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)
Jonathan E. Zimmerman (MA Bar No. 654255)
Andrea V. Arias (DC Bar No. 1004270)
Federal Trade Commission
600 Pennsylvania Ave., NW Mail Stop NJ-8100
Washington, D.C. 20580
Telephone: (202) 326-2276
Fax: (202) 326-3062
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.	CIVIL ACTION NO. 2:13-CV-01887-ES-SCM **PLAINTIFF'S RESPONSE IN OPPOSITION TO THE MOTION TO DISMISS BY DEFENDANT WYNDHAM HOTELS & RESORTS LLC** **MOTION DATE JUNE 17, 2013**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Regulations

INTRODUCTION

Wyndham Hotels and Resorts, LLC ("Hotels and Resorts"), Wyndham Worldwide Corporation ("Wyndham Worldwide"), Wyndham Hotel Group, LLC ("Hotel Group"), and Wyndham Hotel Management, Inc. ("Hotel Management") (collectively, "Wyndham" or "Defendants") failed to implement reasonable data security measures to protect the payment card information of their customers. As a result of Wyndham's failures, cyber criminals were able to penetrate their network three times over a two-year period, steal the payment card information of hundreds of thousands of Wyndham customers, and place fraudulent charges on those customers' accounts, generating more than $10.6 million in fraud loss.

The Federal Trade Commission ("FTC") brought this equitable action under Section 5 of the FTC Act, 15 U.S.C. § 45, alleging that Wyndham engaged in deceptive and unfair practices relating to data security and seeking a permanent injunction to prevent further consumer injury from those practices. Wyndham now asks this Court to be the first to hold that the FTC lacks the authority under the FTC Act to protect consumers from this type of injury. Motion to Dismiss by Defendant Wyndham Hotels & Resorts, ECF No. 91-1 ("Wyndham Mot."). Wyndham's arguments rest on a tortured reading of the statute and a rejection of seventy-five years of enforcement.

The FTC Act prohibits "unfair or deceptive acts or practices." 15 U.S.C. § 45(a)(1). The FTC's two-count complaint alleges that (1) Defendants engaged in "deceptive" practices by misrepresenting that they took "commercially reasonable efforts" to secure customers' payment card data; and (2) Defendants' engaged in "unfair" practices because their lax security measures failed to adequately protect this payment card data. First Amended Complaint for Injunctive and Other Equitable Relief ("Complaint") ¶¶ 44-49, ECF No. 28. The Complaint pleads specific facts that, if proven, would establish that Wyndham is liable on both counts. This should end the

inquiry.

Wyndham abandons any pretense of meeting the 12(b)(6) standard in its motion to dismiss. Instead, Wyndham recasts questions of fact as questions of law, and challenges the FTC's long-established authority under the FTC Act to protect consumers' data from identity theft and other harms as a result of unreasonable data security. Defendants' baseless legal challenge to the "unfairness" portion of the FTC Act inexplicably reads a data security exception into the statute, suggesting that the FTC can enforce the Act against unfair or deceptive acts or practices, but not against unfair practices relating to data security.

Defendants also suggest that the FTC's broad consumer protection mandate—which has been part of the FTC Act since 1914—is unconstitutionally vague because it fails to provide fair notice. This premise undercuts the very purpose of this long-standing statute, which was designed to permit the FTC to protect consumers from unanticipated, unenumerated threats. Moreover, the FTC has prudently pursued its mandate to protect consumers from unfair data security, providing guidance to companies through public statements and nineteen separate enforcement actions on this issue. Indeed, numerous courts have upheld federal agencies' ability to seek equitable relief in court, based on violations of laws that provide far less guidance than the FTC Act and subsequent Commission enforcement actions have provided. Wyndham's arguments lack merit and should be rejected by the Court.

LEGAL STANDARD

Wyndham's motion to dismiss is brought pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. Fed. R. Civ. P. 12(b)(6). To survive such a motion, the plaintiff need only allege facts sufficient to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 570 (2007)). Facial plausibility is established where the plaintiff "pleads factual content that allows the court to draw

the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. In reviewing a Rule 12(b)(6) motion to dismiss for failure to state a claim, courts "'accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief.'" *Phillips v. Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008) (quoting *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 374 n.7 (3d Cir. 2002)). Under this standard, the Complaint states a claim for relief and Wyndham's motion to dismiss must be denied.

ARGUMENT

Section 5 of the FTC Act prohibits unfair or deceptive practices. The FTC pleads sufficient facts in the Complaint to state a plausible claim that Defendants engaged in unfair and deceptive practices as a result of their failure to maintain reasonable data security and their misrepresentations to consumers about the quality of their data security.

I. THE COMPLAINT SATISFIES THE PLEADING STANDARD FOR UNFAIR ACTS OR PRACTICES.

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). To state a claim for unfair practices under Section 5 of the FTC Act, the FTC must plead (1) that an act or practice caused or is likely to cause substantial injury to consumers, (2) that the injury was not reasonably avoidable by consumers, and (3) that the injury was not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n); *FTC v. NHS Sys., Inc.*, No. 08-2215, 2013 WL 1285424, at *5 (E.D. Pa. Mar. 28, 2013). "[T]he consumer injury test is the most precise definition of unfairness articulated by either the Commission or Congress." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985) (rejecting argument that "the FTC has no authority to proscribe the 'kinds' of practices or prevent the 'kinds' of consumer injury at issue in this case").

Applying unfairness to data security practices, the FTC first pleads that Wyndham's practices were unreasonable—that is, that there were no countervailing benefits to Wyndham's failure to address its data security failures. Second, the FTC pleads that substantial injury resulted from Wyndham's unreasonable data security practices. Third, the FTC pleads that this injury was not reasonably avoidable by consumers. Finally, the FTC pleads that Wyndham's unreasonable data security caused this substantial injury to consumers.

A. The FTC Pleads All Elements of Section 5 Unfair Practices.

Wyndham engaged in unreasonable data security practices. Wyndham repeatedly and inaccurately claims that the FTC's Complaint fails to provide any specificity about the nature of Wyndham's data security failures. Wyndham Mot. 4, 22, 27. These claims are baseless. In fact, the Complaint alleges with specificity that Wyndham: failed to limit access among different computer networks through the use of readily available measures, such as firewalls (Compl. at ¶ 24(a)); permitted improperly-configured software, resulting in the storage of payment card information in clear text (*id*. at ¶ 24(b)); failed to ensure the Wyndham-branded hotels had adequate information security policies in place prior to allowing them to access Wyndham's computer network (*id*. at ¶ 24(c)); failed to require servers attached to its networks to have the latest security patches from manufacturers (*id*. at ¶ 24(d)); permitted servers on its network with commonly-known default user IDs and passwords (*id*. at ¶ 24(e)); failed to follow best practices for password complexity (*id*. at ¶ 24(f)); failed to inventory the computers on its network in order to permit Wyndham to identify the origin of intrusion efforts (*id*. at ¶ 24(g)); failed to employ reasonable measures to detect and prevent unauthorized access (*id*. at ¶ 24(h)); failed to follow proper procedures to prevent repeated intrusions (*id*. at ¶ 24(i)); and failed to restrict third-party access to its network (*id*. at ¶ 24(j)).

Wyndham could have avoided or remedied these unreasonable data security practices

through readily available, low-cost measures. Because there are few, if any, benefits to unreasonable data security practices, especially when the remedies are low- or no-cost, there are no countervailing benefits to Wyndham's practices.[1] Regardless, the existence of countervailing benefits of inadequate data security is a question of fact and inappropriate for a motion to dismiss. *See, e.g.*, *NHS Sys.*, 2013 WL 1285424, at *6 (finding no countervailing benefits at summary judgment stage).

Consumers were injured by Wyndham's unfair data security practices. The Complaint alleges that:

> Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.

Compl. ¶ 40. Accepting these well-pleaded allegations as true, and in a light most favorable to the Plaintiff, the FTC alleges consumer injury sufficient to support a claim of unfairness. As discussed further below, Wyndham's contention that consumers were not actually injured in these ways is a classic factual dispute, and not a proper inquiry for a motion to dismiss.

The injury was not reasonably avoidable. The Complaint alleges injury that consumers could not have reasonably avoided. Compl. ¶ 40; *id*. ¶ 48. Consumers could not take steps to avoid Wyndham's unreasonable data security because Wyndham falsely told consumers that it followed "industry standard practices." Compl. ¶ 21. Consumers also could not avoid the injuries resulting from Wyndham's unreasonable data security, including: Lack of access to credit resulting from frozen credit cards; lack of access to funds from frozen debit cards; costs associated with switching payment cards; and "time and money resolving fraudulent charges and

[1] Wyndham offers a different version of this analysis, arguing that the "standard of liability for failing to adequately protect [payment card] data" should be "high" because the risk of consumer injury is low. Wyndham Mot. 22. This misapprehends the pertinent balancing test, which weighs the risks of the practice against the benefits of the practice. 15 U.S.C. § 45(n).

mitigating subsequent harm." Compl. ¶ 40. Finally, and as discussed further below, Wyndham's belief that consumers can reasonably avoid payment card fraud is very much a disputed claim, and therefore not appropriate for a motion to dismiss. *FTC v. Inc21.com Corp.*, 745 F. Supp. 2d 975, 1004 (N.D. Cal. 2010) (finding, in telephone billing context, that "the FTC has met its burden of proving that these unauthorized charges were not reasonably avoidable by consumers."). *See also id*. ("This order declines to allow defendants to blame unsuspecting consumers for failing to detect and dispute unauthorized billing activity.").

Wyndham's unreasonable data security caused this substantial injury. Wyndham makes the astonishing claim that the Complaint does not plead causation. Wyndham Mot. 23. In order to make this argument, Wyndham willfully ignores the extensive description of how hackers were able to exploit specific failures of Wyndham's data security program in order to retrieve consumers' personal information. Compl. ¶¶ 24-39. For example, the Complaint alleges that Wyndham "failed to adequately inventory computers connected to the Hotels and Resorts' network so that Defendants could appropriately manage the devices on its network." Compl. ¶ 24(g). In the description of the first breach, the Complaint alleges that Wyndham was unable to determine that the account lockouts resulting from a brute force attack were coming from two computers on Hotels and Resorts' network because they "did not have an adequate inventory of the Wyndham-branded hotels' computers." *Id*. ¶ 27. In addition, the Complaint states a plausible claim that these breaches resulted in the injury pleaded above, given that these were the same payment cards that are alleged to have been used for at least $10.6 million in fraudulent charges. *Id*. ¶ 40. The Complaint sufficiently alleges that Wyndham's unreasonable data security practices cause these consumer injuries.

B. Wyndham's Remaining Injury Arguments Are Questions of Fact.

Wyndham and its amici raise numerous fact issues to argue that payment card fraud does

not rise to the level of injury necessary to satisfy the FTC Act. These arguments are an attempt by Wyndham to mischaracterize questions of fact as questions of law. As noted above, questions of how much time and money consumers lost, whether they were able to get reimbursed, and whether they could have reasonably avoided injury are all questions of fact to be decided at trial.

Wyndham's reliance on *Reilly v. Ceridian*, 664 F.3d 38 (3d Cir. 2011), in this regard is misplaced. In fact, *Reilly* and other recent Article III standing cases squarely support the FTC's injury argument in this matter. In *Reilly*, the Third Circuit found that plaintiffs did not suffer injury sufficient to confer standing in a case where their personal information was stolen, because "no misuse [was] alleged." *Id*. at 45. The Court suggested that if there had been any misuse, then there would be injury:

> Although Appellants have incurred expenses to monitor their accounts and "to protect their personal and financial information from imminent misuse and/or identity theft," App. 00021, they have not done so as a result of any *actual* injury (e.g. because their private information was misused or their identities stolen). Rather, they prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent. The claim that they incurred expenses in anticipation of future harm, therefore, is not sufficient to confer standing.

Id. at 46 (emphasis in original). This approach was ratified by the Supreme Court in *Clapper v. Amnesty International*, which noted that plaintiffs' "costly and burdensome" mitigation efforts are "fairly traceable" to the practice only if the anticipated injury is "certainly impending." 133 S. Ct. 1138, 1151 (2013). The clear implication of both *Reilly* and *Clapper* is that if misuse has occurred, as it has here, then mitigation efforts to prevent further harm constitute fairly traceable injury sufficient for Article III standing.

The First Circuit in *Anderson v. Hannaford Brothers Co.* holds expressly what *Reilly* and *Clapper* hold by implication. 659 F.3d 151, 164-65 (1st Cir. 2011). In *Hannaford*, the First Circuit found that plaintiffs' mitigation efforts to avoid credit card fraud were reasonable and

recoverable because there were fraudulent charges on their payment cards (even if reimbursed). *Id*. The court distinguished from cases where no unauthorized charges were made:

> These courts reasoned that in the absence of unauthorized charges as to the plaintiffs or those similarly situated, the plaintiffs there lacked a reasonable basis for fearing there would be unauthorized charges to their accounts as a result of the theft. That very reasoning suggests that these courts would reach a different result if the plaintiffs alleged that they had suffered fraudulent charges to their accounts.

Id. at 166. Furthermore, the Court explicitly rejected Hannaford's argument that the alleged "zero-liability" policies of the credit card companies is relevant to injury, especially at the motion to dismiss stage. *Id*. at 164 n.8.

In any event, Wyndham's (and its amici's) arguments fundamentally misrepresent the nature of consumer injuries when their payment card information is stolen. First, Wyndham's argument that consumers did not suffer injury because of caps on liability is quite dubious, if not flatly wrong. *See* Bureau of Justice Statistics, Victims of Identity Theft, 2008 (December 2010) (stating that 14% of victims of credit fraud suffered out-of-pocket financial loss and, of those, victims suffered an average loss of $988"), *available at* http://bjs.gov/content/pub/pdf/vit08.pdf. Second, federal law does not provide these same liability protections for debit cards. 12 C.F.R. § 205.6(b)(1)-(3) (2013) (establishing three tiers of potential liability, the last of which is unlimited liability). Third, Wyndham assumes that all fraudulent charges were reimbursed, which is a question of fact.

Finally, the FTC's well-pleaded claims allege injury other than unreimbursed fraud charges (Compl. ¶ 40), all of which are cognizable under the FTC Act. *See FTC v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010) ("[O]btaining reimbursement required a substantial investment of time, trouble, aggravation, and money. . . . Regardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable injuries that could not be fully mitigated." (internal quotation marks omitted)); *FTC v. Accusearch, Inc.*, 570 F.3d 1187,

1194 (10th Cir. 2009) (finding substantial injury from "emotional harm" and "costs in changing telephone providers"). And, in any event, the test is not substantial injury to any one consumer. As courts have noted, "An injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm." *Am. Fin. Servs. Ass'n*, 767 F.2d at 972 (quotation marks and citation omitted). *See also Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) ("As the Commission noted, although the actual injury to individual customers may be small on an annual basis, this does not mean that such injury is not 'substantial.'" (citation omitted)).

Wyndham compares itself to a "local furniture store" that was robbed, and protests that the FTC is re-victimizing it with this suit. Wyndham Mot. 21. A more accurate analogy would be that Wyndham was a local furniture store that left copies of its customers' credit and debit card information lying on the counter, failed to lock the doors of the store at night, and was shocked to find in the morning that someone had stolen the information. Unlike Wyndham's hypothetical furniture heist, Wyndham's role in this matter was primarily as a vehicle for the victimization of consumers. The FTC is not suing Wyndham for the fact that it was hacked, it is suing Wyndham for mishandling consumers' information such that hackers were able to steal it.

II. THE FTC HAS THE AUTHORITY TO ENFORCE THE FTC ACT AGAINST ENTITIES FOR UNFAIR PRACTICES RELATED TO DATA SECURITY.

As explained above in Part I, the Complaint satisfies the pleading standard for unfair practices. This should end the inquiry. Nonetheless, Wyndham navigates its motion into uncharted territory, arguing that this Court should carve out a data security exception to the FTC's well-established unfairness authority. Moreover, Wyndham claims that it lacked fair notice of the FTC's enforcement authority in this area, notwithstanding the abundance of governmental and non-governmental guidance about what constitutes reasonable data security.

A. Section 5 of the FTC Act Grants the FTC Authority Over Data Security.

Wyndham claims that applying unfairness to data security practices would be inconsistent with the statutory scheme. Wyndham Mot. 7-14. Wyndham does not dispute, however, that Section 5's prohibition of "unfair or deceptive acts or practices in or affecting commerce" should cover deceptive data security practices. Wyndham Mot. 2 ("[Hotels and Resorts] does not dispute that the FTC can bring enforcement actions against companies that make 'deceptive' statements to consumers."). Instead, Wyndham argues that this Court should read a limited, implicit exemption for data security into the middle of the words "unfair" and "deceptive," based on the Supreme Court's decision in *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000).

Wyndham's reliance on *Brown & Williamson* is misplaced. In *Brown & Williamson*, the Supreme Court reversed the FDA's assertion of authority over tobacco due to "extraordinary" circumstances: The FDA for decades had denied that it had such authority, and its assertion of the authority would result in statutory inconsistencies. 529 U.S. at 159; *id*. at 137. Neither of these factors is present here. Indeed, Wyndham contends that the circumstances here only "strongly suggest" that unfairness should not cover data security. Wyndham Mot. 8. Even if there were such a "strong suggestion"—which there is not—the facts here would fall well short of the "extraordinary" circumstances that led the Court to overturn the FDA's assertion of authority over tobacco. *Id*. at 159-60.

1. Data Security Statutes Do Not Limit FTC Authority Under the FTC Act.

First, Wyndham incorrectly argues that several statutes that provide the FTC with legal tools to address data security in specific contexts somehow "preclude" or "foreclose" an interpretation of the FTC Act to cover unfair and deceptive acts or practices related to data security. Wyndham Mot. 7-8. But Wyndham has not argued (nor could it) that there is a

contradiction that requires this Court to reconcile the FTC Act with complementary data security statutes. *Cf. Brown & Williamson*, 529 U.S. at 139 (finding FDA's interpretation to "plainly contradict congressional policy").

Congress deliberately delegated broad power to the FTC under Section 5 of the FTC Act to address unanticipated practices in a changing economy. *See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) ("Congress . . . explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply."). The legislative history of the FTC Act reflects Congress's concerns about attempting to enumerate specific acts and practices. *See* S. Rep. No. 63-597, at 13 (1914) ("there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others"); H.R. Rep. No. 63-1142, at 19 (1914) (Conf. Rep.) ("It is impossible to frame definitions which embrace all unfair practices."). Indeed, the statute also does not mention any of the established uses of its unfairness provision, including online check drafting and delivery (*see Neovi*, 604 F.3d 1150 (9th Cir. 2010); sale of telephone records (*see Accusearch*, 570 F.3d 1187 (10th Cir. 2009)); unilateral breach of contracts (*see Orkin Exterminating Co. v. FTC*, 849 F.2d 1354 (11th Cir. 1988)); telephone billing practices (*see FTC v. Verity Int'l*, 335 F. Supp. 2d 479, 498-99 (S.D.N.Y. 2004)); unsafe farm equipment (*see In the Matter of Int'l Harvester Co.*, 104 F.T.C. 949 (1984)); or many other practices affecting commerce, all of which courts routinely find to be subject to Section 5 of the FTC Act. The FTC's determination to enforce the FTC Act in these contexts—as well as in the data security context—is entitled to deference. *See Arlington v. FCC*, Nos. 11-1545, 11-1547, 2013 WL 2149789, slip op. at *16-17 (May 20, 2013).

The subsequent enactment of sector-specific laws to enhance regulatory authority over data security in particular industries neither contradicts nor is inconsistent with Congress's grant of broad authority to the FTC to prohibit deceptive and unfair practices that injure consumers. Instead, the sector-specific laws enhance FTC authority with new legal tools. For example, Congress provided the FTC with rulemaking and/or civil penalty authority through the enactment of the Fair Credit Reporting Act ("FCRA"), Gramm-Leach-Bliley Act ("GLB"), and Children's Online Privacy Protection Act ("COPPA"). Similarly, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") give the Department of Health and Human Services rulemaking and civil penalty authority. By contrast, the FTC is not seeking civil penalties in this matter; rather, the FTC is seeking only equitable relief. *See* Prayer for Relief, Compl.

These statutes and the FTC Act co-exist without contradiction or inconsistency. They are complementary, and by no means irreconcilable. *Cf. Brown & Williamson*, 529 U.S. at 143 (undertaking the "task of reconciling many laws enacted over time, and getting them to 'make sense' in combination." (citing *United States v. Fausto*, 484 U.S. 439, 453 (1988))).

Lastly, Wyndham does not, and cannot, argue that the scope of the FTC Act has been impliedly repealed. The courts will not infer a statutory repeal "unless the later statute 'expressly contradict[s] the original act'" or unless such a construction "is absolutely necessary ... in order that [the] words [of the later statute] shall have any meaning at all." *See Nat'l Ass'n of Home Builders v. Defenders of Wildlife*, 551 U.S. 644, 662-63 (2007). Wyndham has not met this standard.[2]

[2] Wyndham argues that because the FTC has sought additional data security legislation from Congress, it necessarily lacks authority under Section 5 to challenge data security practices as unfair. *See* Wyndham Mot. 11. Wyndham fails to appreciate that the FTC has sought legislation

2. The FTC Has Always Affirmed, and Never Disavowed, Authority Over Unfair Practices Related to Data Security.

Second, Wyndham argues that the FTC originally disclaimed authority to pursue unfair practices related to data security and that its position in this matter is a "quite recent[]" reversal. Wyndham Mot. 10-11. These claims are contrary to fact: Since 2000, the FTC has brought more than forty data security cases, nineteen of which alleged unfair practices. *See* Legal Resources | BCP Business Center, http://business.ftc.gov/legal-resources/29/35. The FTC has routinely reported and publicized its data security program, including these enforcement activities, to Congress, consumers, and industry. *See, e.g.*, *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing before the Subcomm. on Terrorism, Technology, and Homeland Security of the S. Comm. on the Judiciary*, 110th Cong. at 5-6 (March 21, 2007) (Prepared Statement of the Federal Trade Commission) ("[I]n several of the cases, the alleged security inadequacies led to breaches that caused substantial consumer injury and were challenged as unfair practices under the FTC Act.").[3]

Wyndham incorrectly asserts that the FTC disclaimed its authority in 2000 when it stated that it "lacks authority to require firms to adopt information practice policies." Wyndham Mot. 10 (quoting Federal Trade Commission, *Privacy Online: Fair Information Practices In The Electronic Marketplace* at 33-34 (May 2000) available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf ("Privacy Report")). Wyndham mischaracterizes the Privacy Report, which states only that FTC Act authority under Section 5 is limited to unfair or deceptive

---

to provide additional tools, such as civil penalties, to complement the authority it already has under Section 5.

[3] The FTC has reported to Congress more than thirty times since 2003 on its Section 5 enforcement activities related to data security. In at least a dozen instances, it has specifically stated that failure to maintain reasonable security is an unfair practice. *See, e.g.*, *Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the S. Comm. on the Judiciary*, 110th Cong. (March 21, 2007) (Prepared Statement of the Federal Trade Commission).

practices, and thus would not encompass failure to adopt certain policies absent unfair or deceptive practices. *Id*. The same Privacy Report explicitly states, in a section titled "Current FTC Authority," that "[t]he FTC Act prohibits unfair and deceptive practices in and affecting commerce. It authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain fair information practices." *Id*.

Wyndham also selectively quotes former FTC Chairman Pitofsky's 1998 testimony, omitting the fact that his testimony was expressly about online privacy, and not data security: "I appreciate this opportunity to present the Commission's recommendations for addressing the privacy concerns raised by the wide-spread collection of personal information from consumers by commercial sites on the World Wide Web." *Consumer Privacy on the World Wide Web, Hearing Before Subcomm. on Telecomm., Trade and Consumer Protection of the H. Comm. on Commerce*, 105th Cong. (July 21, 1998). Chairman Pitofsky described the problem of the widespread and rampant collection of information online, which, given technology and business practices at the time, had not risen to the level of "injury" necessary to invoke unfairness. Directly addressing that issue, he stated that the FTC is "limited *in this context* to ensuring that Web sites follow their stated information practices." *Id*. (emphasis added). *See also* Wyndham Mot. 10 (excising "in this context" from quote).

Finally, the testimony by former Bureau Director Vladeck does not disclaim authority, as Wyndham claims. Wyndham Mot. 11. Indeed, it ***showcases*** the authority:

> In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security procedures, or *where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury*.

The Threat of Data Theft to American Consumers: Hearing Before the Subcomm. on Commerce,

Manufacturing, and Trade of the H. Comm. on Energy & Commerce, 112th Cong. 2 (May 4, 2011) (emphasis added). Bureau Director Vladeck immediately followed this comment with a description of two cases, both of which alleged unfair data security practices. *Id*. at 2-4 (describing *In the Matter of Lookout Services, Inc.*, File No. 102 3076 (June 15, 2011); and *In the Matter of Ceridian Corp.*, FTC File No. 102 3160 (June 8, 2011).

Lastly, even if the FTC had originally disavowed its authority, which it did not, that fact would not be controlling. *See Smiley v. Citibank*, 517 U.S. 735, 742 (1996) ("[T]he mere fact that an agency interpretation contradicts a prior agency position is not fatal."). Unlike *Brown & Williamson*, where the FDA had a 70-plus year history of disavowing its authority (529 U.S. at 159), here Wyndham only can point to a few isolated statements, which it misinterprets, to claim disavowal.

3. Legislative and Executive Interest in Data Security Neither Impliedly Nor Explicitly Deprives the FTC of its FTC Act Authority over Unfair and Deceptive Data Security Practices.

Finally, Wyndham suggests that unenacted legislation, an executive order, and the "intense debate among members of Congress" somehow operate by inference to strip the FTC of its established authority over unfair practices pursuant to the FTC Act. Wyndham Mot. 12-13. Wyndham argues that congressional interest in data security, and its failed efforts to pass specific data security legislation, create the presumption that "'Congress could not have intended to delegate'" data security authority to the FTC under the FTC Act. Wyndham Mot. 13 (quoting *Brown & Williamson*, 529 U.S. at 160). This argument is contrary to fact and precedent.

If relevant at all, the facts of the congressional debate over data security affirm FTC authority over unfair practices related to data security. For example, of the six data security bills Wyndham cites in support of its argument, four included savings clauses to preserve the FTC's existing data security authority. *See* S. 1207, 112th Cong. § 6(d) (1st Sess. 2011); H.R. 2577,

112 Cong. § 6(d) (1st Sess. 2011); H.R. 1841, 112 Cong. § 6(d) (1st Sess. 2011); H.R. 1707, 112 Cong. § 6(d) (1st Sess. 2011).[4] Preservation clauses would be unnecessary if the FTC lacked any existing authority. Similarly, Senator Rockefeller, who co-sponsored Senate Bill 1207, asked an FTC representative: "Can you talk about how Senator Pryor's and my bill will complement ***your existing enforcement efforts***?" *Privacy and Data Security: Protecting Consumers in the Modern World: Hearing on S.B. 1207 Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. 32 (June 29, 2011) (emphasis added). Thus there is no support for Wyndham's argument that Congress is implying that it believes the FTC lacks authority.

Similarly, the Obama Administration's recent Executive Order on Improving Critical Infrastructure Cybersecurity in no way precludes FTC authority over unfair data security practices. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 12, 2013) ("Executive Order") (Hradil Decl., Ex. B). The Executive Order neither addresses FTC authority nor addresses threats to anything other than "Critical Infrastructure," which is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Executive Order § 2. In contrast, this case addresses the protection of consumers' payment card data and seeks to protect consumers'—rather than national security—interests.

Finally, Wyndham's assertion that there is a public controversy regarding the regulation of data security actually supports the FTC's interpretation of the scope of the FTC Act: "[D]eference is particularly appropriate where, as here, an agency's interpretation involves issues

[4] Wyndham's suggestion that the Cyber Intelligence Sharing and Protection Act "would grant immunity" against any action for participating businesses is a gross misreading of the liability exemption provision. H.R. 624, 113th Cong. § 3(b)(3)(A) (1st Sess. 2013). The liability exemption provision is expressly limited to potential liability from complying with that Act. *Id.*

of considerable public controversy, and Congress has not acted to correct any misperception of its statutory objectives." *United States v. Rutherford*, 442 U.S. 544, 554 (1979) (citations omitted). Deference also is appropriate where, as here, Congress, after being informed of the agency's interpretation, has amended a statute (*e.g.*, U.S. SAFE WEB Act of 2006, PL 109–455, December 22, 2006, 120 Stat. 3372 (2006)), but not taken any steps to limit the contested interpretation. *See Saxbe v. Bustos*, 419 U.S. 65, 74 (1974) ("This longstanding administrative construction is entitled to great weight, particularly when, as here, congress has revisited the Act and left the practice untouched."); *Bunker Hill Co. v. EPA*, 658 F.2d 1280, 1284 n.2 (9th Cir. 1981) ("[A]n administrative interpretation deserves particular deference where Congress fails to take advantage of an opportunity to alter it." (citations omitted)). Congress's inaction regarding the FTC's longstanding and widely-reported authority over unfair practices related to data security confirms the FTC's position in this litigation.

B. Wyndham Has Fair Notice of What Section 5 Requires.

Wyndham next argues that enforcement of the FTC Act is unconstitutional because "Section 5 itself clearly provides no meaningful notice to regulated parties—it generically prohibits 'unfair and deceptive' business practices without going into any further details as to what practices might be deemed 'unfair' or 'deceptive.'" Wyndham Mot. 17. This extraordinary argument lacks merit. As noted above, the FTC has consistently stated that in the context of data security, reasonableness is the touchstone: unreasonable data security practices are unfair. Wyndham has notice of what it means to have reasonable data security, from both government and industry sources. It is precisely within the expertise of this Court to evaluate the reasonableness of Wyndham's data security program in light of these various types of guidance.

1. Industry Understands the Meaning of Reasonable Data Security.

Wyndham is not operating in the guidance vacuum that it claims. There are a number of

sources of industry guidance on this issue. Indeed, numerous entities have long provided information concerning the various factors companies should consider in addressing data security. *See, e.g.*, NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook (Oct. 1995); Standards.org, http://www.standards.org/standards/listing/pci_dss (describing history of PCI DSS); 27000.org, http://www.27000.org/iso-27001.htm (describing history of ISO/IEC 27001 standard) and http://www.27000.org/iso-27002.htm (describing history of ISO/IEC 27002 standard).[5]

Wyndham cannot and, likely, does not expect to persuade this Court that it simply did not know what it meant to have reasonable data security. Wyndham itself told consumers that it used "industry standard practices" and that it took "commercially reasonable" efforts to create and maintain firewalls. Compl. ¶ 21. In its motion to dismiss, Wyndham twice states that, in fact, it did take substantial security measures: "WHR at the time had substantial security measures in place to protect its network against being hacked." Wyndham Mot. 1. *See also* Wyndham Mot. 2 (describing the breaches as having occurred "notwithstanding the substantial data-security efforts [Hotels and Resorts] undertook both before and after attacks"). Wyndham's claim of "substantial security measures" merely restates the question that the FTC's Complaint puts before the Court—the reasonableness of Wyndham's data security practices.

2. The FTC Provides Notice to Industry Through Business Guidance and Enforcement Actions.

The FTC provides guidance regarding reasonable data security through its public statements. *See, e.g.*, Protecting Personal Information: A Guide for Business (2007),

[5] Wyndham may argue that it did not know *which* standard it was supposed to follow. This argument misses the point. These standards provide guidance that a reasonable person would adapt to the particular needs of the business in question. The purpose of trial is to determine whether Wyndham's data security program was reasonable based on what was known at the time.

http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf. In addition, many of the allegations of Defendants' specific failures, as appear in Paragraph 24 of the FTC's Complaint, correlate to various features of unreasonable data security programs that have been identified in previous FTC enforcement actions. *See, e.g.*, *In the Matter of BJ's Wholesale Club, Inc.*, File No. 042 3160 (Sept. 20, 2005) (alleging failures related to: encryption; passwords; detection; investigation); *In the Matter of Superior Mortgage, Corp.*, File No. 052 3136 (Dec. 14, 2005) (passwords); *In the Matter of DSW, Inc.*, File No. 052 3096 (Mar. 7, 2006) (encryption; passwords; segmentation; detection); *In the Matter of Nations Title Agency, Inc.*, File No. 052 3117 (June 19, 2006) (detection; incident response; investigation); *In the Matter of CardSystems Solutions, Inc.*, File No. 052 3148 (Sept. 5, 2006) (passwords; segmentation; detection; investigation); *In the Matter of Guidance Software, Inc.*, File No. 062 3057 (Mar. 30, 2007) (encryption; detection); *United States v. ValueClick*, No. Civ. 08-01711 (C.D. Cal. Filed Mar. 17, 2008) (encryption); *In the Matter of Life is Good, Inc.*, File No. 072 3046 (Apr. 16, 2008) (encryption; detection); *In the Matter of The TJX Companies, Inc.*, File No. 072 3055 (July 29, 2008) (encryption; passwords; segmentation; detection; investigation); *In the Matter of Reed Elsevier, Inc.*, File No. 052 3094 (July 29, 2008) (passwords).

Although every situation is different, the consent orders in these matters provide industry, including Wyndham, with notice of different features of data security that must be evaluated in order to maintain a reasonable data security program. As the Supreme Court recognized in *General Electric Co. v. Gilbert*, "[T]he rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for

guidance." 429 U.S. 125, 141-42 (1976) (citation omitted).

3. In the Data Security Context, Adjudication is Permitted and Effective.

The FTC's decision to enforce the FTC Act's prohibition of unfair practices through individual enforcement action, or adjudication, rather than rulemaking "lies [within its] informed discretion." *PBW Stock Exch., Inc. v. SEC*, 485 F.2d 718, 732 (3d Cir. 1973) ("The courts have consistently held that where an agency, as in this case, is given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency." (citing *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947); *NLRB v. Wyman Gordon Co.*, 394 U.S. 759, 772 (1969))). "If the agency affords the party a 'full opportunity to be heard before the [agency] makes its determination' [*NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 295 (1974)], we cannot second-guess the agency decision whether to interpret a standard by rulemaking or by adjudication. [*Chenery*, 332 U.S. at 203]." *Beazer E., Inc. v. EPA*, 963 F.2d 603, 609-10 (3d Cir. 1992).

Nor would it be practicable in the data security context to establish through rulemaking the highly particularized guidelines that Wyndham requests. Wyndham Mot. 17 (seeking rules dictating, *inter alia*, "what software they must use, how they must deploy firewalls").[6] Certain fields are "so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule." *Chenery*, 332 U.S. at 203. The measure of reasonable data security correlates to the sensitivity of the information collected, the amount of information collected, threats attendant to a particular network structure, the evolving field of commonly-

[6] Although the FTC has sought rulemaking authority in the field of data security, it has not done so in order to establish particularized technical standards. Instead, the FTC has sought authority to establish rules that create procedural requirements, such as mandating periodic risk assessments, similar to the rules promulgated pursuant to the Gramm-Leach-Bliley Act. *See* Standards for Safeguarding Customer Information, 16 C.F.R. § 314.4 (2013).

targeted vulnerabilities, and many other factors.[7] The Supreme Court articulated the importance of case-by-case adjudication in similar circumstances:

> [The National Labor Relations Board] is not precluded from announcing new principles in an adjudicative proceeding and that the choice between rulemaking and adjudication lies in the first instance within the Board's discretion. Although there may be situations where the Board's reliance on adjudication would amount to an abuse of discretion or a violation of the Act, nothing in the present case would justify such a conclusion. Indeed, there is ample indication that adjudication is especially appropriate in the instant context. As the Court of Appeals noted, "(t)here must be tens of thousands of manufacturing, wholesale and retail units which employ buyers, and hundreds of thousands of the latter." [*Bell Aerospace v. NLRB*, 475 F.2d 485, 496 (2d Cir. 1973)]. Moreover, duties of buyers vary widely depending on the company or industry. It is doubtful whether any generalized standard could be framed which would have more than marginal utility.

Bell Aerospace, 416 U.S. at 294 (permitting NLRB to evaluate the definition of "managerial employees" for the purpose of collective bargaining on a case-by-case basis).

Even the amici in support of Wyndham have recognized the importance of this type of regulatory flexibility in the field of data security. The Chamber, despite now imploring the Court to require "formal guidance" (Chamber Br. at 12), has in the past led the charge on Capitol Hill to prevent the adoption of specific regulatory requirements in this area. *See* Ken Dilanian, U.S. Chamber of Commerce leads defeat of cyber-security bill, Los Angeles Times (Aug. 3, 2012), http://articles.latimes.com/2012/aug/03/nation/la-na-cyber-security-20120803 ("[T]he U.S. Chamber of Commerce and other business groups strenuously opposed the measure,

---

[7] The United States Chamber of Commerce ("Chamber") endeavors to flip on its head the reasoning of *Chenery*, and asserts that "it is *precisely because* the appropriate standards are difficult to ascertain that businesses cannot be held to a nebulous notion of 'reasonableness,' all without any formal guidance before they find themselves in violation of the law." Proposed Brief of Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, American Hotel & Lodging Association, and National Federal of Independent Business in Support of Defendants, ECF No. 95-2 ("Chamber Br.") 12 (emphasis in original). The Chamber offers no legal support for this argument, which contradicts the holding of *Chenery* that "specialized and varying" fields are best-suited to case-by-case adjudication. *Chenery Corp.*, 332 U.S. at 203.

condemning it as excessive government interference in the free market and arguing that cumbersome federal regulations could hamper companies trying to defend against cyber intrusions."). In its statement discouraging passage of the Cybersecurity Act of 2012, the Chamber discouraged any legislative efforts that would create explicit rules for businesses to follow: "The Chamber urges Congress to not complicate or duplicate existing industry-driven security standards with government mandates and bureaucracies . . . ." *See* U.S. Chamber of Commerce, Key Vote letter on S. 3414, the "Cybersecurity Act of 2012" (July 31, 2012), http://www.uschamber.com/issues/letters/2012/key-vote-letter-s-3414-cybersecurity-act-2012."

The FTC's Complaint aligns with the Chamber's previously-advocated position that data security standards can be enforced in an industry-specific, case-by-case manner.[8] This approach saves regulated entities, such as Wyndham, from having to comply unnecessarily with data security standards that may be excessive in light of the circumstances, and permits regulated entities an opportunity to represent to the finder of fact why it believes—as Wyndham apparently did—that its data security was reasonable.

4. Courts Are Well Suited To Evaluate the Reasonableness of Wyndham's Data Security Practices.

When it passed the FTC Act, Congress observed that courts would have an important role to play in evaluating unfairness. *See FTC v. R.F. Keppel & Bro.*, 291 U.S. 304, 312 n.2 (1934) ("It is believed that the term 'unfair competition' has a legal significance which can be enforced by the commission and the courts, and that it is no more difficult to determine what is unfair

[8] For its part, TechFreedom appears to argue even more explicitly for a judiciary-focused approach: "Those aspects of data security that cannot easily be reduced to rules might well be more amenable to case-by-case adjudication. But without Article III court decisions developing binding legal principles and no other meaningful form of guidance from the FTC, the law will remain unconstitutionally vague." Amici Curiae Brief of TechFreedom, International Center For Law and Economics & Consumer Protection Scholars, No. ECF 94-3 ("TechFreedom Br.") 9. Although the FTC disputes that it has provided no meaningful guidance, it agrees that the field would be aided by a body of law that includes "Article III court decisions."

competition than it is to determine what is a reasonable rate or what is an unjust discrimination." (citing S. Rep. No. 597, at 13 (1914)). It is precisely this role that this court will play in evaluating the reasonableness of Wyndham's data security practices.

Agencies routinely bring enforcement actions where the governing statute or rules lack particularized prohibitions. For example, the National Labor Relations Board requires labor unions, among other things, to bargain on behalf of their employees "in good faith." 29 U.S.C. § 158(d). Courts subsequently have developed this language in a manner that is "consistent with the aim of the [National Labor Relations Act] to promote the resolution of conflict in the labor arena." *NLRB v. New Assocs.*, 35 F.3d 828, 834 (3d Cir. 1994). Similarly, the Occupational Safety and Health Act (OSHA) has a "General Duty Clause" that requires employees to furnish a workplace "free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees." 29 U.S.C. § 654. The Third Circuit has interpreted this obligation as invoking the reasonable person standard, informed in part by industry standards. *Voegele Co., Inc. v. Occupational Safety & Health Review Comm'n*, 625 F.2d 1075, 1078 (3d Cir. 1980). In fact, under the Administrative Procedure Act, courts routinely subject numerous agency actions to a similar reasonableness test. 5 U.S.C. § 706.

Although Wyndham relies on several OSHA cases in its fair notice argument, it neglects discussion of the General Duty Clause, which is most analogous to the unfairness prohibition of the FTC Act. For example, Wyndham cites *Fabi Construction Co. v. Secretary of Labor* for the proposition that Fabi lacked fair notice of OSHA regulations. 508 F.3d 1077, 1088 (D.C. Cir. 2007). This same case, however, includes an extensive reasonableness analysis to evaluate whether Fabi violated the General Duty Clause. In its determination that Fabi did not meet this "general duty," the Court evaluated a number of factors, including whether Fabi followed third-

party technical drawings, whether Fabi complied with industry standard practices, and expert opinion on Fabi's likely familiarity with industry standards. *Id*. at 1084. This is the type of inquiry the FTC asks this Court to undertake in this matter.

Nor is there anything extraordinary about courts using these same tools to evaluate the reasonableness of data security. *See, e.g.*, *United States v. Hanjuan Jin*, 833 F. Supp. 2d 977, 1008-09 (N.D. Ill. 2012) (evaluating, in trade secrets action, the reasonableness of Motorola's data security, including password policies, firewalls, physical security, etc.). There is simply no factual or legal basis for Wyndham and the amici's position that this case is somehow unusual, much less that it is unconstitutional.

5. Wyndham's Fair Notice Cases Are Inapposite.

Wyndham relies principally on the Supreme Court's recent decision in *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307 (2012) ("*Fox II*"), to argue that, because the FTC is proceeding through case-by-case enforcement, the FTC Act should be invalidated and this case should be dismissed for lack of fair notice. Wyndham Mot. 14-19. This reliance is badly misplaced. In *Fox II*, the FCC's failure to provide notice had nothing to do with the FCC proceeding by case-by-case enforcement, as Wyndham suggests. Instead, it was undisputed that the FCC had "reversed prior rulings that had found fleeting expletives not indecent." *Id*. at 2314. Indeed, in *Fox I*, the Supreme Court expressly affirmed the FCC's authority to evaluate obscenity on a case-by-case basis: "More fundamentally, however, the agency's decision to consider the patent offensiveness of isolated expletives on a case-by-case basis is not arbitrary or capricious." *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 520 (2009). *See also id.* (recognizing that case-by-case enforcement is necessary to distinguish between obscene language uttered at awards shows, which "draw the attention of millions of children" versus, for example, a "recitation of Geoffrey Chaucer's Miller's Tale").

Moreover, in this matter, the FTC is seeking only equitable relief, and doing so in a field that has been the subject of FTC enforcement activity since 2000. By contrast, the cases that Wyndham relies on, including *Fox II*, expressly limit themselves to instances in which one or both of the following are true: the agency had reversed itself, and the agency was seeking to impose punitive (as opposed to equitable) remedies. *See Fox II*, 132 S. Ct. at 2314 (reversal of position); *id*. at 2318 (legal remedies); *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2169 (2012) (agency "advanced a different interpretation" previously); *id*. at 2167 (interpretation threatened "massive liability"); *General Electric Co. v. EPA*, 53 F.3d 1324, 1329-30 (D.C. Cir. 1995) ("an agency may not deprive a party of property by imposing civil or criminal liability"); *Gates & Fox Co. v. Occupational Safety & Health Review Comm'n*, 790 F.2d 154, 156 (D.C. Cir. 1986) (invalidating application of regulation appropriate "[w]here the imposition of penal sanctions is at issue"); *Dravo Corp. v. Occupational Safety & Health Review Comm'n*, 613 F.2d 1227, 1229 (3d Cir. 1980) ("reject[ing] the approach taken in another proceeding"); *id*. at 1232 (rejecting expansive interpretation because "we deal here with a penal sanction"); *Fabi Construction*, 508 F.3d at 1086 (agency "interpretation fails to make sense"); *id*. at 1089 (resulting in "citation and fine"); *Trinity Broadcasting of Fla., Inc. v. FCC*, 211 F.3d 618, 631-32 (D.C. Cir. 2000) (company penalized by refusal to renew license after "problematic" interpretation that contradicted earlier interpretation); *United States v. Chrysler Corp.*, 158 F.3d 1350, 1355-56 (D.C. Cir. 1998) (NHTSA's interpretation contradicted its "own test schematic," and would "deprive Chrysler of property no less than a fine").

This action falls within neither of those categories. Here, the FTC is seeking to enforce Section 5 in the same way it has for the last decade. Moreover, rather than seek civil penalties, the FTC here is pursuing only equitable relief. Compl. ¶ 51. *Cf. FTC v. Magazine Solutions,*

LLC, 432 F. App'x 155, 158 (3d Cir. 2011) ("[Section] 13(b)'s grant of authority to provide injunctive relief carries with it the full range of equitable remedies[.]" (quotation marks and citations omitted)).

III. THE COMPLAINT SATISFIES THE PLEADING STANDARD FOR DECEPTIVE ACTS OR PRACTICES.

Finally, this Court should reject Wyndham's half-hearted argument that the FTC fails to state a claim for deception. Wyndham's invocation of franchise law is, not only a red herring, but an argument that is highly fact-specific and not suitable for a motion to dismiss.[9] Regardless, the Complaint carefully catalogs the various deceptive statements by each of the Wyndham entities.[10]

A. The Complaint Need Not Meet the Rule 9(b) Standard.

Wyndham cursorily asserts that deception "sounds in fraud" and therefore the Complaint must satisfy the Rule 9(b) pleading requirements for this count. Fed. R. Civ. P. 9(b). This is a question of first impression in this district. The Southern District of New York and several "[o]ther district courts have held that actions brought by the FTC for violations of Section 5(a) of the FTC Act are not subject to Rule 9(b)." *FTC v. Med. Billers Network, Inc.*, 543 F. Supp. 2d 283, 314 (S.D.N.Y. 2008) (collecting cases). Wyndham cites two district court cases from the Ninth Circuit. *FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 853 (C.D. Cal. 2010); *FTC v. Ivy Capital*, No. 2:11-CV-286, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011) (following *Lights of America*). This Court should not follow these cases, however, as they are wrongly decided.

---

[9] The International Franchise Association brief suffers from the same defect. Its argument is entirely dependent on the content of the franchise agreements. Brief Amicus Curiae of the International Franchise Association in Support of Defendant Wyndham Hotels & Resorts' Motion to Dismiss, ECF No. 96-2 ("IFA Br.") 2-10.

[10] As explained further in the FTC's Response in Opposition to the Motion to Dismiss by Wyndham Worldwide, Hotel Group, and Hotel Management, filed simultaneously, the Complaint also pleads that all four Wyndham entities operate as a common enterprise.

As the Tenth Circuit has held, a claim of deceptive practices pursuant to Section 5 of the FTC Act "is not a claim of fraud as that term is commonly understood or as contemplated by Rule 9(b)." *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1203 n.7 (10th Cir. 2005). Moreover, unlike an action for common law fraud, the Commission does not need to prove scienter, reliance, or injury to establish deception under the FTC Act. *Id*. *See also FTC v. Publ'g Clearing House, Inc.*, 104 F.3d 1168, 1171 (9th Cir. 1997) ("[T]he FTC is not required to show that a defendant intended to defraud consumers . . . ." (emphasis omitted)); *FTC v. Figgie Int'l, Inc.*, 994 F.2d 595, 605-06 (9th Cir. 1993) (unlike common law fraud, proof of subjective reliance by individual consumers is not required in FTC enforcement actions). Therefore, Rule 9(b) should not apply.

B. Regardless, the Complaint Meets the Rule 9(b) Standard.

Even if Rule 9(b) were applicable here, the Complaint satisfies it because "the circumstances constituting fraud or mistake" are stated "with particularity." Fed. R. Civ. P. 9(b). The FTC "plead[s] with particularity the 'circumstances' of the alleged fraud in order to place the defendants on notice of the precise misconduct with which they are charged." *Seville Indus. Mach. Corp. v. Southmost Mach. Corp.*, 742 F.2d 786, 791 (3d Cir. 1984); s*ee also In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1418 (3d Cir. 1997) (same).

Wyndham claims that "the FTC relies primarily on allegations concerning the state of data-security ***at the Wyndham-branded hotels***." Wyndham Mot. 24 (emphasis in original). This inaccurately characterizes the allegations in Paragraph 24 of the Complaint. In fact, the Complaint alleges that Wyndham was responsible for these failures because it permitted computers with unreasonable data security measures on its network. Compl. ¶ 24. Thus, for example, the allegation that Wyndham "failed to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their

local computer networks to Hotels and Resorts' computer network" (*id*. ¶ 24(c)), reflects both a failure of the Wyndham-branded hotels (for failing to have adequate information security policies and procedures) and Hotels and Resorts (for permitting vulnerable computers to access its network). Thus, the data security failures that Wyndham attributes to the "Wyndham-branded hotels" are actually data security failures on Wyndham's own network.

Because all of the alleged data security failures in the Complaint are attributable to Wyndham, the FTC does not need to plead "actual control" over the activities of the Wyndham-branded hotels, as Wyndham and its amici assert. Wyndham Mot. 25-27; IFA Br. 6-8. Nevertheless, the Complaint does plead "actual control," over the relevant aspects of the franchisees' data security practices: Wyndham required purchase of a particular property management system (*id*. ¶ 15); managed the systems (*id*. at ¶ 17); at some hotels, had exclusive access to the systems (*id*. ¶ 18); at all hotels, had administrator access to the systems (*id*. ¶ 17); set passwords for the systems (*id*.); and provided exclusive technical support for the systems (*id*. ¶ 19). These facts establish the "control or right to control" necessary to establish franchisor liability and, to the extent Wyndham intends to dispute these facts, that is a question of fact inappropriate for a motion to dismiss. *See Drexel v. Union Prescription Centers, Inc.*, 582 F.2d 781, 789-90 (3d Cir. 1978) (denying motion for summary judgment because further factual development was needed).[11] Furthermore, the allegations that Wyndham concedes are relevant to the data security measures of the Wyndham entities, regarding failure to inventory computers (*id*. ¶ 24(g)), detection of unauthorized access (*id*. ¶ 24(h)), and incident response procedures (*id*. ¶ 24(i)), are sufficient to state a claim for deceptive data security practices.

[11] IFA also threatens that the "FTC's theory would turn franchise law on its head." IFA Br. 10. This concern is meritless. The actual-control exception is a well-established principle of franchise law. *See Drexel*, 582 F.2d at 785-90.

Finally, Wyndham incorrectly claims that a reasonable consumer's understanding of Wyndham's privacy policy is a question of law that can be answered because the privacy policy, "by its plain terms," disclaims responsibility for data security at the franchisees. Wyndham Mot. 25. The Third Circuit has rejected such a "plain terms" approach to evaluating allegedly deceptive statements. *Am. Home Prods. Corp. v. FTC*, 695 F.2d 681, 687 (3d Cir. 1982) ("The impression created by the advertising, not its literal truth or falsity, is the desideratum.").

The FTC alleges that any reasonable consumer would have understood Wyndham's privacy policy to be making express representations about information collected at the Wyndham-branded hotels. Compl. ¶ 21. For example, the policy states that it applies to "hotels of our brand" and "information collected about guests." *See* Wyndham Hotel Group, LLC Customer Privacy Policy and Information Practices Statement ("Wyndham Privacy Policy"), Hradil Decl., Ex. A, ECF No. 91-3, at 1. Wyndham's argument demands that this Court hold, as a matter of law and with no fact-finding, that "any reasonable consumer . . . would have understood that the policy made statements only about data-security practices at Hotels and Resorts and made no representations about data-security practices at the Wyndham-branded hotels." Wyndham Mot. 25-26.[12] Wyndham's argument is premised entirely on one ambiguous disclaimer that comes five pages after language that suggests precisely the opposite: That Wyndham's data security representations cover information collected from hotel "guests" at "hotels of our brand." Even if there were an express statement disclaiming these security

[12] Wyndham also argues that their privacy policy applies only to information Hotels and Resorts *collects*. This contradicts the language of the privacy policy, which makes representations about information that Hotels and Resorts *controls*. Wyndham Privacy Policy at 1. This language suggests that the privacy policy would cover information collected at Wyndham-branded hotels but later controlled by a Wyndham entity. Moreover, Wyndham certainly is responsible for the collection and control of information at hotels that it manages through Hotel Management. *See* Compl. ¶ 10 ("fully operate"); *id*. ¶ 18 ("controls the 'operation" of those hotels").

representations, the effectiveness of such a disclaimer is a fact-specific inquiry and, as such, inappropriate for a motion to dismiss. *See FTC v. Nat'l Urological Group, Inc.*, 645 F. Supp. 2d 1167, 1189 (N.D. Ga. 2008) ("claims or net impressions communicated to reasonable consumers, is fundamentally a question of fact"). Therefore, it is not appropriate to inquire at the motion to dismiss stage about the effectiveness of the disclaimer Wyndham identifies (in a paragraph that does not mention data security) on the bottom of the fourth page (of five pages) of the privacy policy.

CONCLUSION

For the foregoing reasons, the FTC respectfully requests that the Court deny Wyndham's motion to dismiss.

Dated: May 20, 2013.

Respectfully submitted,
s/ Katherine E. McCarron
Lisa Weintraub Schifferle
Kristin Krause Cohen
Kevin H. Moriarty
Katherine E. McCarron
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