

1 David B. Rosenbaum, 009819  
2 Anne M. Chapman, 025965  
3 OSBORN MALEDON, P.A.  
4 2929 North Central Avenue, Suite 2100  
5 Phoenix, Arizona 85012-2793  
6 (602) 640-9000  
7 [achapman@omlaw.com](mailto:achapman@omlaw.com)  
8 [drosenbaum@omlaw.com](mailto:drosenbaum@omlaw.com)

9 Eugene F. Assaf, DC Bar 449778 (*Pro Hac Vice*)  
10 K. Winn Allen, DC Bar 1000590 (*Pro Hac Vice*)  
11 Kirkland & Ellis, LLP  
12 655 Fifteenth St. N.W.  
13 Washington, D.C. 20005  
14 (202) 879-5078  
15 [eugene.assaf@kirkland.com](mailto:eugene.assaf@kirkland.com)  
16 [winn.allen@kirkland.com](mailto:winn.allen@kirkland.com)

17 Douglas H. Meal, MA Bar 340971 (*Pro Hac Vice*)  
18 Ropes & Gray, LLP  
19 Prudential Tower, 800 Boylston Street  
20 Boston, MA 02199-3600  
21 (617) 951-7517  
22 [douglas.meal@ropesgray.com](mailto:douglas.meal@ropesgray.com)

23 Attorneys for Defendants

24 **IN THE UNITED STATES DISTRICT COURT**  
25 **FOR THE DISTRICT OF ARIZONA**

26 Federal Trade Commission,

27 Plaintiff,

28 vs.

Wyndham Worldwide Corporation, et.  
al.,

Defendants.

Case No. CV 12-1365-PHX-PGR

**MOTION TO DISMISS BY  
DEFENDANT WYNDHAM HOTELS  
& RESORTS LLC**

**ORAL ARGUMENT REQUESTED**

## INTRODUCTION

1  
2 From 2008 to 2010, cyber criminals (allegedly from Russia) three times hacked  
3 into Wyndham Hotel and Resorts LLC's ("WHR's") computer network and the  
4 separate networks maintained by several independently owned hotels licensed to use the  
5 "Wyndham Hotels" brand. In response to these crimes, WHR alerted authorities,  
6 retained computer forensic experts, and implemented significant remedial measures. To  
7 WHR's knowledge, these criminals were never apprehended by authorities and no hotel  
8 guest suffered financial injury as a result of these crimes. Notwithstanding that WHR  
9 was a victim of hacking, the FTC has singled out WHR in this unprecedented litigation,  
10 claiming that WHR's cybersecurity practices are "unfair" and "unreasonable."

11 Hacking is an endemic problem. Media stories routinely appear about cyber  
12 attacks on private companies, including Google, Citibank, Microsoft, Sony, and many  
13 others, as well as government entities such as the CIA, DOD, NASA, FBI, and the FTC  
14 itself. To address pressing concerns of cybersecurity, Congress and the White House  
15 have made substantial efforts to enact various comprehensive cybersecurity laws—  
16 including the Cybersecurity Act of 2012—that would establish specific data-security  
17 standards for the private sector. The most recent efforts included a robust debate  
18 among the President, legislators, interest groups, and other stakeholders about the law's  
19 proper scope and the potential costs it could impose on private businesses. While the  
20 Cybersecurity Act failed to pass the Senate in August 2012, the White House has  
21 announced that it may issue an Executive Order addressing cybersecurity.

22 The FTC has not waited for Congress or the President. Instead of allowing the  
23 political process to settle the debate over the costs and benefits of cybersecurity policy,  
24 the FTC filed this action under Section 5 of the FTC Act, which forbids "unfair or  
25 deceptive" trade practices. WHR does not dispute that the FTC can bring enforcement  
26 actions against companies that make "deceptive" statements to consumers. But the  
27 Commission is attempting to do much more than that in this case. Relying on Section  
28 5's prohibition on "unfair" trade practices—which has traditionally been read to

1 prohibit certain unconscionable or oppressive acts toward consumers—the FTC  
2 assumes that it has the statutory authority to do that which Congress has refused:  
3 establish data-security standards for the private sector and enforce those standards in  
4 federal court. But the FTC previously disclaimed the very authority it purports to wield  
5 here. In a report issued in 2000, the FTC acknowledged that it lacked authority to  
6 require firms to adopt specific data-security practices, and it asked Congress for  
7 legislation that would grant it that authority. *See infra* at 6-7. Although Congress never  
8 responded to that request, the FTC “decided to move forward on its own without any  
9 new, specific privacy laws or delegation of authority from Congress.” M. Scott, *The*  
10 *FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has The*  
11 *Commission Gone Too Far?*, 60 Admin. L. Rev. 127, 143 (2008).

12       Nothing in Section 5 gives the FTC the power to set standards for the extremely  
13 complex computer software and hardware systems that businesses employ to ensure  
14 data security. And no court has *ever* held that the “unfairness” prong of Section 5 gives  
15 the Commission the authority to regulate a private company’s data-security practices.  
16 Indeed, it is inconceivable that Congress would have delegated a policy choice of such  
17 significant political and economic consequence to the FTC through a statute that does  
18 no more than forbid “unfair” trade practices—“[Congress] does not, one might say, hide  
19 elephants in mouseholes.” *Whitman v. Am. Trucking Ass’ns, Inc.*, 531 U.S. 457, 468  
20 (2001). Confirming that intuition, Congress has enacted no less than 10 federal statutes  
21 prescribing specific data-security standards for elements of the private sector. None  
22 grants the FTC the authority it claims here. Those subsequent acts shape the meaning  
23 of Section 5 and confirm that the statute’s reference to “unfair” practices does not  
24 empower the FTC to oversee the data-security practices of private companies. As  
25 recently put in the *Wall Street Journal*, “[u]sing consumer protection laws to address  
26 cyber vulnerabilities is stretching the FTC’s mission beyond recognition.” Michael  
27 Chertoff, *The Lesson of Google’s Safari Hack*, *Wall Street Journal* (July 22, 2012),  
28

1 available at <http://online.wsj.com/article/SB10001424052702303933704577532>  
2 572854142492.html.

3 Indeed, the FTC's approach to data-security regulation in this very case only  
4 confirms that the Commission has neither the expertise nor the statutory authority to  
5 establish data-security standards for the private sector. The FTC has not published *any*  
6 rules or regulations that might provide the business community with *ex ante* notice of  
7 what data-security protections a company must employ to be in compliance with the  
8 law. *See* Scott, 60 Admin. L. Rev. at 143-144 (there are no "rulemaking proceedings,  
9 policy statements or guidelines from the Commission explaining what conduct ... it  
10 deems 'unreasonable,' and hence actionable"). Instead, the FTC is enforcing its vision  
11 of data-security policy through this selective, *ex post* enforcement action, which seeks  
12 to hold WHR liable without any fair notice as to what the law required. Moreover, after  
13 a two-year investigation into WHR's data-security practices, the FTC is still unable to  
14 allege anything more specific than that WHR failed to employ protections that were  
15 "reasonable," "appropriate," "adequate," or "proper." The FTC's inability or  
16 unwillingness to state precisely what WHR did wrong—or to tell others in the business  
17 community what they must do to avoid similar lawsuits in the future—confirms that the  
18 Commission has no business trying to regulate data-security practices under the  
19 "unfairness" prong of the FTC Act.

20 The implications of the FTC's legal theories in this case are far-reaching.  
21 American businesses already face a dizzying array of specific federal statutes regarding  
22 data security—but WHR is not alleged to have violated any of those specific statutes.  
23 Instead, despite having previously conceded that it lacks authority to regulate data  
24 security, the FTC is now seeking judicial approval to extend its statutory power beyond  
25 what Congress has allowed and into highly technical areas where the FTC has no  
26 regulatory expertise. The FTC's approach would subject businesses to vague,  
27 unpublished, and uncertain requirements that would drastically alter the competitive  
28

1 landscape—without Congress or the President actually settling the debate about the  
2 costs and benefits of data security for American businesses.

### 3 **BACKGROUND**

4 WHR is a hospitality company that provides services to hotels operating under  
5 the “Wyndham Hotels” brand name (the “Wyndham-branded hotels”), a full-service  
6 hotel chain with over 70 locations in the United States. Am. Compl. ¶ 9. With few  
7 exceptions, each Wyndham-branded hotel is independently owned by a third party  
8 unaffiliated with WHR or the other defendants. *Id.* Most of those independent owners  
9 are authorized to use the “Wyndham Hotels” brand name pursuant to franchise  
10 agreements with WHR, through which WHR licenses the use of the brand name and  
11 agrees to provide services to the franchisee, who retains day-to-day responsibility for  
12 the hotel. *Id.* Other independent owners entered into management agreements with  
13 Wyndham Hotel Management, Inc. (“WHM”). *Id.* ¶ 10.

14 WHR maintains and operates a computer network that it uses to provide services  
15 to the Wyndham-branded hotels. *Id.* ¶ 16. Each Wyndham-branded hotel maintains  
16 and operates its own computer network that is separate from, but linked to, WHR’s  
17 network. *Id.* ¶ 15. On three occasions from 2008 to 2010, criminal hackers gained  
18 unauthorized access into WHR’s computer network and into the separate computer  
19 networks of several Wyndham-branded hotels. *Id.* ¶ 25. The intrusions into the  
20 Wyndham-branded hotels’ networks may have resulted in the hackers stealing payment  
21 card data that the independent hotel owners had collected from their guests. *Id.*  
22 Significantly, the FTC does not allege that the hackers stole (or even had access to) any  
23 payment card data collected by WHR.

24 The FTC alleges that WHR violated Section 5 of the FTC Act—which forbids  
25 “unfair or deceptive acts or practices in or affecting commerce,” 15 U.S.C. § 45(a)(1)—  
26 by not maintaining “reasonable and appropriate” data-security protections. Am. Compl.  
27 ¶ 1. Although no court has ever construed Section 5 to apply to a private company’s  
28 data-security practices, the FTC advances two legal theories for its novel construction

1 of the Act. Count I relies on Section 5’s prohibition on “decepti[ve]” practices and  
2 alleges that WHR deceived consumers by stating on its website that it used  
3 “commercially reasonable efforts” to secure payment card data that it collected. *Id.* ¶¶  
4 21, 44-46. Count II, in contrast, alleges that WHR’s data-security protections amounted  
5 to “unfair” trade practices under Section 5 because those practices were not “reasonable  
6 and appropriate.” *Id.* ¶¶ 47-49.

### 7 ARGUMENT

8 This case is a classic example of agency overreaching. The FTC’s Count II  
9 “unfairness” claim—which this brief addresses first—stretches far beyond the  
10 traditional bounds of the Commission’s authority. Nothing in the text or history of  
11 Section 5 purports to give the Commission authority to decide whether data-security  
12 protections are “unfair,” “reasonable,” or “appropriate,” and Congress’s repeated  
13 enactment of specific data-security statutes (and failed attempts to enact comprehensive  
14 data-security laws) confirm that the statute cannot be construed so broadly. Simply put,  
15 Section 5’s prohibition on “unfair” trade practices does not give the FTC authority to  
16 regulate the data-security practices of private companies.

17 Although more securely grounded in the requirements of the statute, the FTC’s  
18 Count I “deception” claim—which relies exclusively on certain statements in WHR’s  
19 online privacy policy—must also be dismissed. As alleged, the only information  
20 compromised during the criminal cyber attacks was certain payment card data collected  
21 by independent Wyndham-branded hotels—no data collected *by WHR* was ever placed  
22 at risk. Numerous sections of the privacy policy make abundantly clear that WHR  
23 made *no representations at all* about the security of data collected by the independent  
24 Wyndham-branded hotels. And to the extent the FTC purports to allege that WHR’s  
25 representations regarding its own data-security practices were deceptive, those  
26 allegations fall well short of the heightened pleading requirements of Rule 9(b).

## I. THE COUNT II UNFAIRNESS CLAIM MUST BE DISMISSED

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

“Regardless of how serious the problem an administrative agency seeks to address, ... it may not exercise its authority in a manner that is inconsistent with the administrative structure that Congress enacted into law.” *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000) (quotation marks omitted). That perfectly describes the FTC’s complaint in this case. In delegating to the FTC authority to regulate “unfair .... acts or practices,” Congress clearly did not authorize the FTC to regulate anything and everything that the Commission might deem “unfair.” To the contrary, the reach of the FTC’s authority is necessarily limited by Section 5’s text, history, and “place in the overall statutory scheme.” *Id.* at 133.

Nothing in the plain text of Section 5 suggests that Congress gave the FTC authority to regulate data security, which is itself strong evidence that no such authority exists. *Whitman*, 531 U.S. at 468 (“[Congress] does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions.”). Section 5’s legislative history also confirms that no such delegation was intended. Since its enactment in 1914, Section 5 has consistently been understood to give the FTC power to forbid certain “unfair” practices; but in enacting Section 5, Congress also thought the FTC would “have *no power* to prescribe the methods of competition to be used in the future.” 51 Cong. Rec. 14932 (1914) (emphasis added); *see also FTC v. Sinclair Ref. Co.*, 261 U.S. 463, 475 (1923) (“[The FTC] has no general authority to compel competitors to a common level, to interfere with ordinary business methods or to prescribe arbitrary standards for those engaged in ... competition.”).

Indeed, until quite recently, the FTC specifically *disclaimed* the authority to mandate data-security standards through Section 5’s “unfair ... practices” language. In a 2000 report on information security, the FTC requested broader legislation requiring websites to “take reasonable steps to protect the security of the information they collect from consumers” and “provid[ing] an implementing agency with the authority to



1 promulgate more detailed standards pursuant to the Administrative Procedure Act.”  
2 FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, May  
3 2000, at 36-37, available at <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.  
4 Such legislation was necessary, the Report concluded, because “the Commission *lacks*  
5 *authority to require firms to adopt information practice policies.*” *Id.* at 34 (emphasis  
6 added); see also Scott, 60 Admin. L. Rev. at 130-31 (“In its 2000 Report, the  
7 Commission indicated that ... it could not require companies to adopt privacy policies  
8 [and] proposed legislation that would provide it with the authority to issue and enforce  
9 specific privacy regulations.”).<sup>1</sup> Since that time, the FTC has made an about-face: now  
10 the Commission says that its jurisdiction over “unfair” practices *does* give it authority  
11 to mandate that companies adopt certain data-security practices.

12 The FTC’s initial view reflected the correct understanding of Congressional  
13 intent. As the Supreme Court has explained, subsequently enacted laws “shape or focus  
14 [the] meaning[.]” of ambiguous statutes, “particularly ... where the scope of the earlier  
15 statute is broad but the subsequent statutes more specifically address the topic at hand.”  
16 *Brown & Williamson*, 529 U.S. at 143. Here, the vast array of more-specific laws  
17 governing data security preclude an interpretation of Section 5 that would grant the  
18 FTC jurisdiction to regulate data-security practices. For example:

- 19 • The Fair Credit Reporting Act (“FCRA”), Pub. L. 108-159, 117 Stat. 1953,  
20 codified at 15 U.S.C. § 1681 *et seq.*, imposes requirements for the collection,  
21 disclosure, and disposal of data collected by consumer reporting agencies and  
22 requires the FTC and other agencies to develop rules for financial institutions to  
23 reduce the incidence of identity theft.
- The Gramm-Leach-Bliley Act (“GLBA”), Pub. L. 106-102, 113 Stat. 1338,  
codified at 15 U.S.C. § 6801 *et seq.*, mandates data-security requirements for  
financial institutions, and instructs the FTC and federal banking agencies to

---

24 <sup>1</sup> Other FTC officials have echoed the view that the Commission lacks authority to  
25 require private companies to implement certain data-security protections. See Jeffrey  
26 Benner, *FTC Powerless to Protect Privacy*, *Wired*, May 31, 2001, available at  
27 [www.wired.com/politics/security/news/2001/05/44173](http://www.wired.com/politics/security/news/2001/05/44173) (“But according to FTC, it  
28 doesn’t have that kind of power. The agency can order a company to make its stated  
policy align with practice, but it cannot dictate what those practices will be, or prevent  
it from changing a policy. ‘The agency’s jurisdiction is (over) deception,’ Lee Peeler,  
the FTC’s associate director for advertising practices, said. ‘If a practice isn’t  
deceptive, we can’t prohibit them from collecting information. The agency doesn’t  
have the jurisdiction to enforce privacy.’”).



1 establish standards for financial institutions “to protect against unauthorized access  
2 to or use of such records or information.” 15 U.S.C. § 6801(b)(3).

- 3 • The Children’s Online Privacy Protection Act (“COPPA”), Pub. L. 105-277, 112  
4 Stat. 2581-728, codified at 15 U.S.C. § 6501 *et seq.*, requires covered website  
5 operators to establish and maintain reasonable procedures to protect the  
6 confidentiality and security of information gathered from children.
- 7 • The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Pub.  
8 L. No. 104-191, codified at 45 U.S.C. § 1320d *et seq.*, requires health care  
9 providers to maintain security standards for electronic health information.
- 10 • The Health Information Technology for Economic and Clinical Health Act  
11 (“HITECH Act”), Pub. L. No. 111-5, 123 Stat. 115, codified at 42 U.S.C. § 17921  
12 *et seq.*, requires regulated entities to provide notice of unsecured breaches of health  
13 information in certain circumstances and strengthens protections for such data.
- 14 • The Cable Television Consumer Protection and Competition Act, Pub. L. No. 102-  
15 385, 106 Stat. 1460, codified at 42 U.S.C. § 551, requires cable companies to take  
16 steps to prevent unauthorized access to the certain subscriber information.<sup>2</sup>

17 Significantly, several of these laws, including the FCRA, GLBA, and COPPA,  
18 grant the FTC authority to regulate data-security standards—but *only* in certain specific,  
19 limited contexts. Those statutes are powerful evidence that the FTC lacks authority to  
20 regulate data-security practices in cases (like this one) that fall outside the confines of  
21 those narrow delegations. Indeed, if Section 5’s prohibition on “unfair” practices grants  
22 the FTC the broad authority it claims in this case, then those statutes would have been  
23 entirely superfluous. By delegating certain limited authority to the FTC, Congress has  
24 foreclosed any interpretation of Section 5 that would give the Commission overarching  
25 authority to set data-security standards for the private sector.

26 Courts, moreover, “must be guided to a degree by common sense as to the  
27 manner in which Congress is likely to delegate a policy decision of such economic and  
28 political magnitude to an administrative agency.” *Brown & Williamson*, 529 U.S. at  
133. Establishing substantive data-security standards for private companies has been a  
topic of intense debate among members of Congress, the Executive Branch, interest  
groups, and relevant stakeholders. No less than eight data-security bills were

---

<sup>2</sup> These laws are only the tip of the iceberg. *See also, e.g.*, Video Privacy Protection Act, Pub. L. 100-618 (1988); Driver’s Privacy Protection Act of 1994, Pub. L. 103-322; Computer Fraud Abuse Act of 1986, codified as amended at 18 U.S.C. § 1030 *et seq.*

1 introduced in 2011 alone,<sup>3</sup> including bills that would have expressly given the FTC the  
2 very power that it claims in this litigation. None was enacted. More recently, in a very  
3 high-profile and well-publicized debate, Congress considered (and rejected) the  
4 Cybersecurity Act of 2012, S. 2105, 112th Cong. (Feb. 14, 2012), which would have  
5 created comprehensive “cybersecurity performance requirements” for the private sector.  
6 *Id.* § 104. In light of the important economic and political considerations involved in  
7 establishing data-security standards for the private sector, and the intense political  
8 debate that has surrounded efforts to establish such standards, it offends common sense  
9 to think that Congress would have delegated that responsibility to the FTC—  
10 particularly through a century-old statute that does nothing more than forbid “unfair”  
11 practices. “Congress could not have intended to delegate a decision of such economic  
12 and political significance to an agency in so cryptic a fashion.” *Brown & Williamson*,  
13 529 U.S. at 160; *see Gonzales v. Oregon*, 546 U.S. 243, 267 (2006) (rejecting the “idea  
14 that Congress gave the Attorney General such broad and unusual authority through an  
15 implicit delegation”); *Whitman*, 531 U.S. at 468 (stating that it is “implausible that  
16 Congress would give to the EPA through ... modest words the power to determine  
17 whether implementation costs should moderate national air quality standards”).

18 Nor is it conceivable that Congress, through implication, would have delegated  
19 the task of mandating affirmative data-security requirements *to the FTC*—an agency  
20 that has no particular expertise in either the policy or technology of data-security issues.  
21 Congress delegates legislative authority primarily to harness the “relative expertness”  
22 that a specialized agency can bring to bear on a subject matter. *United States v. Mead*  
23 *Corp.*, 533 U.S. 218, 228 (2001). The FTC’s expertise, however, is in evaluating fair  
24 competition and consumer fraud and deception—not in establishing and enforcing

---

26 <sup>3</sup>See Personal Data Privacy and Security Act of 2011, S. 1151; Data Security and  
27 Breach Notification Act of 2011, S. 1207; Data Breach Notification Act of 2011, S.  
28 1408; Data Security Act of 2011, S. 1434; Personal Data Protection and Breach  
Accountability Act of 2011, S. 1535; Data Accountability and Trust Act, H.R. 1707  
(2011); Data Accountability and Trust Act of 2011, H.R. 1841; Secure and Fortify  
Electronic Data Act, H.R. 2577 (2011).

1 cybersecurity standards for the private sector. For proof of that, the Court need look no  
2 further than the FTC's Amended Complaint in this case. After a two-year investigation  
3 into WHR's data-security practices, the FTC is unable to allege anything more specific  
4 than that WHR failed to employ practices that were "reasonable," "appropriate,"  
5 "adequate," or "proper." If an agency can provide no more guidance than that, then it  
6 has no business attempting to regulate data-security practices in the first-place. There  
7 is, in short, little reason to think that Congress would have wanted the FTC to play such  
8 a critical role in an area so far afield from its core competencies.

9 In the end, this case is analogous to *Brown & Williamson*, in which the Supreme  
10 Court rejected the FDA's attempt to regulate tobacco products under the Federal Drug  
11 and Cosmetics Act because Congress had subsequently enacted tobacco-specific  
12 legislation. 529 U.S. 120. As in *Brown & Williamson*, "Congress has enacted several  
13 statutes addressing the particular subject of [data security]" and has done so "against the  
14 background" of the FTC asserting that it "lacks jurisdiction" to mandate data-security  
15 practices. *Id.* at 155-56. "Under these circumstances, it is clear that Congress' [data-  
16 security-specific] legislation has effectively ratified the [FTC's] previous position that it  
17 lacks jurisdiction to regulate [data security]." *Id.* at 156.

18 **B. Even Assuming the FTC Could Regulate Data Security, Any Such**  
19 **Requirements Would Have To Be Established Through Rulemaking.**

20 For these reasons, Section 5 does not give the FTC authority to mandate data-  
21 security standards for the private sector. But even if it did, the FTC would have to  
22 establish data-security standards *ex ante* through rulemaking, rather than *ex post*  
23 through a selective enforcement action.

24 Although agencies have some discretion to make law through the adjudicative  
25 process, the Supreme Court and the Ninth Circuit have recognized important limits on  
26 that discretion that stem from fundamental notions of fair notice and due process. Thus,  
27 when an agency tries to use an adjudication to announce new principles of law that  
28 could have widespread application, the agency has abused its authority by forgoing *ex*

1 *ante* rulemaking in favor of *ex post* adjudication. See *Ford Motor Co. v. FTC*, 673 F.2d  
2 1008 (9th Cir. 1981); *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 294 (1974). In *Ford*  
3 *Motor Co.*, for example, the Ninth Circuit invalidated the FTC’s attempt to use an  
4 adjudication to announce for the first time that a dealership’s practice of repossessing  
5 cars could violate Section 5. The FTC’s adjudication, the court held, (1) established  
6 new law without notice, as it was “the first [relevant] agency action against a dealer,”  
7 and (2) had “general application” because “practices similar to those [found unlawful]  
8 [were] widespread in the car dealership industry,” *Ford Motor Co.*, 673 F.2d. at 1010.  
9 If the FTC was going to regulate in that area at all, it had to do so through rulemaking.

10 The same is true in this case. If the Court were to hold that the FTC has  
11 authority to mandate data-security standards for the private sector under Section 5, that  
12 holding would amount to a clear departure from existing law. And that departure would  
13 have widespread application: every U.S. business that collects data from consumers  
14 would be required to implement what the FTC mandates. Thus, even if Section 5 could  
15 be construed to give the FTC authority over data-security practices, the FTC would be  
16 obligated to exercise that authority through rulemaking, not through adjudication. See  
17 *id.*; *Patel v. INS*, 638 F.2d 1199, 1204-05 (9th Cir. 1980).

18 Indeed, permitting the FTC to impose general data-security standards on WHR  
19 in this case would raise serious constitutional questions of fair notice and due process.  
20 It is a bedrock principle of constitutional law that a defendant must be given fair notice  
21 of what the law requires before it can be held liable for its violation. See *United States*  
22 *v. Wunsch*, 84 F.3d 1110, 1119 (9th Cir. 1996); see also *General Elec. Co. v. EPA*, 53  
23 F.3d 1328-29 (D.C. Cir. 1995). Section 5 by itself clearly provides no notice as to what  
24 data-security practices a company must adopt to be in compliance with the statute. And  
25 the FTC has not issued *any* rules, regulations, or other guidance that would provide  
26 such notice. In the absence of any affirmative guidance as to what Section 5 requires in  
27 the world of data security, WHR cannot reasonably (or constitutionally) be found to  
28 have violated any of the FTC’s *post-hoc* data-security standards.

### C. Section 5 Does Not Govern The Security of Payment Card Data

Even if Section 5 could be construed to give the FTC authority over some aspects of data security, the statute clearly cannot be stretched so far as to authorize the FTC to regulate the security of consumer payment card data. Under the statute, a practice can be found unfair only if it “causes or is likely to cause *substantial injury to consumers* which is *not reasonably avoidable* by consumers themselves.” 15 U.S.C. § 45(n) (emphasis added). But, because of the special nature of payment card data, consumer injury from the theft of such data is always avoidable and never substantial. Federal law places a \$50 limit on the amount for which a consumer can be liable for the unauthorized use of a payment card. *See Id.* § 1643(a)(1)(B). And all major card brands have adopted policies that waive liability for even that small amount.<sup>4</sup> Thus consumers can always “reasonably avoid” any financial injury stemming from the theft of payment card data simply by having their issuer rescind any unauthorized charges.

Indeed, at least one FTC Commissioner has taken the view that the FTC cannot use its “unfairness” authority to regulate most data-security practices because the consumer harm involved is “intangible.” *See* Dissenting Statement of J. Thomas Rosch, *Protective Consumer Privacy in an Era of Rapid Change*, at C-4 (March 26, 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>. As Commissioner Rosch explained, use of the FTC’s “unfairness” authority in that fashion “goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).”

---

<sup>4</sup> *See* Visa, [http://usa.visa.com/personal/security/visa\\_security\\_program/zero\\_liability.html](http://usa.visa.com/personal/security/visa_security_program/zero_liability.html) (“zero liability” for unauthorized card use); MasterCard, <http://www.mastercard.us/zero-liability.html> (same); Discover, <http://www.discovercard.com/customer-service/fraud/protect-yourself.html> (same); American Express, [https://www212.americanexpress.com/dsmlive/dsm/dom/us/en/fraudprotectioncenter/fraudprotectioncenter\\_purchaseprotection.do?vgnextoid126e0918a025c110VgnVCM200000d0faad94RCRD&vgnnextchannel=9ee6d6954360c110VgnVCM100000defaad94RCRD&appinstancename=default](https://www212.americanexpress.com/dsmlive/dsm/dom/us/en/fraudprotectioncenter/fraudprotectioncenter_purchaseprotection.do?vgnextoid126e0918a025c110VgnVCM200000d0faad94RCRD&vgnnextchannel=9ee6d6954360c110VgnVCM100000defaad94RCRD&appinstancename=default) (same) (all last visited Aug. 22, 2012).

1 *Id.* at C-5. Adhering to that view, Commissioner Rosch dissented from the FTC’s  
2 decision to include an “unfairness” claim in its complaint in this case.<sup>5</sup>

3 Even if Section 5 could be construed to mandate certain data-security  
4 requirements for payment card data, the standard of liability for failing to protect that  
5 data would be demanding and far above what the FTC has alleged in this case. By  
6 statutory command, the requirements imposed by Section 5 must be balanced against  
7 the risk of consumer injury. *See* 15 U.S.C. § 45(n). And because the risk of consumer  
8 injury posed by the theft of payment card data is either non-existent or, at a minimum,  
9 exceedingly small, the standard of liability for failing to adequately protect such data  
10 would have to be correspondingly high. That is precisely why courts examining data-  
11 security issues under state unfair-trade-practices statutes have held that such practices  
12 are unfair only when they are egregious or “reckless” in nature. *See, e.g., Worix v.*  
13 *MedAssets, Inc.*, 2012 WL 1419257, at \*6 (N.D. Ill. Apr. 24, 2012). The FTC, of  
14 course, does not allege such recklessness or egregiousness here.

15 As support for its novel theory of Section 5’s “unfairness” authority, the FTC is  
16 likely to rely on *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010). That case, however,  
17 is of no help to the FTC here. *Neovi* involved a website—Qchex.com—that provided  
18 software allowing registered users to electronically draw checks from their bank  
19 account and to transmit those checks to third parties. The website quickly became a  
20 tool for “con artists and fraudsters.” *Id.* at 1154. Having stolen names and bank  
21 account information via other means, these fraudsters would open accounts on  
22 Qchex.com and draw funds from bank accounts that they did not own. *Id.* Because it  
23 “facilitated and provided substantial assistance” to those fraudulent activities, *id.* at  
24 1156, Oxchex was found liable under the FTC Act.

25 The FTC’s theory of liability here is much different. *Neovi*, to begin, was not a  
26 data-security case: Qchex was liable not because it failed to secure sensitive consumer  
27

---

28 <sup>5</sup> *See* FTC Press Release, *FTC Files Complaint Against Wyndham Hotels* (June 26,  
2012), available at <http://www.ftc.gov/opa/2012/06/wyndham.shtm>.



1 data that it had collected (which is the FTC’s theory in this case), but because its  
2 software allowed fraudsters to exploit data that they previously had stolen *from other*  
3 *entities*. The case thus cannot, and does not, support the FTC’s attempt to extend its  
4 unfairness jurisdiction to regulating data-security practices. In addition, *Neovi* did not  
5 involve the use of payment card data, and thus the Ninth Circuit had no occasion to  
6 consider how and whether Section 5 should apply to security for such data. Finally,  
7 *Neovi* presented exactly the kind of egregious conduct that traditionally has been the  
8 subject of Section 5 litigation. In the website’s six-year existence, over 13,750  
9 fraudulent accounts were opened, nearly 155,000 fraudulent checks were issued, and  
10 more than *\$400 million* in fraudulent funds were drawn from consumers’ accounts—an  
11 amount that was *more than half* of the total funds that were drawn using Qcheck.com.  
12 *Id.* at 1154. That conduct cannot sensibly be compared to that of WHR in this case.

#### 13 **D. The Unfairness Count Fails Federal Pleadings Requirements.**

14 Finally, the Amended Complaint should be dismissed for the independent reason  
15 that it fails to satisfy basic federal-pleading requirements. *See Ashcroft v. Iqbal*, 556  
16 U.S. 662, 678 (2009). The Amended Complaint criticizes WHR for failing to employ  
17 practices that were “readily available,” “adequate,” “commonly-used,” and “proper.”  
18 Am. Compl. ¶¶ 24. But nowhere does the FTC give any factual detail as to what  
19 procedures, or combination of procedures, would have met those conclusory standards.  
20 For example, the FTC alleges that defendants “failed to ensure the Wyndham-branded  
21 hotels implemented adequate information security policies,” *id.* ¶ 24(c), but never states  
22 what policies would be “adequate.” It criticizes defendants’ operating systems as  
23 “outdated,” *id.* ¶ 24(d), but fails to allege what alternative systems would be current.  
24 And it states that defendants “failed to employ reasonable measures to detect and  
25 prevent unauthorized access,” *id.* ¶ 24(h), but does not explain what measures would be  
26 “reasonable”—now or when the alleged breaches occurred. Simply put, the FTC’s  
27 allegations are nothing more than “legal conclusions couched as factual allegations”  
28



1 and do not state a plausible claim for relief. *Worden v. Fed. Home Loan Mortg. Corp.*,  
2 2010 WL 2292943 (D. Ariz. June 8 2010).

## 3 **II. THE COUNT I DECEPTION CLAIM FAILS AS A MATTER OF LAW**

4 The FTC's Count I deception claim fares no better than its Count II unfairness  
5 claim. To impose liability under the "deception" prong of Section 5, the FTC must  
6 identify (1) a representation; that (2) is "likely to mislead consumers acting reasonably  
7 under the circumstances;" that (3) is "material." *FTC v. Stefanchik*, 559 F.3d 924, 928  
8 (9th Cir. 2009). Because such a claim "sounds in fraud," the FTC must meet the  
9 heightened pleading requirements of Rule 9(b) when alleging unlawful deception. *FTC*  
10 *v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 853 (C.D. Cal. 2010); *FTC v. Ivy Capital,*  
11 *Inc.*, 2011 WL 2118626, at \*3 (D. Nev. May 25, 2011).

12 As the sole basis for its claim, the FTC alleges that WHR deceived consumers  
13 because its online privacy policy stated that it used "industry standard practices" and  
14 "commercially reasonable efforts" to secure the payment card data that it collected. *See*  
15 Ex. 1, Allen Decl., Ex. A, at 1.<sup>6</sup> Those statements were deceptive, the FTC claims,  
16 because WHR failed to implement "reasonable and appropriate measures" to protect the  
17 payment card data collected by the Wyndham-branded hotels. Am. Compl. ¶ 45. But  
18 there is a clear disconnect in those allegations—namely, the FTC fails to recognize the  
19 fundamental distinction between data collected by WHR itself (to which the privacy  
20 policy applies) and data collected by the independently owned Wyndham branded  
21 hotels (to which the privacy policy expressly does not apply.)

22 WHR and the independently owned Wyndham-branded hotels each engage in  
23 their own separate data-collection and storage practices. As a franchisor, WHR collects  
24 payment card data through its centralized reservations service—which permits guests to  
25 book hotel rooms either online or over the phone—and stores that information on its

---

26 <sup>6</sup> "Consideration of materials incorporated by reference in the complaint is permitted  
27 when plaintiff's claim depends on the contents of a document, the defendant attaches  
28 the document to its motion to dismiss, and the parties do not dispute the authenticity of  
the document." *Spinedex Physical Therapy USA, Inc. v. United Healthcare of Ariz.,*  
*Inc.*, 661 F. Supp. 2d 1076, 1083 (D. Ariz. 2009).

1 corporate network. *See* Allen Decl., Ex. A, at 2. In addition, and separate and apart  
2 from WHR’s practices, the independently owned hotels also collect payment card data  
3 and store that data on their local networks. *Id.* at 4.

4 As the text of the WHR privacy policy makes abundantly clear, the policy  
5 applies only to the security of payment card data collected by WHR and does not  
6 purport to say anything at all about the security of payment card data collected by the  
7 Wyndham-branded hotels. Thus, the privacy policy consistently uses the terms “we,”  
8 “us,” or “our” when making representations about WHR’s data-security practices, and  
9 specifically defines those terms to *exclude* the Wyndham-branded hotels. *Id.* at 1. The  
10 policy also expressly caveats each representation about data-security by explaining that  
11 those representations apply only to “our collection” of data and only “to the extent we  
12 control the Information”—caveats that plainly exclude any data collected by the  
13 Wyndham-branded hotels. *Id.* And if all of that were not enough, the privacy policy  
14 includes a separately-titled section—which the FTC conveniently omitted from its  
15 quotation of WHR’s privacy policy in the Amended Complaint—that explains the  
16 policy makes *no representations* about the security of data collected by franchisees:

17 **Our Franchisees.**

18 Each Brand hotel is owned and operated by an independent  
19 Franchisee that is neither owned nor controlled by us or our  
20 affiliates. Each Franchisee collects Customer Information and  
21 uses the Information for its own purposes. We do not control the  
22 use of this Information or access to the Information by the  
23 Franchisee and its associates. The Franchisee is the merchant who  
24 collects and processes credit card information and receives  
25 payment for the hotel services. The Franchisee is subject to the  
26 merchant rules of the credit card processors it selects, which  
27 establish its card security rules and procedures.

28 *Id.* at 4. Thus, evaluating the “net impression” of the privacy policy and construing the  
policy “as a whole,” *FTC v. Connelly*, 2006 WL 6267337, at \*10 (C.D. Cal. Dec. 20,  
2006), any reasonable consumer would have understood that the policy was making  
statements only about data collected by WHR, and not about the security of data  
collected by independently-owned Wyndham-branded hotels.



1 DATED this 27th day of August, 2012.

2 OSBORN MALEDON, P.A.

3 By s/David B. Rosenbaum

4 David B. Rosenbaum  
5 Anne M. Chapman  
6 2929 North Central Avenue, Suite 2100  
7 Phoenix, Arizona 85012-2794

8 Eugene F. Assaf, P.C., 449778, *pro hac vice*  
9 K. Winn Allen, 1000590, *pro hac vice*  
10 Kirkland & Ellis LLP  
11 655 Fifteenth Street, N.W.  
12 Washington, D.C. 20005

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

17 Attorneys for Defendants  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**CERTIFICATE OF SERVICE**

I hereby certify that on August 27, 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 the following CM/ECF registrants:

- **Kristin Krause Cohen;** [kcohen@ftc.gov](mailto:kcohen@ftc.gov)
- **John Andrew Krebs;** [jkrebs@ftc.gov](mailto:jkrebs@ftc.gov)
- **Katherine E McCarron;** [kmccarron@ftc.gov](mailto:kmccarron@ftc.gov)
- **Kevin H Moriarty;** [kmoriarty@ftc.gov](mailto:kmoriarty@ftc.gov)
- **Lisa Naomi Weintraub Schifferle;** [lschifferle@ftc.gov](mailto:lschifferle@ftc.gov)
- **Andrea V. Arias;** [aarias@ftc.gov](mailto:aarias@ftc.gov)

Attorneys for Plaintiff, Federal Trade Commission

s/Kelly Dourlein \_\_\_\_\_