David B. Rosenbaum, 009819
Anne M. Chapman, 025965
OSBORN MALEDON, P.A.
2929 North Central Avenue, Suite 2100
Phoenix, Arizona 85012-2793
(602) 640-9000
achapman@omlaw.com
drosenbaum@omlaw.com

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

Douglas H. Meal, MA Bar 340971 (*Pro Hac Vice*)
Ropes & Gray, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517
douglas.meal@ropesgray.com

Attorneys for Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

vs.

Wyndham Worldwide Corporation, et. al.,

Defendants.

Case No. CV 12-1365-PHX-PGR

REPLY IN SUPPORT OF MOTION TO DISMISS BY DEFENDANT WYNDHAM HOTELS & RESORTS LLC

INTRODUCTION

The FTC's brief asserts a staggeringly broad theory of agency power. According to the FTC, a 1914 statute that prohibits "unfair" trade practices empowers the Commission to regulate the extremely complex computer systems that American businesses use to protect consumer information. The FTC believes that it can engage in such regulation without publishing any rules or regulations explaining in advance what companies must do to comply with the law. Instead, the FTC can provide no notice at all and bring "case-by-case" enforcement actions against companies that have suffered cyber attacks. Only after a company has been attacked, had data stolen, participated in an agency investigation, and been subjected to litigation, will the FTC then decree whether it believes the company's data-security practices to have been "reasonable."

Such an Orwellian understanding of governmental power is so foreign to our system of justice that Congress could not possibly have intended the FTC to wield it. To the contrary, Congress has given every indication that the FTC has no authority at all to impose its own view of data-security policy on the business community. Over the past 20 years, Congress has enacted numerous statutes that expressly authorize particular agencies to establish data-security standards in narrow sectors of the economy. None grants the FTC the sweeping power to set data-security standards for ***all*** American businesses operating in ***all*** industries. That statutory history reveals that, when Congress intends a federal agency to impose data-security requirements, it does so expressly through a targeted legislative grant, not through the general and indirect provisions of a statute like Section 5 of the FTC Act. And lest there be any doubt, the FTC ***itself*** previously agreed with that interpretation, stating on several occasions that it lacked authority to prescribe affirmative data-security standards.

The facts here aptly illustrate why the FTC is ill-equipped to pursue its own data-security program completely apart from Congress. Like scores of other private companies and government agencies, Wyndham Hotels & Resorts, LLC ("WHR") was victimized by hackers. In response, WHR alerted authorities, retained expert consulting

firms, and implemented comprehensive remedial measures. Such conduct should be applauded, not targeted by an overzealous federal agency eager to punish American businesses—as opposed to the hackers themselves—for data-security breaches.

Although the FTC has strong-armed other companies into signing settlement agreements on this theory, no ***court*** has ever held that Section 5 permits the FTC to regulate the data-security practices of American businesses. This Court should not be the first. The significant political and economic decisions involved in setting data-security policy should be made by Congress—not by an independent federal agency with no statutory mandate, no expertise in the area, and no political accountability.

I. THE COUNT II UNFAIRNESS CLAIM MUST BE DISMISSED

A. The FTC's Unfairness Authority Does Not Extend To Data Security

The FTC's regulatory authority argument begins from the erroneous premise that WHR must identify something that ***exempts*** data security from the FTC's regulatory reach. *See, e.g.*, FTC Opp. at 4 ("FTC unfairness authority does not *exclude* data security.") (type and font altered). That is backwards. The FTC, like every other federal agency, has the burden of showing that Congress intended to delegate to it the specific authority that it claims. *See Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986) ("[A]n agency literally has no power to act … unless and until Congress confers power upon it."). The FTC cannot meet that burden here. It is implausible that Congress would have given the FTC authority to set data-security policy through a 1914 statue that forbids "unfair" trade practices. The Supreme Court has consistently refused to construe such open-ended provisions as empowering agencies to impose sweeping regulations on the business community. *See, e.g.*, *Gonzales v. Oregon*, 546 U.S. 243 (2006); *Whitman v. Am. Trucking Assns.*, 531 U.S. 457 (2001); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000); *MCI Telecomms. Corp. v. AT&T Co.*, 512 U.S. 218 (1994). That is particularly true where Congress—as it has done with respect to data security—"has spoken subsequently and more specifically to the topic at hand" by enacting more targeted legislation. *Brown &*

Williamson Tobacco, 529 U.S. at 133. And if that were not enough, the FTC's history of disavowing authority to set data-security standards provides yet another reason for this court to refuse to endorse its novel theory of Section 5. *See id*. at 144-46.

The FTC attempts to distinguish *Gonzales*, *Whitman*, *Brown & Williamson*, and *MCI*, by arguing that it "never disclaimed authority" to regulate data security and that Congress's subsequent enactment of data-security laws is not "inconsistent or irreconcilable" with the FTC's regulation of data security under Section 5. FTC Opp. at 11. Neither argument is correct. *First*, the FTC cannot run away from the fact that for many years it took the position that Section 5's "unfair … practices" language did not give it authority to regulate the data-security practices of private companies. On several occasions, the Commission stated that its authority over data security was "limited ... to ensuring that Web sites follow their stated information practices," *Consumer Privacy on the World Wide Web*, Hearing before H. Comm. on Commerce, Subcomm. on Telecomm., (July 21, 1998) at n. 23., *available at* http://www.ftc.gov/os/1998/07/privac98.htm, and that it "lack[ed] authority to require firms to adopt information practice policies," 2000 FTC Privacy Report at 34.[1] As put by an FTC official in 2001, "[t]he agency's jurisdiction is (over) deception…. If a practice isn't deceptive, we can't prohibit them from collecting information." Jeffrey Benner, *FTC Powerless to Protect Privacy*, Wired, May 31, 2001. Indeed, the FTC's belief that it lacked authority to mandate data-security standards is precisely why the FTC repeatedly asked Congress to enact new legislation that would have given it the very authority that it now purports to find in Section 5. *See* WHR Mot. to Dismiss at 7.

Second, the FTC does not dispute that Congress has enacted no fewer than ten federal statutes authorizing particular federal agencies to regulate data-security

[1] The FTC's attempt to explain away the statements in its 2000 Privacy Report is particularly unconvincing. Although the Report does make the unremarkable statement that the "FTC Act prohibits unfair and deceptive practices," the very same paragraph goes on to explain that the Act's "unfair … practices" language did not permit the FTC to impose data-security standards on the private sector: "[T]he Commission lacks authority to require firms to adopt information practice policies." 2000 Privacy Report at 33-34.

practices in certain narrow areas. *Id*. at 7-8 (citing statutes). Instead, the FTC insists that those statutes are irrelevant because they do not "expressly or impliedly restrict FTC Act authority." FTC Opp. at 8. But that is precisely what they do. It is a well-established principle of statutory interpretation that "where the scope of [an] earlier statute is broad but the subsequent statutes more specifically address the topic at hand," the "later federal statute should control [a court's] construction of the [earlier] statute." *Brown & Williamson*, 529 U.S. at 143 (quotations omitted). That is all the more true here, where several of the subsequently enacted statutes—such as FCRA, GLBA, and COPPA—grant the FTC limited authority over data-security matters, but only in narrow contexts that are not implicated in this case. *See* WHR Mot. to Dismiss at 8. Contrary to the FTC's argument, FCRA, GLBA, and COPPA were not simply procedural laws that "enhance[d] the FTC's legal tools." FTC Opp. at 8. Instead, those statutes by their express terms gave the FTC the underlying substantive authority to regulate data security in certain narrow contexts—authority that Section 5 itself does not provide.

Searching for a Congressional delegation that it was never given, the FTC argues that its ***own activities*** provide a basis from which it can claim authority to regulate the data-security practices of American businesses. As the FTC points out, it has brought "forty-one enforcement actions" in the past decade (but only "seventeen [that] alleged unfair practices") and has "reported and publicized its data security program." FTC Opp. at 5, 7. But the "determinative question" is "not what the [Commission] thinks it should do but what Congress has said it can do." *CAB v. Delta Air Lines, Inc.*, 367 U.S. 316, 322 (1961). And Congress has ***never*** endorsed the FTC's theory that Section 5 gives it unfettered authority to act as a roving policeman of data security for the business community. If anything, the FTC's history of bringing enforcement actions is only further cause for concern. None of the FTC's actions resulted in a judicial decision on the merits—instead, in each case the defendants entered into settlement agreements prior to any significant litigation activity. Those settlement agreements are of course not precedential. *See, e.g.*, *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312

(7th Cir. 1976) (consent decrees "do[] not adjudicate the legality of any action" and are not "controlling precedent for later Commission action"). But more significantly, they reveal a pattern of agency conduct through which the FTC has been using the high costs of litigation to "strong-arm[] … regulated parties into 'voluntary compliance' without the opportunity for judicial review." *Sackett v. EPA*, 132 S. Ct. 1367, 1374 (2012).

In the end, the FTC is reduced to arguing that Congress has "acquiesced" in its regulation of data security under Section 5 because it has not "taken any steps to limit the [FTC's] contested interpretation." FTC Opp. at 10. The Supreme Court, however, has often "expressed skepticism toward reading the tea leaves of Congressional inaction," because what the FTC describes as "Congress's deliberate acquiescence should more appropriately be called Congress's failure to express any opinion." *Rapanos v. United States*, 547 U.S. 715, 749-50 (2006). The Court has thus demanded "***overwhelming*** evidence" that Congress "considered and rejected the ***precise*** issue presented before the Court" before it will accept Congressional acquiescence as a plausible theory of statutory interpretation. *Id*. at 750 (emphases added). Far from establishing "overwhelming evidence" that Congress has specifically considered and approved of the FTC's use of Section 5 to impose data-security standards on the private sector, all relevant indicators of Congressional intent suggest that Congress has not delegated such significant power to the FTC.[2] *See supra* at 2-4.

Finally, in an attempt to salvage its "we can regulate anything" approach, the FTC points to other instances in which it has "use[d] … its unfairness provision." *See* FTC Opp. at 6. But far from supporting the FTC's view of Section 5, those examples

[2] Trying to bolster its thin Congressional acquiescence argument, the FTC points to four proposed (but not enacted) data-security bills that included language "[p]reserve[ing] … the Commission's authority under any other provision of law." FTC Opp. at 10; *see also* S. 1207 § 6(d). None of those bills addressed, much less endorsed, the FTC's claimed authority to regulate data security under Section 5. And in context, that language more sensibly applies to the FTC's narrow delegations of data-security authority under FCRA, GLBA, and COPPA. In any event, four un-enacted statutes is hardly the kind of "overwhelmingly evidence" necessary to support a Congressional acquiescence argument, particularly when Congress considered four ***other*** cybersecurity bills that included no language at all "preserving" authority for the FTC. *See* S. 1151, S. 1408, S. 1434, S. 1535.

only confirm that the FTC is operating far beyond its delegation and core competencies in this case. With the exception of *Neovi* (which WHR addressed elsewhere, *see* WHR Mot. to Dismiss at 13-14), all of the examples cited by the FTC were cases in which the defendant engaged in some kind of misleading or fraudulent conduct. *See In re Int'l Harvester Co.*, 104 F.T.C. 949 (1984) (failing to disclose safety hazards with farm equipment); *FTC v. Stefanchik*, 559 F.3d 924 (9th Cir. 2009) (falsely advertising that consumers could easily make money from selling mortgages); *FTC v. Garvey*, 383 F.3d 891 (9th Cir. 2004) (issuing false advertisements about weight-loss products); *FTC v. Inc21.com Corp.*, 475 F. App'x 106 (9th Cir. 2012) (fraudulently enrolling customers in internet service and billing them without their knowledge). In none of those cases did the FTC try to use its unfairness authority as it wants to in this case: to enact freestanding substantive requirements to which companies must adhere. To the contrary, one of the FTC's own cases ***expressly disclaims*** the power to set standards for the private sector, *see Int'l Harvester Co.*, 104 F.T.C. at *88 ("The Commission does not ordinarily seek to mandate specific conduct or specific social outcomes, but rather seeks to ensure simply that markets operate freely, so that consumers can make their own decisions."), and two others ***did not discuss unfairness liability at all***, but merely addressed deception claims. *See Stefanchik*, 559 F.3d 924; *Garvey*, 383 F.3d 891. And, of course, none of the FTC's examples resembled the legislative context at issue here, where Congress has enacted at least ten federal laws addressing data-security matters and is currently engaged in a robust debate over comprehensive cybersecurity legislation.

B. The FTC Refuses To Give Fair Notice Of What The Law Requires

Even assuming the FTC had some limited authority to regulate data security, it surely could not exercise that authority in this fashion. The FTC's astonishing position is that it cannot (and will not) state in advance what companies must do to avoid liability. *See* FTC Opp. at 12. Instead, the FTC believes that it can wait until ***after*** a

data-breach has occurred, at which point it will investigate the "reasonableness" of a company's practices on a "case-by-case" basis. *Id*. at 12-13.

That theory of liability is entirely foreign to our system of justice. As a matter of basic fairness and constitutional due process, the FTC "owes a duty to define the conditions under which conduct … would be unfair so that businesses will have an inkling as to what they can lawfully do rather than be left in a state of complete unpredictability." *E.I. du Pont de Nemours & Co. v. FTC*, 729 F.2d 128, 138-39 (2d Cir. 1984); *see also FCC v. Fox*, 132 S. Ct. 2307, 2317 (2012). But "complete unpredictability" is exactly what the FTC's approach has created. As the *amicus* briefs submitted in this case persuasively explain, the FTC's "case-by-case" approach has left American businesses completely in the dark as to what the law requires and what they can do in advance to avoid liability. *See* Br. of *Amici Curiae* Chamber of Commerce, et al., at 7-12. That is not a tenable, or desirable, regulatory regime.

All of this goes to show that, if the FTC can regulate data security at all, it must do so through published rules that give regulated parties fair notice of what the law requires. The FTC's response that "an agency is not precluded from announcing new principles in the adjudicative proceeding," FTC Opp. at 12 (quotations omitted), is beside the point. Although agencies do have some discretion to make law through adjudication, fundamental concepts of fair notice and due process place critical limits on that discretion. *See Ford Motor Co. v. FTC*, 673 F.2d 1008 (9th Cir. 1981); *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 294 (1974). And here, those considerations require that the FTC set data-security standards in advance, so that businesses can fairly know what is required of them before the FTC seeks to hold them liable.

C. Section 5 Does Not Apply To The Security of Payment-Card Data

The FTC's efforts to regulate the security of payment-card data is particularly unjustified. Because federal statutes and card-brand rules eliminate the possibility that consumers can suffer financial injury from the theft of payment-card data, practices regarding the security of that data cannot trigger the necessary precondition of FTC

jurisdiction—namely, that there be "substantial injury to consumers which is not reasonably avoidable by consumers themselves." 15 U.S.C. § 45(n).[3]

The FTC does not (and cannot) dispute that the theft of credit card information does not cause financial injury to consumers. Instead, it argues that the Ninth Circuit has held that the "aggravation" associated with "obtaining reimbursement" from card issuers constitutes the kind of "substantial injury" that is the focus of the FTC Act. FTC Opp. at 14 (quoting *FTC v. Neovi*, 604 F.3d 1150, 1158 (9th Cir. 2010)). That is an over-reading of what the Ninth Circuit has held. In *Neovi*—which did not involve payment-card data—the Court held, unremarkably, that withdrawal of $400 million in fraudulent funds from consumers' accounts constituted "substantial" injury under Section 5. The Court did not hold, and had no occasion to hold, that ***non-economic***, nuisance-type "injuries" of the sort relied on by the FTC here were also "substantial" consumer injuries that the FTC is empowered to address.[4] That would have been an extraordinary holding for the Court to embrace, particularly because other courts (and even the FTC itself) have expressly rejected it. *See, e.g.*, *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 973 n. 18 (D.C. Cir. 1985) ("[S]ubstantial injury involves economic or monetary harm and does not cover subjective examples of harm.").

Even if Section 5 could be stretched to embrace the theft of payment card data, the standard of liability for failing to protect such data would be far above what the FTC has alleged in this case. As WHR has explained, courts facing similar theories of liability under state law have applied "egregiousness" or "recklessness" standards. WHR Mot. to Dismiss 13 (citing *Worix v. MedAssets, Inc.*, 2012 WL 1419257, at *6 (N.D. Ill. Apr. 24, 2012)). The FTC offers no response at all to that case law—perhaps because it knows that it could not plausibly allege such conduct by WHR. Moreover,

[3] It is well-established that courts may consider publicly available documents on a 12(b)(6) motion where the parties "do not dispute the authenticity of the document" and the "plaintiff's claim depends on the contents" of the document. *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

[4] Rather, *Neovi*'s discussion of such nuisance "injuries" was limited to whether they were caused by the defendant and were reasonably avoidable.

where the evidence of substantial consumer injury is at a minimum unclear, even the FTC has acknowledged that a Section 5 unfairness claim must additionally be predicated on an alleged violation of established public policy. *See* FTC Unfairness Policy Statement (Dec. 17, 1980), *appended to In re Int'l Harvester*, 1984 WL 565290, at *98. No such allegation appears—or could have been advanced—in the Amended Complaint, as there is no established public policy requiring businesses to take any particular measures to protect payment-card data they collect.

D. The FTC's Unfairness Claim Fails Federal Pleading Requirements

Finally, the FTC is on no firmer ground when it argues that the Amended Complaint "satisfies the pleading standard for unfairness." FTC Opp. at 3 (font and capitalization altered). The FTC insists that it has "identifie[d], with specificity, ten data security failures," pointing to paragraph 24 of its Amended Complaint. *Id*. at 4. But upon inspection, those purportedly "specific[]" allegations are really nothing more than generic allegations of unreasonableness couched in technical terms. Thus, the FTC faults WHR for not using practices that were "reasonable," "adequate," or "proper," Am. Compl. ¶ 24, without providing any factual specificity as to what those vague standards require. Conclusory allegations of "unreasonableness" become no more specific simply because they are surrounded by technical language.

Even looking past the FTC's conclusory allegations of liability, the Commission also has not adequately pleaded causation. *See* 15 U.S.C. § 45(n). The Amended Complaint contains no factual allegations explaining how the alleged data-security failures caused the data breaches (or otherwise resulted in consumer injury). Instead, the FTC simply asserts without explanation that the breaches were the "result" of WHR's data-security program. Am. Compl. ¶¶ 25, 32. Such conclusory allegations of wrongdoing are exactly the kind of unadorned assertions that fail federal pleading requirements. *See Ashcroft v. Iqbal*, 556 U.S. 662 (2009). After a two-year investigation into WHR's data-security practices, surely the FTC should be required to say more about how the alleged vulnerabilities "result[ed]" in the data breaches.

II. THE COUNT I DECEPTION CLAIM MUST BE DISMISSED

The FTC's attempt to salvage its wayward deception claim is no more convincing. To begin, two other district courts in this circuit have recently held that deception allegations under Section 5 must comply with Rule 9(b) because they "sound in fraud." *FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 852 (C.D. Cal. 2010); *FTC v. Ivy Cap., Inc.*, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011). Although the FTC believes that those cases were "wrongly decided," FTC Opp. at 14, it offers no legal argument for setting aside the cogent and reasoned analyses that those courts set forth.

Regardless of what pleading standard controls, the FTC's deception count—which is based solely on WHR's online privacy policy—fails as a matter of law. The FTC alleges that the privacy policy was deceptive because it misrepresented the state of data security at the independent Wyndham-branded hotels. *See* Am. Compl. ¶¶ 25, 30-31, 34-35, 37. But the privacy policy ***does not make*** any representations about the state of data security at the Wyndham-branded hotels. *See* WHR Mot. to Dismiss at 16. Indeed, the policy ***expressly disclaims*** making any such representations. *Id*.

The FTC does not dispute that the privacy policy fails to say anything at all about data-security practices at the Wyndham-branded hotels. Instead, it offers three reasons for why that fact should not matter. *First*, the FTC argues that the privacy policy makes representations about the security of all data collected from "guests" that WHR "controls," "irrespective of how the information was collected." FTC Opp. at 16. But that is neither here nor there. The express disclaimer in the privacy policy states that although each hotel "collects Customer Information and uses the Information for its own purpose," WHR "do[es] not control the use of this Information or access to the Information." Allen Decl., Ex. A, at 4. The privacy policy thus goes out of its way to make clear that WHR does not control data collected by its franchised and managed properties, and thus that the representations in the policy do not apply to that data.

Unperturbed, the FTC insists that this Court should ignore the express disclaimer because the "effectiveness of such a disclaimer is a fact-specific inquiry" that is

"inappropriate for a motion to dismiss." FTC Opp. at 17. But this is not a case in which a disclaimer is buried in "fine print" or otherwise obscured. *Id*. The disclaimer in WHR's privacy policy is set forth in its own separate paragraph, with its own bold-face heading, using the same size and type of font used elsewhere in the document. In similar circumstances, courts have not hesitated to rely on such language in dismissing deception or fraud-based claims. *See, e.g.*, *Girard v. Toyota Motor Sales, USA, Inc.*, 316 F. App'x 561, 563 (9th Cir. 2008) (affirming motion to dismiss in light of express disclaimer); *Baxter v. Intelius, Inc.*, 2010 WL 3791487 (C.D. Cal. Sept. 16, 2010) (granting motion to dismiss in light of express disclaimer).[5]

Second, the FTC argues that it has adequately alleged that WHR made deceptive statements about its own data-security practices. But, as explained, those allegations fail to satisfy the demanding pleading standard of Rule 9(b) or even the plausibility standard of *Iqbal*. WHR Mot. to Dismiss at 17. And even if those deficiencies were adequately pleaded, the FTC does nothing to explain how the potential deficiencies it has identified did anything to place consumers' personal information at risk.

Third, the FTC argues that WHR "participated directly in the data security failures" at certain Wyndham-branded hotels, through its sister company Wyndham Hotel Management. FTC Opp. at 17. As the motion to dismiss filed by the other defendants in this case explains, however, the Amended Complaint fails to allege facts establishing such an aggressive theory of imputed liability. *See* WWC, et al., Mot. to Dismiss [Dkt. # 33]. And even if it did, the FTC nowhere identifies what unreasonable actions WHM took with respect to data security at the Wyndham-branded hotels.

[5] In passing, the FTC selectively refers to language explaining that the privacy policy applies to "hotels of our Brands located in the United States … only." Ex. A, at 5. That language merely restricts the geographic scope of the policy. And to the extent it acknowledges that certain provisions might apply to Wyndham-branded hotels, that acknowledgement is unremarkable: whether or not other provisions of the policy apply to Wyndham-branded hotels, the express disclaimer makes clear that the policy does not apply to the data-security practices of the Wyndham-branded hotels.

DATED this 23rd day of October, 2012.

OSBORN MALEDON, P.A.

By s/David B. Rosenbaum

David B. Rosenbaum
Anne M. Chapman
2929 North Central Avenue, Suite 2100
Phoenix, Arizona 85012-2794

Eugene F. Assaf, P.C., 449778, *pro hac vice*
K. Winn Allen, 1000590, *pro hac vice*
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005

Douglas H. Meal, 340971, *pro hac vice*
Ropes & Gray, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600

Attorneys for Defendants

CERTIFICATE OF SERVICE

☒ I hereby certify that on October 23, 2012, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to all CM/ECF registrants.

s/Kelly Dourlein