware limited liability company,
AND WYNDHAM HOTEL MANAGEMENT, INC., a Delaware corporation

WYNDHAM HOTELS & RESORTS, LLC,

Appellant

On Appeal from the U.S. District Court for the District of New Jersey (Salas, J.)
Civil Action No. 2:13-cv-01887-ES-JAD

APPELLANT'S REPLY BRIEF

Michael W. McConnell
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, DC 20005
(202) 879-5000

Eugene F. Assaf, P.C.
Christopher Landau, P.C.
Susan M. Davies
K. Winn Allen
Ronald K. Anguas, Jr.
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, DC 20005
(202) 879-5000

Counsel for Appellant Wyndham Hotels & Resorts, LLC

Additional Counsel Listed on Inside Cover

December 8, 2014

Additional Counsel for
Appellant Wyndham Hotels & Resorts, LLC

Douglas H. Meal
David T. Cohen
ROPES & GRAY LLP
800 Boylston Street
Boston, MA 02199
(617) 951-7000

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

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Other Authorities

INTRODUCTION

The FTC's brief proposes a breathtaking expansion of agency authority. In alleging that Wyndham committed an "unfair" business practice, the Commission does not assert that Wyndham sought to take advantage of its customers or otherwise acted unethically or unscrupulously toward them. To the contrary, the Commission acknowledges, as it must, that Wyndham *itself* was victimized by criminal hackers, and its customers were thereby victimized only derivatively. The FTC insists, however, that Wyndham committed an "unfair" business practice by breaching "reasonable standards of care" in protecting consumer payment-card data. FTC Br. 40. But that is nothing more than an allegation of negligence. It has been settled for almost a century that negligence is neither necessary nor sufficient to establish an "unfair" business practice, and no court has ever interpreted the FTC's authority over "unfair" business practices as a free-floating power to enforce "common law principles of negligence." *Id.* at 44. This Court should not be the first.

And even assuming that the FTC had such sweeping authority, it has not provided regulated entities with constitutionally adequate

notice of what the law purportedly requires and forbids. There are few more pressing issues confronting American society than cybersecurity. For the Commission to give American businesses, large and small, no more guidance than a simple command to act "reasonably"—on pain of administrative prosecution and sanctions—is to make a mockery of basic constitutional norms of fair notice.

Finally, the FTC has not pleaded facts that plausibly state a claim of substantial and non-avoidable consumer injury. The Commission cannot, and does not, deny that consumers can avoid fraudulent charges by simply notifying their payment-card companies. Indeed, the Commission has admitted in discovery in this case that it has yet to identify a *single* individual consumer who was not fully reimbursed. Given the absence of any facts plausibly showing substantial and non-avoidable consumer injury, the Commission's conclusory recitation of the applicable legal standard cannot save the complaint from dismissal.

ARGUMENT

I. An Alleged Failure To Provide "Reasonable" Cybersecurity Is Not An "Unfair" Business Practice.

By attempting to equate "unfair" business practices with allegedly "unreasonable" cybersecurity protections, the FTC advances an open-

ended and untenable theory of its own authority. According to the Commission, Congress gave it "broad discretion" to deem business practices "unfair" under Section 5(a), FTC Br. 4, subject "only" to the limitations set forth in Section 5(n), *id*. at 22, 25. The FTC thus argues that Section 5(n) defines "unfair" business practices under Section 5(a), so that the agency can regulate *any* business practice that causes "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); *see* FTC Br. 19-22.

That argument fails as a matter of statutory interpretation. Section 5(n) does not purport to define what constitutes an "unfair" business practice under Section 5(a); rather, by its plain terms Section 5(n) states that "[t]he Commission shall have *no* authority ... to declare unlawful an act or practice on the grounds that such act or practice is unfair *unless* the act or practice" satisfies certain requirements. 15 U.S.C. § 45(n) (emphasis added). Far from defining what acts or practices may be deemed "unfair" in the first instance, Section 5(n) simply specifies that acts or practices may *not* be deemed "unfair" unless those requirements are satisfied. Because that provision is

phrased in the negative, not the affirmative, it does not remotely suggest that any act or practice that *satisfies* those requirements *ipso facto* may be deemed "unfair." The Commission's contrary argument represents an ironic attempt to transform a *limitation* on its unfairness authority into an *expansion* of that authority.

Once it is recognized that the term "unfair" in Section 5(a) has meaning separate and apart from the requirements of Section 5(n), the FTC's theory falls apart. Both as a matter of common usage and common sense, an "unfair" business practice is one that seeks to take advantage of consumers, or otherwise injures them through unscrupulous or unethical behavior. *See* Wyndham Br. 18-21.[1] That is precisely the conduct that Congress targeted when it amended the FTC Act in 1938 to add the "unfair … acts or practices" language at issue here. *See* S. Rep. No. 74-1705, at 2 (1936) ("[T]he Commission should

[1] Contrary to the FTC's assertion, this argument is not "waived." FTC Br. 23. Wyndham has consistently argued that Section 5 does not give the FTC authority to regulate cybersecurity. Having preserved that legal issue, Wyndham is free to advance all supporting arguments. *See, e.g.*, *Citizens United v. FEC*, 558 U.S. 310, 330-31 (2010) ("[O]nce a federal claim is properly presented, a party can make any argument in support of that claim; parties are not limited to the precise arguments they made below.") (internal quotation omitted).

have jurisdiction to restrain unfair or deceptive acts and practices *which deceive and defraud the public generally*.") (emphasis added); *id.* at 3 ("Under the proposed amendment, the Commission would have jurisdiction *to stop the exploitation or deception of the public*.") (emphasis added).

And that is precisely how other courts have construed the term "unfair." *See, e.g.*, *Crawford v. LVNV Funding, LLC*, 758 F.3d 1254, 1258 (11th Cir. 2014) ("The plain meaning of 'unfair' is 'marked by injustice, partiality, or deception.'") (quoting *LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1200 (11th Cir. 2010) (*per curiam*)); *Massachusetts Eye & Ear Infirmary v. QLT Phototherapeutics, Inc.*, 412 F.3d 215, 243 (1st Cir. 2005) (looking to whether an act is "immoral, unethical, oppressive, or unscrupulous" in determining whether it violates state law prohibiting "unfair or deceptive acts or practices") (internal quotation omitted).

The FTC points to other dictionaries that define "unfair" as acting "unreasonably," FTC Br. 24 n.8, or "contrary to laws or conventions," *id.* at 23 (internal quotations omitted). The FTC thus argues that a business acts "unfairly" not only when it preys on consumers, but also

when it acts "negligen[tly]" and consumers are harmed by such negligence. *See, e.g.*, FTC Br. 29 (arguing that Section 5 liability can be imposed if "a business … exposes itself to harm through negligence"); *id.* at 40 (arguing that the FTC is enforcing "basic negligence principles").

Whatever else the term "unfair" in Section 5 might mean, it surely cannot mean simple negligence. Such an interpretation would drastically expand the scope of Section 5 by turning any common law tort into an "unfair" business practice under the FTC Act. If a supermarket is sloppy about sweeping up banana peels and customers slip and fall, the supermarket may be liable for negligence, but it has not committed an "unfair" act or practice within the meaning of the FTC Act. There is absolutely no indication that the 1938 Congress intended to turn the FTC into a federal enforcer of state "common-law negligence principles." FTC Br. 41; c*f. United States v. Bass*, 404 U.S. 336, 350 (1971) (rejecting proposed interpretation of federal statute that would transform "traditionally local criminal conduct" into "a matter for federal enforcement"). Indeed, numerous state and federal courts have rejected attempts to equate mere negligence with unfairness in the

context of construing analogous state prohibitions on "unfair" trade practices. *See, e.g.*, *Clarkson v. Orkin Exterminating Co.*, 761 F.2d 189, 190-91 (4th Cir. 1985) ("There is no support in [state] law for the proposition that a service person violates the unfair trade practice statute if he performs his job poorly or overlooks something which should have attracted his attention."); *Hachigian v. Royal Barry Wills Assocs., Inc.*, No. 05-CV-3830-F, 2009 WL 4894554, at *2 (Mass. Super. Ct. Oct. 7, 2009) ("It is axiomatic that mere negligence is not an unfair trade act or practice."); *A-G Foods, Inc. v. Pepperidge Farm, Inc.*, 579 A.2d 69, 76 (Conn. 1990) ("[Defendant] argues that its negligence was not an unfair or deceptive trade practice…. We agree.").

Nor does it "contradict[] decades of precedent," FTC Br. 26, to recognize that the statutory term "unfair" does not embrace any and all negligent conduct, such as a company's alleged failure to adopt "reasonable" cybersecurity practices. Indeed, the FTC cites *no* court in the history of American law that has deemed allegedly negligent acts *ipso facto* to be "unfair" practices under the FTC Act. Indeed, the great majority of the cases cited by the FTC found practices "unfair" in precisely the circumstances identified by Wyndham—namely, when

businesses sought to prey on consumers through unscrupulous or unethical behavior. *See, e.g.*, *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1356-58 (11th Cir. 1988) (business raised prices for pest-control services despite stating in consumer marketing materials and in over 200,000 contracts with homeowners that prices would not increase for the lifetime of a dwelling); *American Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 973-74 (D.C. Cir. 1985) (business routinely took security interests in used household goods with intent to threaten consumers with repossession if they did not agree to unfavorable refinancing terms); *Spiegel, Inc. v. FTC*, 540 F.2d 287, 290-91 (7th Cir. 1976) (business intentionally sued its customers in courts far from their homes because the travel costs alone would exceed the debts sought to be recovered).[2]

[2] Recognizing that businesses only treat consumers "unfairly" when they seek to take advantage of them is entirely consistent with the FTC's 1980 Policy Statement. *See* FTC Br. 26. That document states that the Commission will not regard "immoral, unethical, oppressive, or unscrupulous" conduct as "an *independent* basis for a finding of unfairness" under Section 5. FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), *available at* http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (emphasis added). Wyndham has never suggested that "immoral, unethical, oppressive, or unscrupulous conduct" alone—without some evidence of substantial, unavoidable consumer harm—is actionable under the FTC Act.

The FTC fares no better by pointing to cases in which a business "furnishe[d] another with the means of consummating a fraud." FTC Br. 28 (internal quotation omitted). Those cases simply reject a "*Napster*"-style defense, *see A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); *see also MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), by holding that a business acts "unfairly" when it knowingly provides others with the goods or services necessary to prey on consumers, *see*, *e.g.*, *FTC v. Winsted Hosiery Co.*, 258 U.S. 483 (1922) (clothing manufacturer knowingly sold mislabeled wool products to retailers, who sold them to consumers); *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1154 (9th Cir. 2010) (company provided software that fraudsters used to draft over 155,000 fraudulent checks, totaling more than $400,000,000). But Wyndham is not alleged to have provided the hackers with the tools used to undertake their illegal acts, or to have profited in any way from their wrongdoing; to the contrary, Wyndham *itself* was a victim of those crimes.

Sustaining the FTC's claimed authority over cybersecurity would also be inconsistent with the narrow grants of cybersecurity authority that Congress *has* made to the FTC through the Fair Credit Reporting

ACT ("FCRA"), Gramm-Leach-Bliley Act ("GLBA"), and Children's Online Privacy Protect Act ("COPPA"). *See* Wyndham Br. 24-28. The FTC attempts to dismiss those statutes as merely "supplement[ing] the FTC's general authority to proceed under Section 5." FTC Br. 30. But those statutes do not merely provide the FTC with "streamlined rulemaking authority" and additional "remedies." *Id.* at 30-31. Instead, all three statutes include clear grants of *substantive* authority authorizing the FTC to regulate cybersecurity in certain narrow contexts. *See* Wyndham Br. 26-27. The FTC does not (because it cannot) explain why those grants of substantive authority would have been necessary if the FTC already possessed "general authority [over cybersecurity] under Section 5." FTC Br. 30.[3]

[3] The Commission asserts that "all three statutes authorize the FTC to obtain relief even when it cannot demonstrate substantial consumer injury." FTC Br. 31. That assertion is demonstrably incorrect. COPPA, for example, authorizes enforcement "with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the [FTC] Act ... were incorporated into and made part of this chapter." 15 U.S.C. § 6505(d). Similarly, the GLBA authorizes enforcement "under the [FTC] Act." *Id.* § 6805(a)(7). And while FCRA authorizes FTC enforcement against any person who violates that statute, "irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the [FTC] Act," *id.* § 1681s(a)(1), that only underscores (contrary to the FTC's argument)

Nor, contrary to the FTC's assertion, did Congress enact the FCRA, GLBA, and COPPA merely to "*require[]* the FTC … to address policy concerns" in areas where "the FTC already had discretionary authority to act." *Id.* at 31 (emphasis omitted). None of those statutes "require" the FTC to do anything—they merely authorize agency action (and thereby underscore the previous lack of authority). *See, e.g.*, 15 U.S.C. § 1681s(a)(1) ("The [FTC] shall be *authorized* to enforce compliance with the requirements imposed by [FCRA]" (emphasis added)); *id.* § 6804(a)(1)(C) ("[T]he [FTC] shall have *authority* to prescribe such regulations as may be necessary to carry out the purposes of [GLBA]") (emphasis added); *id.* § 6505(d) (authorizing FTC enforcement of COPPA "with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the [FTC] Act ... were incorporated into and made part of this chapter."). The FTC tellingly cites no statutory text or legislative history suggesting that Congress believed that it was mandating the exercise of some latent discretionary authority that the FTC already possessed under Section 5.

---

that the requirements of Section 5(n) are logically and legally distinct from the element of "unfairness" in Section 5(a).

The FTC also argues that the FCRA, GLBA, and COPPA are irrelevant to construing the scope of Section 5 because there is no "affirmative conflict between the FTC Act and the more recent statutes." FTC Br. 33. That is wrong and, in any case, irrelevant. The substantive grants of authority in the FCRA, GLBA, and COPPA *do* "affirmative[ly] conflict" with the FTC's assertion of "general authority" over data security under Section 5. But even setting aside that conflict, a court's duty to "make sense rather than nonsense out of the *corpus juris*," *West Va. Univ. Hosps., Inc. v. Casey*, 499 U.S. 83, 101 (1991), is not triggered "*only* when statutes conflict," FTC Br. 35 (emphasis added). To the contrary, "a specific policy embodied in a later federal statute should control our construction of the [earlier] statute, even though it ha[s] not been expressly amended." *United States v. Estate of Romani*, 523 U.S. 517, 530-31 (1998).[4]

[4] The Commission asserts that *Romani* "involved a 'plain inconsistency' between statutes," FTC Br. 35 (quoting 523 U.S. at 520), but the quoted words are drawn from the Supreme Court's description of the *lower* court's analysis. The Supreme Court held that "it does not seem appropriate to view the issue in this case as whether the [later statute] has implicitly amended or repealed the [earlier] statute," but instead "how best to harmonize the impact of the two statutes ...." 523 U.S. at 530; *see also Things Remembered, Inc. v. Petrarca*, 516 U.S. 124, 127-29 (1995) (harmonizing non-conflicting statutes); *id.* at 131-36

Using similar reasoning, the FTC attempts to explain away its prior requests to Congress for general data-security authority as merely having sought tools that would have "*supplemented* the FTC's existing Section 5 authority." FTC Br. 35 (emphasis in original). That is revisionist history. After asking Congress for years to enact legislation providing such general authority, *see, e.g.*, FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* at 37 (2000), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf, the FTC abandoned those efforts and "decided to move forward on its own without any new, specific privacy laws or delegation of authority from Congress," Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 Admin. L. Rev. 127, 143 (2008). Such an attempt to skirt the legislative process contravenes bedrock principles of administrative law.

(Ginsburg, J., concurring); *Miles v. Apex Marine Corp.*, 498 U.S. 19, 30-33 (1990) (same).

The FTC's recent administrative ruling in *LabMD*—in which the Commission unsurprisingly sustained its own authority to regulate cybersecurity as an "unfair" business practice—is also not entitled to *Chevron* deference. *See* FTC Br. 37-40 (citing *In re LabMD*, FTC Dkt. No. 9357 (Jan. 16, 2014) (attached to FTC Br.)). Deference is unwarranted at *Chevron* step one because the plain meaning of the statutory term "unfair" unambiguously excludes conduct that is alleged merely to be "negligent" or to fall short of "reasonable standards of care." *See supra* at 3-9; *Chevron USA, Inc. v. NRDC, Inc.*, 467 U.S. 837, 842-43 (1984). And even if Section 5 were ambiguous on that point, the statute's prohibition on "unfair" business practices cannot "reasonably" be read to include such behavior. *See id.* at 843; *see also AT&T Corp. v. Iowa Utilities Bd.*, 525 U.S. 366, 392 (1999); *Pennsylvania Fed'n of Sportsmen's Clubs, Inc. v. Kempthorne*, 497 F.3d 337, 351-53 (3d Cir. 2007); *Zheng v. Gonzales*, 422 F.3d 98, 116-20 (3d Cir. 2005).

Deferring to the Commission's interpretation of its authority would be particularly inappropriate here because that interpretation raises serious constitutional questions under the non-delegation doctrine. *See* Wyndham Br. 32-35; *Edward J. DeBartolo Corp. v.*

Florida Gulf Coast Bldg. & Constr. Trades Council, 485 U.S. 568, 574-75 (1988) (declining to afford deference to an agency's construction of a statute that would raise "serious constitutional problems"). Like the district court below, the FTC proposes no meaningful limiting principle on the scope of its "unfairness" authority, arguing instead that its enforcement efforts are within its own "broad discretion." FTC Br. 4. Courts typically construe statutes to avoid such "open-ended grant[s]," *Industrial Union Dep't v. American Petroleum Inst.*, 448 U.S. 607, 646 (1980) (plurality opinion), and applying that principle here requires construing the term "unfair" to, at the very least, exclude a business' alleged failure to adhere to "reasonable standards of care." FTC Br. 40.

Nor is the broad power claimed by the FTC to define the term "unfair" analogous to the discretion afforded to other agencies in other contexts. *See id.* at 39 (quoting 47 U.S.C. §§ 201(b) & 307(a) and 29 U.S.C. § 158(d)). As the Supreme Court has explained, "the degree of agency discretion that is acceptable varies according to the scope of the power congressionally conferred," *Whitman v. American Trucking Ass'ns, Inc.*, 531 U.S. 457, 475 (2001)—the narrower the scope of the delegated power, the greater the permissible delegation.

The FTC misses the point by citing examples of agencies given broad discretion in relatively narrow contexts: setting communications rates, awarding broadcast licenses, and assessing labor negotiations. *See* FTC Br. 39. Where, as here, the delegated authority "affect[s] the entire national economy"—such as determining what constitutes an "unfair" business practice—Congress "must provide substantial guidance." *Whitman*, 532 U.S. at 475.[5]

In the end, the FTC and its *amici* resort to policy arguments to justify the FTC's attempts to regulate cybersecurity. *See, e.g.*, FTC Br. 2, 16, 25-26; *see also, e.g.*, Br. of *Amici Curiae* Public Citizen, Inc. *et. al* 5-6; Br. of *Amici Curiae* Ctr. for Democracy & Tech. *et. al* 21-24; Br. of *Amici Curiae* Elec. Privacy Info. Ctr. *et. al* 8-18. But those arguments miss the point. No one disputes that cybersecurity is a critically important matter—particularly when new hacks are reported almost

[5] The FTC's assertion that Section 5 has "withstood repeated attack on delegation grounds," FTC Br. 39 (internal quotation omitted), misses the point. Wyndham does not suggest that term "unfair" in the FTC Act inherently represents an unconstitutional delegation of legislative authority. Rather, as explained in the text, the non-delegation problem here arises from the FTC's novel interpretation of the term "unfair" to sweep in all of negligence law, *see id.* at 41, even where (as here) there is no allegation that a business sought to prey on consumers or benefit from others' preying on consumers.

daily against not only businesses but also government entities. *See*, *e.g.*, Nicole Perlroth, *State Department Targeted by Hackers in 4th Agency Computer Breach*, New York Times, Nov. 16, 2014, *available at* http://www.nytimes.com/2014/11/17/us/politics/state-department-targeted-by-hackers-in-4th-agency-computer-breach.html?_r=0. "[N]o matter how important, conspicuous, and controversial the issue," however, an agency's authority to regulate "must always be grounded in a valid grant of authority from Congress." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 161 (2000) (internal quotation omitted). Indeed, the more "important, conspicuous, and controversial the issue," the *less* likely that Congress would have delegated regulatory authority in an obscure or tacit manner, and the more skeptical courts should be of an agency's "claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy." *Utility Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2444 (2014) (internal quotation omitted). And that point is all the more compelling here, where Congress *specifically prohibited* the FTC from invoking "public policy considerations" as a "primary basis" for a determination of unfairness. 15 U.S.C. § 45(n).

II. The FTC Has Not Provided Constitutionally Adequate Notice Of What Constitutes "Reasonable" Cybersecurity.

The FTC next defends its "*ex post* rather than *ex ante*" enforcement regime, Maureen K. Ohlhausen, *The Procrustean Problem with Prescriptive Regulation*, Remarks at the Free State Foundation Telecom Conference at 11 (Mar. 18, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/291361/140318fsf.pdf, claiming that regulated entities are not "entitled to detailed written guidance" and that the FTC is no different from an ordinary tort plaintiff bringing a negligence suit, FTC Br. 41. The FTC cannot meet its fair-notice obligations, however, merely by telling businesses to "act reasonably," and then evaluating after-the-fact whether that indeterminate standard was satisfied. Indeed, the Director of the FTC's Bureau of Consumer Protection recently acknowledged the need for "transparency" with respect to the FTC's position on data security, as well as the Commission's traditional reluctance to deliver a "clear message and lesson" in this area. Allison Grande, *FTC Bureau Head Wants More Privacy Closing Letters Issued*, Law360 (Dec. 3, 2014), *available at* https://www.law360.com/articles/601348.

A. A Command to "Act Reasonably" Does Not Satisfy the FTC's Fair-Notice Obligation.

The FTC's primary argument is that the FTC Act alone—without further elaboration—provides constitutionally adequate notice because Section 5 incorporates "basic negligence principles" and "[a]ll companies are on notice that … they must follow commercially reasonable standards of care." FTC Br. 40. That argument proves far too much. If an agency can satisfy fair-notice principles merely by telling regulated entities to "act reasonably," then the FTC has worked a revolution in the law. *See, e.g.*, *Belle Maer Harbor v. Charter Twp. of Harrison*, 170 F.3d 553, 558 (6th Cir. 1999) ("[T]his court cannot say that a commonly accepted meaning exists for the term 'reasonable' which would provide an inspection officer with guidance in interpreting the Ordinance."); *see also In re Metro-East Mfg. Co.*, 655 F.2d 805, 810-11 (7th Cir. 1981) (concluding that a regulation authorizing "reasonable investigative techniques" by OSHA did not provide fair notice of what air sampling devices would be used). As the Sixth Circuit has explained, a "reasonableness" standard cannot satisfy fair-notice requirements in the enforcement context because the concept of "reasonableness" is "susceptible to a myriad of interpretations conferring on the

[government] a virtually unrestrained power" to bring suit. *Belle Maer Harbor*, 170 F.3d at 558 (internal quotation omitted).

The FTC argues that its "reasonableness" standard provides fair notice because it incorporates "background common law principles" of which Wyndham (and others) should be aware. FTC Br. 44. In the same breath, however, the FTC insists that "common law principles do *not* limit the FTC's authority under Section 5 as a general matter." *Id.* (emphasis added). These two propositions are, of course, irreconcilable. As a matter of law and logic, "common law principles" that do not limit the FTC's enforcement authority cannot provide fair notice of what the law requires.

Proving the point, the same "background common law principles" on which the FTC relies to rebut Wyndham's fair-notice argument would mandate *dismissal* of this case if those principles actually constrained the Commission. For example, although the FTC argues that Wyndham "effectively acted in the position of a bailee, which must exercise reasonable and ordinary care in protecting the property it has accepted from a bailor," FTC Br. 41 (quotations omitted), such a bailment theory has been rejected in every data-breach case in which it

has been asserted. *See, e.g.*, *Bell v. Blizzard Entm't, Inc.*, No. 12-CV-09475, slip op. at 15 (C.D. Cal. July 11, 2013) ("No court has held that personal information is a chattel that can be bailed."); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 974-75 (S.D. Cal. 2012); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1126-27 (N.D. Cal. 2008), *aff'd* 380 F. App'x 689 (9th Cir. 2010). And, under the laws of most States, the economic loss doctrine generally bars recovery under a negligence theory for all losses arising from a data breach, unless the plaintiff can show that the breach caused physical injury. *See, e.g.*, *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 175-78 (3d Cir. 2008) (Pennsylvania law); *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498-99 (1st Cir. 2009) (Massachusetts law); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 530-31 (N.D. Ill. 2011) (Illinois law). The FTC cannot have it both ways: either those same "background common law principles" should apply to an FTC enforcement action under Section 5 (in which case this lawsuit should be dismissed) or the FTC cannot rely on those same principles to defeat a fair-notice challenge.

The FTC's attempt to analogize its cybersecurity enforcement efforts to common-law negligence actions also fails because there is, in fact, no "common law" of Section 5 data security to which businesses can look to understand their obligations *ex ante*. In tort law, parties have centuries' worth of judicial precedents—stemming from cases adjudicated on the merits—to inform their conduct. *See, e.g.*, *City of Okla. City v. Tuttle*, 471 U.S. 808, 818 n.5 (1985) ("One reason why courts render decisions and written opinions is so that parties can order their conduct accordingly."). That is simply not the case here, where no court has ever opined on what data-security practices are "reasonable."

It is no answer for the FTC to argue that "similarly general standards of conduct are ubiquitous in statutory law." FTC Br. 42. The FTC's cherry-picked examples have substantially more gloss than the Commission's bare directive to employ "reasonable" data security. The "Rule of Reason" under the Sherman Act, for example, has been a part of American jurisprudence for over a century, *see generally Standard Oil Co. of N.J. v. United States*, 221 U.S. 1 (1911), and has been fleshed out through hundreds of reasoned judicial decisions. Similarly, an employer attempting to determine what occupational safety protections

it must employ can look to hundreds of adjudications for guidance. *See* "ALJ Decisions—2013," *OSHRC*, *available at* http://www.oshrc.gov/decisions/alj13.html (listing more than 50 cases involving OSHA safety regulations that were decided by ALJs in 2013 alone).

Finally, the fact that Wyndham's *own* privacy policy stated that the company would take "'commercially reasonable efforts'" to protect consumer information does not solve the FTC's fair-notice problem. FTC Br. 43 (quoting Wyndham privacy policy). Wyndham believes that it undertakes and always has undertaken "commercially reasonable" data-security practices. Wyndham's view of what data-security practices are reasonable, however, is not necessarily the same as the FTC's. Wyndham's privacy policy described the specific practices that the company understood to be "commercially reasonable," including the use of "128-bit encryption" and a "Secure Sockets Layer" to encrypt data. To the extent the FTC contends Wyndham did not employ those particular data-security measures, that argument goes to the FTC's separate *deception* claim, which is not before this Court. To the extent the FTC argues that its understanding of the term "reasonable" required Wyndham to do *more* than what was in the privacy policy,

Wyndham lacked notice of what the FTC believed those additional practices to be.

B. Unlitigated Consent Decrees Do Not Provide Fair Notice.

The FTC next argues that it has provided fair notice because it has issued "a series of administrative decisions finding specific companies liable for inadequate data-security practices." FTC Br. 45. That argument grossly overstates the content of the "complaints and consent decrees" on which the FTC relies. *Id.* Those materials are *not* "finding[s]" of "liab[ility]" made by a neutral arbiter after an adversarial litigation process. To the contrary, they are settlements, and—like most settlements—often involve pragmatic business decisions to avoid protracted litigation, not admissions of liability. Indeed, many of the FTC's data-security consent decrees include explicit *denials* of wrongdoing. *See*, *e.g.*, *In re CVS Caremark Corp.,* Agreement Containing Consent Order at 2, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/02/090218cvsagree.pdf. ("Proposed respondent expressly denies the allegations set forth in the draft complaint … and expressly denies that the law has been violated."). The consent decrees on which the FTC relies neither

purport to say what the law *is* nor bind the FTC's enforcement discretion going forward.

Contrary to the FTC's assertion, the Supreme Court has never stated that unligitated, non-binding consent decrees "are precisely the type of administrative materials that ... parties may 'properly resort to for guidance.'" FTC Br. 48-49 (quoting *General Elec. Co. v. Gilbert*, 429 U.S. 125, 142 (1976)). *Gilbert* involved a formal agency guideline, not a consent decree, and the Court in *Gilbert* actually found the guideline at issue to be unpersuasive. *See* 429 U.S. at 143. Indeed, the Supreme Court has explained that "[t]he circumstances surrounding … negotiated [consent] agreements are so different that *they cannot be persuasively cited in a litigation context*." *United States v. E.I. du Pont de Nemours & Co.*, 366 U.S. 316, 330 n.12 (1961) (emphasis added); *see also* Wyndham Br. 41. The fact that the FTC "publishes these materials on its website" and "provides notice in the Federal Register," FTC Br. 45-46, moreover, is immaterial—the problem is not that Wyndham lacked notice *of the consent decrees*, but that consent decrees by their nature do not give notice *of what Section 5 requires*.

That distinction is hardly "beside the point." FTC Br. 48. To provide the notice required by due process, a statement must in some sense declare what conduct the law proscribes and thereby constrain enforcement discretion. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999). Otherwise, the statement provides no real notice at all. Here, the consent decrees at issue do not purport to say what the law requires, are not "controlling precedent for later Commission action," and do not limit the Commission's enforcement authority in any way. *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976). Such documents cannot provide the fair notice that due process requires.

And even if the FTC's consent decrees were properly part of the fair-notice analysis, the Commission overstates the guidance those documents provide. There were only five "unfair practices" consent decrees issued before the first cyberattack against Wyndham, *see* FTC Br. 47 n.16, and all of them used general language to describe the purportedly wrongful conduct—such as failing to take "sufficient" measures to detect intrusions or to use "readily available security measures." *In re BJ's Wholesale Club*, 140 F.T.C. 465, 467 (2005). Those vague descriptions, moreover, amounted to an alleged violation

only when they were "taken together." *Id.* at 476; *see also* Wyndham Br. 42-43. That "taken together" qualifier, when coupled with the decrees' vague language, prevents businesses from understanding what cybersecurity protections are *actually required* to avoid liability.

C. The FTC's Data Security Brochure Does Not Provide Fair Notice.

The FTC's reliance on its informal data-security brochure is also misplaced. Although the FTC never relied on the brochure before Wyndham raised its fair-notice challenge, the FTC now argues that the brochure provides a "catalogue" of the data-security practices Section 5 requires. *See* FTC Br. 49 (arguing that the brochure "identified the basic data-security obligations that Wyndham failed to satisfy") (typeface and capitalization modified); *id.* (arguing that the brochure "provided a catalogue of reasonable data-security practices"); *id.* at 51 (arguing that the brochure "provided considerable guidance on the elements of commercially reasonable data-security measures"). Indeed, the FTC even points to language that "warns explicitly that 'the Federal Trade Commission Act may require you to provide reasonable security' of the types described within [the brochure]." *Id.* But if the FTC is correct that the brochure "describe[s]" the data-security practices that

Section 5 "require[s]," *id.*, then the FTC has jumped from the fair-notice frying pan into the administrative-law fire.

Agency documents "designed to implement, interpret, or prescribe law" are considered to be "rules" under the Administrative Procedure Act. 5 U.S.C. § 551(4); *accord Chamber of Commerce v. United States Dep't of Labor*, 174 F.3d 206, 211-12 (D.C. Cir. 1999) (describing a rule as an agency pronouncement that "has a substantial impact upon private parties and puts a stamp of agency approval or disapproval on a given type of behavior") (internal quotation omitted). And "rules which define with specificity acts or practices which are unfair or deceptive acts or practices" can be promulgated by the FTC only pursuant to the procedural requirements of Section 18(b) of the FTC Act. 15 U.S.C. § 57a(a)-(b). Thus, if the FTC is correct that the brochure describes the data-security practices that Section 5 "require[s]," FTC Br. 51, the brochure is invalid as an improperly promulgated rule. *See, e.g.*, *Ford Motor Co. v. FTC*, 673 F.2d 1008, 1009-10 (9th Cir. 1981) (vacating FTC order as improperly promulgated rule); *see also NRDC v. EPA*, 643 F.3d 311, 320-21 (D.C. Cir. 2011) (vacating EPA "guidance document" as

improperly promulgated rule); *Chamber of Commerce*, 174 F.3d at 213 (vacating OSHA "directive" as improperly promulgated rule).

Even if the brochure were relevant to the fair-notice analysis, the FTC greatly overstates its relevance. The FTC has repeatedly described the brochure as "a guide to help small and medium-sized businesses," *see, e.g.*, FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, 2010 WL 4918697, at *11 & n.33 (Dec. 2010), thus making its relevance to a large company like Wyndham questionable at best. In any event, the brochure is rarely updated to reflect current data-security realities, with the most-recent version having been issued over *three years* ago—a lifetime in this context. *See* Wyndham Br. 43-44.

III. The FTC Has Not Pleaded Sufficient Facts To State A Plausible Claim Of Substantial, Unavoidable Consumer Injury.

Finally, the FTC argues that it has pleaded sufficient facts to state a plausible claim that consumers suffered "substantial" and "[un]avoidable" injury from the cyberattacks. *See* FTC Br. 52-61. Again, the Commission is wrong. The Commission insists that a court can "infer[]" that some consumers must have sustained "unreimbursed

charges" notwithstanding the undisputed regime preventing such charges. FTC Br. 53. But such unvarnished speculation fails the "plausibility" pleading standard. *See, e.g.*, *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Indeed, the FTC recently admitted in discovery (which has since been stayed) that—after having investigated the cyberattacks against Wyndham for nearly five years—it has failed to identify a *single* individual consumer who suffered unreimbursed financial loss. *See* FTC Br. 57; *see also* Pl.'s Resps. to Defs.' Fourth Set of Requests for Admission (10/15/14), at 6-8 (attached as an addendum to this brief).[6]

The FTC insists, however, that this Court is obliged to turn a blind eye to the laws and policies that protect consumers from unreimbursed payment-card fraud because they fall "outside the four corners of the complaint." FTC Br. 54. But such an attempt to hide behind pleading rules no longer works in light of *Iqbal* and *Twombly*. A

[6] In its opening brief, Wyndham referred to a potential unreimbursed fraud loss of $1.25. *See* Wyndham Br. 50. The FTC subsequently disclaimed reliance on any such loss, admitting that, as of October 15, 2014, it had identified *no* single individual consumer who had suffered *any* unreimbursed fraud loss. *See* Pl.'s Resps. to Defs.' Fourth Set of Requests for Admission (10/15/14), at 6-8 (attached as an addendum to this brief).

litigant cannot "nudge[] [its] claims across the line from conceivable to plausible," *Twombly*, 550 U.S. at 570, by asking a court to bury its head in the sand. Courts do not "assess the plausibility of an inference in a vacuum," and the the "existence of obvious alternative[s]" to the FTC allegations of "unreimbursed charges"—*i.e.*, that consumers were in fact reimbursed as required by federal law and card-brand policies—"simply illustrates the unreasonableness of the inference sought and the implausibility of the claims made." *16630 Southfield Ltd. P'ship v. Flagstar Bank, F.S.B.*, 727 F.3d 502, 505 (6th Cir. 2013).

The FTC speculates that some consumers "*might* not have detected the fraudulent charges" or "*might* not have undertaken the effort and expense of seeking a refund." FTC Br. 55 (emphasis added). But such speculation, unsupported by any specific facts, is precisely what *Iqbal* and *Twombly* prohibit. And even if such consumers did in fact exist (notwithstanding the FTC's inability to locate them over the past five years), any financial harm stemming from those failures could have been "reasonably avoid[ed]" by simply calling a payment-card issuer and having the fraudulent charges reversed. 15 U.S.C. § 45(n); *see also Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1168-69 (9th

Cir. 2012) (holding that credit card annual fee was reasonably avoidable because it "was completely refundable if [plaintiff] closed his account within 90 days").

The FTC fares no better by citing cases "reject[ing] the proposition that a guarantee of … [a] refund prevents injury." FTC Br. 55 (omission and alteration in original; internal quotation omitted). Those cases all involved defendants who argued that any harm from their allegedly fraudulent conduct was avoidable because *they* made "offers of full refunds to dissatisfied consumers." *Id.* Obviously a defendant's attempts to use its own "largely illusory money-back offer" to avoid liability for selling bogus products, *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1103 (9th Cir. 1994), says nothing at all about whether consumers can "reasonably avoid" injury from a cybersecurity breach merely by contacting their payment-card issuers.

Unable to plausibly show that consumers suffered substantial, unavoidable financial injury as a result of the cyberattacks, the FTC resorts to arguing that the "time, expense, and effort spent by consumers to mitigate injuries constitutes substantial injury under Section 5(n)." FTC Br. 60. That is wrong. Again, the FTC can act

under Section 5 only when the harm is not "reasonably avoidable by consumers themselves." 15 U.S.C. § 45(n). And in determining whether harm is "reasonably avoidable," "[t]he question … is not whether subsequent mitigation was convenient or costless, but whether it was reasonably possible." *Davis*, 691 F.3d at 1169 (internal quotation omitted). By its terms, therefore, Section 5(n) recognizes that consumers may incur "reasonable" costs in mitigating injury and that such costs do not trigger the FTC Act. By trying to characterize the steps necessary to *avoid* injury as themselves imposing a "substantial" injury, the FTC is trying to write the "avoidable" requirement out of the statute.

Moreover, both Congress and the FTC have recognized that "substantial" injury requires something more than the attenuated mitigation costs—including the "opportunity costs" of "wasted time"[7]—

[7] The FTC argues that, even if consumers were reimbursed for all fraudulent charges, they still suffered "unavoidabl[e] lost access to funds or credit." FTC Br. 57 (internal quotation omitted). Properly understood, this contention is nothing more than an extension of the FTC's argument that consumers suffered "opportunity costs" from dealing with payment-card fraud. The FTC has not alleged any facts showing that any consumers suffered *actual* (as opposed to *potential*) harm from any short-term inability to access certain funds or credit temporarily held up by fraudulent transactions.

on which the FTC relies here. FTC Br. 58. As the Senate Report accompanying Section 5(n) explains, "substantial injury is not intended to encompass merely trivial or speculative harm," but "[i]n most cases … involve[s] monetary or economic harm or unwarranted health and safety risks." S. Rep. No. 103-130, at 13 (1993); *accord FTC Policy Statement on Unfairness* (Dec. 17, 1980). And courts in data-security cases have rejected such attenuated and speculative harms as not constituting sufficient consumer injury—even in cases that do not apply the heighted "substantial injury" bar to which the FTC is subject. *See, e.g.*, *Remijas v. Neiman Marcus Grp., LLC*, No. 14 C 1735, 2014 WL 4627893, at *4 (N.D. Ill. Sept. 16, 2014); *Clark v. Experian Info. Solutions, Inc.*, No. 03 C 7882, 2006 WL 2224049, at *3 (N.D. Ill. Aug. 2, 2006), *aff'd*, 256 F. App'x 818 (7th Cir. 2007).

None of the cases on which the FTC relies conclude otherwise. The Ninth Circuit's decision in *Neovi* involved fraudulent checks, *see* 604 F.3d at 1154, which are not subject to the same federal laws and bank policies as payment cards, *see* 15 U.S.C. § 1693a(7) (excluding from the Electronic Funds Transfer Act any transaction "originated by check, draft, or similar paper instrument"). *Neovi* was also decided

before the Ninth Circuit squarely addressed the question of what constitutes "reasonably avoidable" injury in *Davis*. *See Davis*, 691 F.3d at 1169 (explaining that, in determining whether harm is "reasonably avoidable," "[t]he question … is not whether subsequent mitigation was convenient or costless, but whether it was 'reasonably possible.'"). And the Tenth Circuit's decision in *FTC v. Accusearch Inc.* proves nothing because it did not even address the injury question. *See* 570 F.3d 1187, 1194 (10th Cir. 2009) ("On appeal Accusearch does not challenge the analysis of the unfair-practice elements."); *see also United States v. L.A. Tucker Truck Lines, Inc.*, 344 U.S. 33, 37-38 (1952) (issue not "raised in briefs or argument nor discussed in the opinion of the Court" is "not a binding precedent").

CONCLUSION

For the foregoing reasons, this Court should reverse the order denying Wyndham's motion to dismiss Count II of the FTC's amended complaint, and direct the district court to grant that motion.

December 8, 2014

Respectfully submitted,

/s/ *Eugene F. Assaf*

Eugene F. Assaf, P.C.
(DC Bar No. 449778)
Christopher Landau, P.C.
Susan M. Davies
K. Winn Allen
Ronald K. Anguas, Jr.
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, DC 20005
(202) 879-5000

Michael W. McConnell
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, DC 20005
(202) 879-5000

Douglas H. Meal
David T. Cohen
ROPES & GRAY LLP
800 Boylston Street
Boston, MA 02199
(617) 951-7000

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

Counsel for Appellant Wyndham Hotels & Resorts, LLC

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

I. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because the brief contains 6,994 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

II. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010, in 14-point Century Schoolbook.

December 8, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

CERTIFICATE OF IDENTICAL COMPLIANCE OF BRIEFS

I, Eugene F. Assaf, P.C., hereby certify that the text of the electronically filed brief is identical to the text of the original copies that were dispatched on December 8, 2014, by Federal Express Overnight delivery to the Clerk of the Court of the United States Court of Appeals for the Third Circuit.

December 8, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

CERTIFICATE OF PERFORMANCE OF VIRUS CHECK

I, Eugene F. Assaf, P.C., hereby certify that on December 8, 2014, I caused a virus check to be performed on the electronically filed copy of this brief using the following virus software: Microsoft Forefront Endpoint Protection, version 4.2.223.0. No virus was detected.

December 8, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

CERTIFICATE OF SERVICE

I, Eugene F. Assaf, P.C., hereby certify that on December 8, 2014, I caused seven (7) copies of Appellant's Reply Brief to be dispatched by Federal Express Overnight delivery to the Clerk of the Court for the United States Court of Appeals for the Third Circuit, and filed an electronic copy of the brief via CM/ECF. I also caused a copy of this brief to be served electronically on the following counsel for Appellee:

Joel R. Marcus-Kurn, Esq. (*jmarcuskurn@ftc.gov*)
David C. Shonka, Esq. (*dshonka@ftc.gov*)
David Sieradzki, Esq. (*dsieradzki@ftc.gov*)
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Mail Stop H-584
Washington, DC 20580

December 8, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

ATTACHMENT

PLAINTIFF'S RESPONSES AND OBJECTIONS
TO DEFENDANTS' FOURTH SET OF
REQUESTS FOR ADMISSION

Lisa Weintraub Schifferle (DC Bar No. 463928)
Kristin Krause Cohen (DC Bar No. 485946)
Kevin H. Moriarty (DC Bar No. 975904)
Katherine E. McCarron (DC Bar No. 486335)
John A. Krebs (MA Bar No. 633535)
Andrea V. Arias (DC Bar No. 1004270)
Allison M. Lefrak (DC Bar No. 485650)
James A. Trilling (DC Bar No. 467273)
Katherine R. White (VA Bar No. 68779)
Jacqueline K. Connor (NY Reg. No. 5208400)
Federal Trade Commission
600 Pennsylvania Ave., NW Mail Stop CC-8232
Washington, D.C. 20580
Telephone: (202) 326-2804
lschifferle@ftc.gov
kcohen@ftc.gov
kmoriarty@ftc.gov
kmccarron@ftc.gov
jkrebs@ftc.gov
aarias@ftc.gov
alefrak@ftc.gov
jtrilling@ftc.gov
kwhite@ftc.gov
jconnor@ftc.gov

Attorneys for Plaintiff Federal Trade Commission

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

Federal Trade Commission, Plaintiff, v. Wyndham Worldwide Corporation, *et al.*, Defendants.	Case No. 2:13-CV-01887-ES-JAD **PLAINTIFF'S RESPONSES AND OBJECTIONS TO DEFENDANTS' FOURTH SET OF REQUESTS FOR ADMISSION**

Plaintiff, Federal Trade Commission ("FTC," "Commission," or "Plaintiff"), pursuant to Federal Rules of Civil Procedure 26 and 36, and Local Rule 36.1, makes the following objections and provides the following responses to the Fourth Set of Requests to the Federal Trade Commission ("Requests for Admission") served by Wyndham Worldwide Corporation ("Wyndham Worldwide"), Wyndham Hotel Group, LLC ("Hotel Group"), Wyndham Hotels and Resorts, LLC ("Hotels and Resorts"), and Wyndham Hotel Management (collectively, "Wyndham" or "Defendants").

I. General Statements

1. The FTC states that these responses are its governmental response, pursuant to Federal Rule of Civil Procedure 33(b)(l)(B). Information necessary to prepare these responses has been supplied from a number of sources and these responses have been verified on the FTC's behalf by authorized representatives.

2. To the extent required by Rule 26(e) of the Federal Rules of Civil Procedure, the FTC will supplement its responses to the Requests for Admission. The FTC reserves the right to supplement, revise, modify, or otherwise change or amend its responses to the Requests for Admission in light of any documents that it subsequently may obtain or discover. Because discovery is ongoing, the FTC's responses should not be construed to limit the FTC's basis for any relief sought from Defendants in this action. Therefore, the FTC's responses to the Requests for Admission represent the FTC's present knowledge based on its investigation, information, and preparation to date.

3. By responding to the Requests for Admission, the FTC does not waive or intend to waive, but rather reserves and intends to reserve: (a) any objections to the

competency, relevance, materiality, privilege, or admissibility as evidence, for any purpose, of any information produced in response to the Requests for Admission; and (b) the right to object on any Requests for Admission.

4. The FTC's responses are based upon the discovery it has received to date. The FTC notes that discovery is ongoing. Accordingly, the FTC expressly reserves its right to supplement, revise, modify, or otherwise change or amend its responses to the Requests for Admission based on any new facts obtained through further investigation and discovery.

II. General Objections

1. The FTC objects to the Requests for Admission to the extent that the Definitions attempt to impose upon the FTC obligations greater than those required by the Federal Rules of Civil Procedure and/or the applicable Local Rules.

2. The FTC objects to the Requests for Admission to the extent that they call for identification of documents or information protected from disclosure by the attorney-client privilege, the attorney work product doctrine, the governmental deliberative process privilege, the law enforcement evidentiary or investigatory files privilege, the Speech or Debate Clause privilege, the common interest rule, or any other applicable privilege of law. The FTC does not intend to waive any of the privileges asserted in this objection by any inadvertent reference to, or production of, protected documents or information that may occur, and reserves the right to seek the return of any such material inadvertently produced to Defendants. The documents and information for which the FTC asserts these privileges include but are not limited to: (1) correspondence between

the FTC and law enforcement agencies; (2) notes of telephone conversations between the FTC and law enforcement agencies; (3) drafts of pleadings; (4) internal documents circulated among FTC staff; (5) memoranda from FTC staff to any of the Commissioners; (6) communications and other correspondence between FTC attorneys and among FTC staff, except to the extent such staff have submitted declarations in this lawsuit and/or will be testifying witnesses and the correspondence or communication relates to the particular subject(s) addressed in their declaration and/or testimony; (7) other notes and documents prepared for or in anticipation of litigation by FTC staff; and (8) communications with Members of Congress or their aides.

3. The FTC objects to the Requests for Admission to the extent that they seek information that is not relevant to any party's claim or defense or is not reasonably calculated to lead to the discovery of admissible evidence.

4. The FTC objects to the Requests for Admission to the extent that they are vague, ambiguous, overbroad, or unduly burdensome.

5. The FTC objects to the Requests for Admission to the extent they seek to require the FTC to admit any Request based on information that is not within the FTC's possession, custody, or control.

6. The FTC objects to the Requests for Admission to the extent that they require the FTC to undertake legal research for Defendants.

7. The FTC objects to the Requests for Admission to the extent that they require the FTC to analyze or organize factual evidence for Defendants.

8. The FTC objects to the Requests for Admission to the extent that they seek information that the FTC has already provided to Defendants.

9. The FTC objects to the Requests for Admission to the extent that they define "Plaintiff or FTC" and "you or your" to include consultants and/or "persons purporting to act on behalf" of the agency.

10. Each of the above-listed General Objections is incorporated hereby reference to each specific answer and objection set forth below. The specific answers and objections set forth below are made without waiving any of the above-listed General Responses and General Objections.

III. Specific Responses and Objections

REQUEST FOR ADMISSION NO. 48:

At the time the FTC filed its initial complaint in this case, the FTC had not identified a consumer who was not reimbursed by their credit- or debit-card issuer for all fraudulent charges arising out of the Cyberattacks that the consumer reported to the credit- or debit-card issuer.

RESPONSE TO REQUEST FOR ADMISSION NO. 48:

The FTC objects to this Request on the grounds that it is vague and ambiguous as to the meaning of the phrase "identified a consumer." The FTC objects to this request to the extent it seeks information that is protected from disclosure by the attorney work product doctrine. The FTC further objects to this Request to the extent that it seeks information that is not within the possession, custody or control of the FTC, namely

whether a specific consumer suffered unreimbursed fraud loss arising out of the Cyberattacks which the consumer did not report to their credit- or debit-card issuer.

Subject to and without waiving these objections and the General Objections, Request for Admission No. 48 is admitted to the extent that the phrase "identified a consumer" means specific individual consumers. Subject to and without waiving these objections and the General Objections, Request for Admission No. 48 is denied to the extent that surveys of identity theft victims reveal that a certain percentage of consumers who suffer fraud on their existing payment card accounts suffer direct out-of-pocket loss, including unreimbursed fraudulent charges.

REQUEST FOR ADMISSION NO. 49:

At the time the FTC filed its amended complaint in this case, the FTC had not identified a consumer who was not reimbursed by their credit- or debit-card issuer for all fraudulent charges arising out of the Cyberattacks that the consumer reported to the credit- or debit-card issuer.

RESPONSE TO REQUEST FOR ADMISSION NO. 49:

The FTC objects to this Request on the grounds that it is vague and ambiguous as to the meaning of the phrase "identified a consumer." The FTC objects to this request to the extent it seeks information that is protected from disclosure by the attorney work product doctrine. The FTC further objects to this Request to the extent that it seeks information that is not within the possession, custody or control of the FTC, namely whether a specific consumer suffered unreimbursed fraud loss arising out of the Cyberattacks which the consumer did not report to their credit- or debit-card issuer.

Subject to and without waiving these objections and the General Objections, Request for Admission No. 49 is admitted to the extent that the phrase "identified a consumer" means specific individual consumers. Subject to and without waiving these objections and the General Objections, Request for Admission No. 49 is denied to the extent that surveys of identity theft victims reveal that a certain percentage of consumers who suffer fraud on their existing payment card accounts suffer direct out-of-pocket loss, including unreimbursed fraudulent charges.

REQUEST FOR ADMISSION NO. 50:

On November 7, 2013, when oral argument was held in this case, the FTC had not identified a consumer who was not reimbursed by their credit- or debit-card issuer for all fraudulent charges arising out of the Cyberattacks that the consumer reported to the credit- or debit-card issuer.

RESPONSE TO REQUEST FOR ADMISSION NO. 50:

The FTC objects to this Request on the grounds that it is vague and ambiguous as to the meaning of the phrase "identified a consumer." The FTC objects to this request to the extent it seeks information that is protected from disclosure by the attorney work product doctrine. The FTC further objects to this Request to the extent that it seeks information that is not within the possession, custody or control of the FTC, namely whether a specific consumer suffered unreimbursed fraud loss arising out of the Cyberattacks which the consumer did not report to their credit- or debit-card issuer.

Subject to and without waiving these objections and the General Objections, Request for Admission No. 50 is admitted to the extent that the phrase "identified a

consumer" means specific individual consumers. Subject to and without waiving these objections and the General Objections, Request for Admission No. 50 is denied to the extent that surveys of identity theft victims reveal that a certain percentage of consumers who suffer fraud on their existing payment card accounts suffer direct out-of-pocket loss, including unreimbursed fraudulent charges.

REQUEST FOR ADMISSION NO. 51:

To date, the FTC has not identified a consumer who was not reimbursed by their credit- or debit-card issuer for all fraudulent charges arising out of the Cyberattacks that the consumer reported to the credit- or debit-card issuer.

RESPONSE TO REQUEST FOR ADMISSION NO. 51:

The FTC objects to this Request on the grounds that it is vague and ambiguous as to the meaning of the phrase "identified a consumer." The FTC objects to this request to the extent it seeks information that is protected from disclosure by the attorney work product doctrine. The FTC further objects to this Request to the extent that it seeks information that is not within the possession, custody or control of the FTC, namely whether a specific consumer suffered unreimbursed fraud loss arising out of the Cyberattacks which the consumer did not report to their credit- or debit-card issuer.

Subject to and without waiving these objections and the General Objections, Request for Admission No. 51 is admitted to the extent that the phrase "identified a consumer" means specific individual consumers. Subject to and without waiving these objections and the General Objections, Request for Admission No. 51 is denied to the extent that surveys of identity theft victims reveal that a certain percentage of consumers

who suffer fraud on their existing payment card accounts suffer direct out-of-pocket loss, including unreimbursed fraudulent charges.

REQUEST FOR ADMISSION NO. 52:

Of those consumers with whom the FTC has communicated regarding the Cyberattacks, any consumers who were not reimbursed by their credit- or debit-card issuers for all fraudulent charges arising out of the Cyberattacks were not reimbursed because they failed to communicate the fraudulent nature of the unreimbursed charges to their credit- or debit-card issuer.

RESPONSE TO REQUEST FOR ADMISSION NO. 52:

The FTC objects to this Request to the extent that it seeks information that is not within the possession, custody or control of the FTC, namely whether a consumer suffered unreimbursed fraud loss arising out of the Cyberattacks which the consumer did not communicate to their credit- or debit-card issuer. The FTC further objects to this request to the extent it seeks information that is protected from disclosure by the attorney work product doctrine.

Subject to and without waiving these objections and the General Objections, the FTC, after reasonable inquiry, lacks sufficient information to admit or deny Request for Admission No. 52.

REQUEST FOR ADMISSION NO. 53:

The $10.6 million fraud loss alleged in paragraph 40 of the First Amended Complaint includes losses to issuing banks, credit- and debit-card brands, and merchants who accept credit and debit cards.

RESPONSE TO REQUEST FOR ADMISSION NO. 53:

Subject to and without waiving the General Objections, the FTC lacks sufficient information to admit or deny Request for Admission No. 53. The basis for the $10.6 million fraud loss alleged in paragraph 40 of the First Amended Complaint is a document the FTC received from VISA, WHR-FTC1 000009996-000010005. The document does not specify whether the $10.6 million fraud loss includes losses to issuing banks, credit- and debit-card brands, and merchants who accept credit and debit cards.

REQUEST FOR ADMISSION NO. 54:

The $10.6 million fraud loss alleged in paragraph 40 of the First Amended Complaint includes amounts other than unreimbursed fraudulent charges to consumers.

RESPONSE TO REQUEST FOR ADMISSION NO. 54:

Subject to and without waiving the General Objections, Request for Admission No. 54 is admitted.

REQUEST FOR ADMISSION NO. 55:

Fraudulent charges that were reversed or refunded by a consumer's credit- or debit-card issuer do not constitute substantial injury to consumers which is not reasonably avoidable by consumers themselves.

RESPONSE TO REQUEST FOR ADMISSION NO. 55:

The FTC maintains that every consumer whose payment card was compromised as a result of Defendants' violations of the FTC Act suffered injury. Such injury includes but is not limited to: increased costs, and loss of access to funds, credit, cash-back, reward points, and other loyalty benefit programs. Consumers also expended time and

money resolving fraudulent charges and mitigating subsequent harm. Such injury to a large number of people constitutes substantial harm under the FTC Act.

Subject to and without waiving the General Objections, and to the extent further response is required, Request for Admission No. 55 is denied.

REQUEST FOR ADMISSION NO. 56:

Time expended by consumers modifying recurring- or automated-payment information with merchants does not constitute substantial injury to consumers which is not reasonably avoidable by consumers themselves.

RESPONSE TO REQUEST FOR ADMISSION NO. 56:

The FTC maintains that every consumer whose payment card was compromised as a result of Defendants' violations of the FTC Act suffered injury. Such injury includes but is not limited to: increased costs, and loss of access to funds, credit, cash-back, reward points, and other loyalty benefit programs. Consumers also expended time and money resolving fraudulent charges and mitigating subsequent harm. Such injury to a large number of people constitutes substantial harm under the FTC Act.

Subject to and without waiving the General Objections, and to the extent further response is required, Request for Admission No. 56 is denied.

REQUEST FOR ADMISSION NO. 57:

Postage costs incurred by consumers in connection with the Cyberattacks do not constitute substantial injury to consumers which is not reasonably avoidable by consumers themselves.

RESPONSE TO REQUEST FOR ADMISSION NO. 57:

The FTC maintains that every consumer whose payment card was compromised as a result of Defendants' violations of the FTC Act suffered injury. Such injury includes but is not limited to: increased costs, and loss of access to funds, credit, cash-back, reward points, and other loyalty benefit programs. Consumers also expended time and money resolving fraudulent charges and mitigating subsequent harm. Such injury to a large number of people constitutes substantial harm under the FTC Act.

Subject to and without waiving the General Objections, and to the extent further response is required, Request for Admission No. 57 is denied.

Dated this 15th day of October, 2014.

/s/ Allison M. Lefrak
Kristin Krause Cohen
Lisa Weintraub Schifferle
Kevin H. Moriarty
Katherine E. McCarron
John A. Krebs
Andrea V. Arias
Allison M. Lefrak
James A. Trilling
Katherine R. White
Jacqueline K. Connor

Federal Trade Commission
600 Pennsylvania Ave., NW Mail Stop CC-8232
Washington, D.C. 20580

Attorneys for Plaintiff Federal Trade Commission

CERTIFICATE OF SERVICE

I hereby certify that on October 15, 2014, I served the attached document via electronic mail to all Counsel of Record for Defendants.

/s/ Allison M. Lefrak
Allison M. Lefrak