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

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice to be filed
K. Winn Allen, DC Bar 1000590
Pro Hac Vice to be filed
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 to be filed
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 NEW JERSEY

FEDERAL TRADE COMMISSION Plaintiff, v. WYNDHAM WORLDWIDE CORPORATION, et al., Defendants.	Civil Action No.: 2:13-cv-01887-ES-SCM **MOTION TO DISMISS BY DEFENDANT WYNDHAM HOTELS & RESORTS LLC** **ORAL ARGUMENT REQUESTED** **MOTION DATE JUNE 17, 2013**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

This is an unprecedented lawsuit with far-reaching implications. For the first time ever, the FTC is asking a federal court to hold that Section 5 of the FTC Act—a 1914 statute that prohibits "unfair and deceptive acts or practices"—authorizes the Commission to regulate the sophisticated technologies that businesses use to protect sensitive consumer information. Large and small businesses already are subject to a dizzying array of federal statutes that establish data-security standards in specific sectors of the economy. None of those statutes, however, apply in this case. Notwithstanding that statutory silence, the FTC argues that the general language of Section 5 gives it the broad authority to set data-security standards for ***any*** American business operating in ***any*** industry. No court has ever held that Section 5 gives the FTC such unbounded authority.

Hacking is an endemic problem. Media stories routinely appear about cyberattacks on private companies, including Facebook, Google, Apple, Citibank, Microsoft, Sony, and many others, as well as government entities such as the CIA, DOD, NASA, FBI, and the FTC itself. The hospitality industry has not been immune to such attacks. From 2008 to 2010, cybercriminals (allegedly from Russia) three times hacked into Wyndham Hotel and Resorts LLC's ("WHR's") computer network and the separate computer networks of several independently owned hotels licensed to use the "Wyndham Hotels" brand. WHR at the time had substantial security measures in place to protect its network against being hacked, and in response to the attacks, WHR alerted law enforcement agencies, retained computer forensic experts, and implemented significant remedial measures. To WHR's knowledge, no hotel guest suffered financial injury as a result of these crimes, and the cybercriminals responsible for the attacks have never been apprehended (or even seriously pursued) by law enforcement officials.

To address pressing concerns of cybersecurity, Congress and the President have made substantial efforts to enact laws that would establish specific data-security standards for the private

sector. Just last year, a comprehensive data-security law, the Cybersecurity Act of 2012, failed to pass the Senate despite extensive negotiations among the President, legislators, and scores of interest groups. In response, the President in February 2013 issued an Executive Order and a Presidential Policy Directive on cybersecurity issues, which require the development of minimum data-security standards for businesses operating critical-infrastructure systems or assets. In stark contrast to the FTC's approach to regulation in this case, however, the Executive Order requires the formulation of specific data-security standards far in advance of any regulatory enforcement efforts and after an open public comment and review process. For its part, Congress has continued to pursue cybersecurity legislation. Just last week the House of Representatives passed an entirely new cybersecurity bill, the Cyber Intelligence Sharing and Protection Act, which now is pending before the Senate Intelligence Committee.

The FTC is not waiting for the political process to determine the proper scope and contours of cybersecurity regulation. Notwithstanding that WHR was a victim of hacking, and notwithstanding the substantial data-security efforts WHR undertook both before and after attacks, the FTC brought this unprecedented lawsuit against WHR, claiming that the company—as opposed to the hackers themselves—should be held responsible for the attacks. Although no specific statute grants the FTC authority to establish and enforce data-security standards for the private sector, the Commission claims that such authority can be found in Section 5's general prohibition on "unfair and deceptive" trade practices—a provision that has traditionally been understood to forbid certain dishonest or unscrupulous business practices. WHR does not dispute that the FTC can bring enforcement actions against companies that make "deceptive" statements to consumers. But in this case the Commission is attempting to do much more than that. Relying on Section 5's prohibition on "unfair" trade practices, the FTC argues that it has the statutory authority to do what Congress has

refused: establish data-security standards for the private sector and enforce those standards in federal court.

That is an untenable theory of agency jurisdiction. The Supreme Court has consistently refused to construe broad and open-ended statutory language—such as the "unfairness" prohibition in Section 5—as empowering administrative agencies to impose sweeping new requirements on American businesses. "[Congress] does not, one might say, hide elephants in mouseholes." *Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 468 (2001). That is particularly true when 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. *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000). Congress has enacted no fewer than 10 federal statutes expressly authorizing particular agencies to establish data-security standards in certain narrow sectors of the economy. None of those laws grant the FTC the sweeping power to set data-security standards in ***all*** sectors of the economy. To the contrary, that statutory landscape only confirms that Section 5 should not be interpreted to grant the FTC a general police power over data-security matters. As one former government official recently explained, "[u]sing consumer protection laws to address cyber vulnerabilities is stretching the FTC's mission beyond recognition." Michael Chertoff, *The Lesson of Google's Safari Hack*, Wall Street Journal (July 22, 2012), *available at* http://online.wsj.com/article/SB10001424052702303933704577532572854142492.html.

The FTC ***itself*** previously agreed that it lacked the very authority that it purports to wield in this case. On multiple occasions in the 1990s and early 2000s, the FTC publicly acknowledged that it lacked authority to prescribe substantive data-security standards under Section 5. For that very reason, the FTC has repeatedly asked Congress over the past decade to enact legislation giving it such authority. Although Congress never granted that request, the FTC "decided to move forward

on its own without any new, specific privacy laws or delegation of authority from Congress." M. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has The Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 143 (2008).

The FTC's approach to data-security regulation in this case only confirms that the Commission has neither the expertise nor the statutory authority to establish data-security standards for the private sector. The FTC has not published ***any*** rules or regulations that might provide the business community with *ex ante* notice of what data-security protections a company must employ to comply with Section 5. *See, e.g.*, *id.* at 143-144 (there are no "rulemaking proceedings, policy statements or guidelines from the Commission explaining what conduct … it deems 'unreasonable,' and hence actionable"). Instead, the FTC is enforcing its vision of data-security policy through this selective, *ex post* enforcement action, which seeks to hold WHR liable for violating the FTC Act without any fair notice as to what data-security protections that Act supposedly requires. Indeed, after a two-year investigation into WHR's data-security practices, the FTC is unable to allege anything more specific than that WHR failed to employ protections that were "reasonable," "appropriate," "adequate," or "proper." The FTC's inability or unwillingness to state precisely what WHR did wrong—or tell others in the business community what they must do to avoid similar lawsuits in the future—confirms that the Commission has no business trying to regulate data-security practices under the FTC Act.

At a fundamental level, the central question here is whether the Government can maintain an enforcement action in this case despite not having any specific delegation from Congress, despite having previously conceded that it lacks authority to regulate data security, and despite not having published any rules or regulations providing fair notice of what conduct is prohibited. That approach, if accepted, would subject businesses to vague, unpublished, and uncertain requirements

that would drastically alter the regulatory landscape—without Congress or the President actually settling the debate about the proper scope of data-security regulation. For these reasons, and for those explained below, the FTC's Amended Complaint should be dismissed.

BACKGROUND

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

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

The FTC alleges that WHR violated Section 5 of the FTC Act by not maintaining "reasonable and appropriate" data-security protections. *Id*. ¶ 1. Although no court has ever construed Section 5 to apply to a private company's data-security practices, the FTC advances two legal theories for its novel construction of the Act. Count I relies on Section 5's prohibition on "decepti[ve]" practices and alleges that WHR deceived consumers by stating on its website that it used "commercially reasonable efforts" to secure payment card data that it collected. *Id*. ¶¶ 21, 44-46. Count II alleges that WHR's data-security protections amounted to "unfair" trade practices under Section 5 because those practices were not "reasonable and appropriate." *Id*. ¶¶ 47-49.

LEGAL STANDARD

WHR brings this motion under Federal Rule of Civil Procedure 12(b)(6) , which requires dismissal if the complaint fails to state a claim upon which relief can be granted. To survive a motion to dismiss under Rule 12(b)(6) , "a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1949 (2009) (quotations omitted). This "plausibility" determination is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Matthews v. Carson*, 2010 WL 572101, at *2 (D.N.J. Feb. 17, 2010) (quotations omitted). A plaintiff's obligation to cross the plausibility threshold "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

ARGUMENT

This case is a classic example of agency overreach. The Supreme Court has warned time and again that, "[r]egardless 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." *Brown & Williamson*, 529 U.S. at 125 (quotations omitted). The FTC's Count II unfairness claim—which this brief addresses first—stretches far beyond the traditional bounds of the Commission's authority. Nothing in the text or history of Section 5 purports to give the FTC authority to decide whether data-security protections are "unfair," and Congress's repeated enactment of specific data-security statutes (and failed attempts to enact comprehensive data-security laws) confirm that the statute cannot be construed so broadly. Simply put, Section 5's prohibition on "unfair" trade practices does not give the FTC authority to prescribe data-security standards for all private businesses.

The FTC's Count I "deception" claim—which relies exclusively on certain statements in WHR's online privacy policy—must also be dismissed. The only information allegedly compromised during the criminal cyber attacks was certain payment card data collected by independent Wyndham-branded hotels—no data collected ***by WHR*** was ever placed at risk. Numerous sections of the privacy policy make abundantly clear that WHR made ***no representations at all*** about the security of data collected by the independent Wyndham-branded hotels. And to the extent the FTC purports to allege that WHR's representations regarding its own data-security practices were deceptive, those allegations fall well short of bedrock federal-pleading requirements.

I. THE COUNT II UNFAIRNESS CLAIM MUST BE DISMISSED

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

Enacted in 1914, Section 5 of the FTC Act prohibits "unfair … acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). In delegating authority to the FTC to enforce that provision, Congress clearly did not authorize the FTC to regulate anything and everything that the Commission might deem "unfair." *See, e.g.*, *Scientific Mfg. Co. v. FTC*, 124 F.2d 640, 644 (3d Cir. 1941) (holding that Section 5 does not authorize the FTC to regulate publications "concerning an

article of trade by a person not engaged or financially interested in commerce in that trade," because otherwise "the Commission would become the absolute arbiter of the truth of all printed matter"). To the contrary, the scope of Section 5 is necessarily limited by that provision's "place in the overall statutory scheme" and by common understandings as to the "manner in which Congress is likely to delegate" significant policy decisions to administrative agencies. *Brown & Williamson*, 529 U.S. at 133 (quotations omitted).

The overall statutory landscape strongly suggests that the "unfair … acts or practices" language in Section 5 of the FTC Act should not be interpreted to empower the FTC to establish data-security standards for the private sector. When the FTC Act was first enacted in 1914, the statute might well have had "a range of plausible meanings." *Brown & Williamson*, 529 U.S. at 143. "Over time, however, subsequent acts [have] shape[d] or focus[ed] those meanings." *Id*. In particular, it is a well-established cannon of statutory construction that "where the scope of [an] earlier statute is broad but … subsequent statutes more specifically address the topic at hand," the "later federal statute[s] should control [a court's] construction of the [earlier] statute." *Id.* (quotations omitted); *see also id*. at 133 ("[T]he meaning of one statute may be affected by other Acts, particularly where Congress has spoken subsequently and more specifically to the topic at hand"); *see also United States v. Fausto*, 484 U.S. 439, 453 (1988) ("[T]he implications of a statute may be altered by the implications of a later statute."). Courts thus recognize that the later enactment of more-specific statutes targeting the subject matter at issue controls the interpretation of an earlier general statute. *See, e.g.*, *Brown & Williamson*, 529 U.S. at 143 (Congress's later enactment of tobacco-specific statutes foreclosed the FDA from exercising jurisdiction over tobacco products under the general provisions of the Food, Drug, and Cosmetic Act ("FDCA")); *Nutritional Health Alliance v. FDA*, 318 F.3d 92, 102 (2d Cir. 2003) (Congress's later enactment of statutes

"specifically targeted [at] the problem of accidental poisoning of children" foreclosed the FDA from assuming jurisdiction over poison-prevention packaging under the general provisions of the FDCA).

That rule of statutory interpretation applies in this case and requires that the FTC's unfairness claim be dismissed. Since the FTC Act was enacted, Congress has enacted a vast array of laws that specifically authorize particular federal agencies to establish minimum data-security standards in narrow sectors of the economy. For example:

- The Fair Credit Reporting Act ("FCRA"), Pub. L. 108-159, 117 Stat. 1953, codified at 15 U.S.C. § 1681 *et seq*., imposes requirements for the collection, disclosure, and disposal of data collected by consumer reporting agencies and requires the FTC and other agencies to develop rules for financial institutions to 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 establish standards for financial institutions "to protect against unauthorized access to or use of such records or information." 15 U.S.C. § 6801(b)(3).

- The Children's Online Privacy Protection Act ("COPPA"), Pub. L. 105-277, 112 Stat. 2581-728, codified at 15 U.S.C. § 6501 *et seq*., requires covered website operators to establish and maintain reasonable procedures to protect the confidentiality and security of information gathered from children.

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, codified at 45 U.S.C. § 1320d *et seq*., requires health care providers to maintain security standards for electronic health information.

- The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), Pub. L. No. 111-5, 123 Stat. 115, codified at 42 U.S.C. § 17921 *et seq*., requires regulated entities to provide notice of unsecured breaches of health information in certain circumstances and strengthens protections for such data.

- The Cable Television Consumer Protection and Competition Act, Pub. L. No. 102-385, 106 Stat. 1460, codified at 42 U.S.C. § 551, requires cable companies to take steps to prevent unauthorized access to certain subscriber information.[1]

[1] 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*.

Those later-enacted statutes, all of which are specifically focused on data-security issues, "shape or focus" the meaning of Section 5 of the FTC Act, *Brown & Williamson*, 529 U.S. at 143, and preclude any interpretation of Section 5 that would give the FTC general authority to set data-security standards.

Significantly, several of these laws, including the FCRA, GLBA, and COPPA, explicitly grant the FTC authority to regulate data security—but ***only*** in certain specific, limited contexts. Those statutes are powerful evidence that the FTC lacks general authority under Section 5 to regulate data-security practices in cases (like this one) that fall outside the confines of those narrow delegations. Indeed, if Section 5's prohibition on "unfair … acts or practices" granted the FTC the broad authority it claims in this case, the specific delegations of authority to the FTC in the FCRA, GLBA, and COPPA would have been entirely superfluous. By delegating certain limited authority to the FTC to regulate data security in narrow sectors of the economy, Congress has foreclosed any interpretation of Section 5 that would give the Commission overarching authority to set data-security standards for ***all*** businesses operating in ***all*** industries.

Indeed, until quite recently, the FTC specifically ***disclaimed*** the authority to regulate data security under Section 5's "unfair … practices" language. In the late 1990s and early 2000s, the Commission repeatedly stated that it "lack[ed] authority to require firms to adopt information practice policies," FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, (hereinafter, "2000 Privacy Report"), at 34 (2000), *available at* http://www.ftc.gov/reports/privacy2000/.pdf, and that its authority over data-security matters 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., 105th Cong., at n.23. (July 21, 1998), *available at* http://www.ftc.gov/os/1998/07/privac98.htm; *see also* Scott, 60 ADMIN. L. REV.

at 130-31 ("In its 2000 Report, the Commission indicated that … it could not require companies to adopt privacy policies."). 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. The agency doesn't have the jurisdiction to enforce privacy.'" Jeffrey Benner, *FTC Powerless to Protect Privacy*, Wired, May 31, 2001 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC).

The FTC's self-professed lack of power to regulate data security through Section 5's "unfairness" language is precisely why the FTC has for over a decade asked Congress to enact broader legislation giving the Commission the very authority it purports to wield in this case. *See, e.g.*, FTC, *Privacy Online* at 36-37 (asking Congress to enact 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 promulgate more detailed standards pursuant to the Administrative Procedure Act"); *see also Prepared Statement of the FTC on Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (May 4, 2011) ("[T]he Commission reiterates its support for federal legislation that would (1) impose data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach."); *Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (June 15, 2011) (same).

For good reasons, courts are generally reluctant to adopt a construction of a statute that the agency itself previously disclaimed. *See Brown & Williamson*, 529 U.S. at 144 (refusing to construe the FDCA as authorizing the FDA to regulate tobacco products because, *inter alia*, the FDA had made "consistent and repeated statements that it lacked authority under the FDCA to regulate tobacco"). While agencies are certainly free to change their mind, *see FCC v. Fox Television*

Stations Inc., 556 U.S. 502, 514-15 (2009), "[a]n agency interpretation of a relevant provision which conflicts with the agency's earlier interpretation is entitled to considerably less deference than a consistently held agency view," *INS v. Cardozo-Fonseca*, 480 U.S. 421, 447 n. 30 (1987). At the very least, the agency must give a "reasoned explanation" for its change in position and "show that there are good reasons for the new policy." *Fox Television*, 556 U.S. at 515. Here, however, the FTC has provided no reasons at all for why, despite its earlier assertions to the contrary, Section 5 of the FTC Act should be construed to permit the Commission to establish data-security standards for the private sector. Because it has failed to meet its "burden of rationally explaining its departure from its previous position," this Court should reject the FTC's novel interpretation of Section 5. *Pa. Fed'n of Sportsmen's Clubs, Inc. v. Kempthorne*, 497 F.3d 337, 351 (3d Cir. 2007) (rejecting Department of Interior's interpretation of its own regulations because it failed to reasonably explain its change in position).

Courts must also "be guided to a degree by common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and 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. In a very high-profile and well-publicized debate, Congress recently considered (and rejected) the Cybersecurity Act of 2012, S. 2105, 112th Cong. (Feb. 14, 2012), which would have created comprehensive "cybersecurity performance requirements" for the private sector. *Id.* § 104. Just last week, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 624, 113th Cong. (Apr. 18, 2013), a bill that aims to enhance cybersecurity practices by allowing private businesses and federal agencies to share cybersecurity information with one another. That

legislation abandons any attempt to create comprehensive cybersecurity performance requirements. And it would ***grant immunity*** to private businesses that share information about cybersecurity threats, including attacks on their own networks, with the federal government. *Id.* § 3(a) (providing "[n]o civil or criminal cause of action shall lie or be maintained in Federal or State court" in those circumstances). This legislative language is irreconcilable with the FTC's assertion that Congress wants the Commission to regulate private-sector data security through Section 5 of the FTC Act.

Indeed, in light of the important economic and political considerations involved in establishing data-security standards for the private sector, and the intense political debate that has surrounded efforts to establish such standards, it defies common sense to think that Congress would have delegated that responsibility to the FTC—particularly through a 1914 statute that does nothing more than forbid "unfair" practices. "Congress could not have intended to delegate a decision of such economic and political significance to an agency in so cryptic a fashion." *Brown & Williamson*, 529 U.S. at 160. Applying a similar intuition, the Supreme Court has consistently refused to construe ambiguous and open-ended statutory provisions as empowering administrative agencies to impose sweeping new regulations on American businesses. *See, e.g.*, *Gonzales v. Oregon*, 546 U.S. 243, 267 (2006) (rejecting the "idea that Congress gave the Attorney General such broad and unusual authority through an implicit delegation"); *Whitman*, 531 U.S. at 468 (stating that it is "implausible that Congress would give to the EPA through … modest words the power to determine whether implementation costs should moderate national air quality standards"); *MCI Telecomms. Corp. v. AT&T Co.*, 512 U.S. 218, 231 (1994) (the FCC's power to "modify" requirements in the communications laws does not include the power to make "radical or fundamental" changes to regulatory requirements).

In the end, this case is analogous to *Brown & Williamson*, in which the Supreme Court rejected the FDA's attempt to regulate tobacco products under the FDCA. 529 U.S. 120. Like the FTC here, the FDA had previously taken the position that the FDCA did not give it authority to regulate tobacco products. *See id.* at 145-46, 153-55. Like here, Congress "considered and rejected several proposals to give the FDA the authority to regulate tobacco"—authority the FDA later tried to claim through agency action. *Id.* at 147, 153-55. And like here, Congress ultimately settled on "a less extensive regulatory scheme" and passed narrowly tailored legislation. *Id.* at 148. Under these analogous circumstances, the Court concluded that Congress' more narrowly tailored legislation "ha[d] effectively ratified the FDA's previous position that it lack[ed] jurisdiction." *Id.* at 156. There is no stronger basis for the FTC to claim authority to regulate data-security in this case than there was for the FDA to claim authority to regulate tobacco in *Brown & Williamson*.

Data security is undoubtedly an important issue. But "no matter how important … the issue, an administrative agency's power to regulate in the public interest must always be grounded in a valid grant of authority from Congress." *Id.* at 161. Here, Congress has indicated that the FTC's authority to regulate "unfair" trade practices under Section 5 does not extend to creating data-security standards that every business in America must obey. The FTC's Count II unfairness claim therefore should be dismissed.

B. The FTC Failed To Provide Fair Notice Of What Section 5 Requires

Even if Section 5 did give the FTC authority to mandate data-security standards for the private sector, WHR cannot be held liable through this *ex post* enforcement action. The Constitution forbids the United States from punishing private citizens and businesses for failing to follow standards of conduct of which the Government failed to provide fair notice. *See Vartelas v. Holder*, 132 S.Ct. 1479, 1486 (2012) (noting "the *Ex Post Facto* Clause, the Contracts Clause, and the Fifth

Amendment's Due Process Clause" all embody the doctrine that new laws should not govern "transactions or considerations already past" (quotations omitted)). Because the FTC has not published ***any*** rules, regulations, or other guidelines explaining what data-security practices the Commission believes Section 5 to forbid or require, it would violate basic principles of fair notice and due process to hold WHR liable in this case.

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). Administrative law has "thoroughly incorporated" this constitutional "fair notice" requirement to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. *General Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995). Specifically, although agencies have some discretion to make law through enforcement actions, *see NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 294 (1974), agencies generally cannot use enforcement actions simultaneously to make new rules and to hold a party liable for violating the newly announced rule, *see, e.g.*, *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986) (Scalia, J.). Instead, to hold a party liable in an enforcement action, existing law must "state with ***ascertainable certainty*** . . . the standards" the agency expects parties to obey. *Dravo Corp. v. OSHRC*, 613 F.2d 1227, 1232-33 (3d Cir. 1980) (emphasis added); *General Elec.*, 53 F.3d at 1329. As the D.C. Circuit has recognized, these limits on agency power do nothing more than extend the "no punishment without notice" protections routinely afforded criminal defendants to other private actors the Government seeks to punish. *See General Elec.*, 53 F.3d at 1328-29.

Two recent Supreme Court cases reaffirm the well-established rule that agencies cannot use enforcement actions to impose *ex post* liability on private citizens and businesses without having provided fair notice of what the law required. In the first case, *Christopher v. SmithKline Beecham*

Corp., 132 S.Ct. 2156 (2012), the Court rejected the Department of Labor's unexpected, after-the-fact interpretation of its own regulations offered in a class-action suit seeking money damages—an interpretation ordinarily entitled to substantial deference, *see Chase Bank USA, N.A. v. McCoy*, 131 S.Ct. 871, 880 (2011). In doing so, the Court rejected the argument that "regulated parties [must] divine the agency's [position] in advance or else be held liable when the agency announces its [position] for the first time in an enforcement proceeding." *Christopher*, 132 S.Ct. at 2167-69. In the second case, *Fox Television*, the Court set aside an FCC adjudicative order against two television broadcasters because the agency did not provide "fair notice of what was forbidden." 132 S. Ct. at 2318.

For decades, the Third Circuit and other Courts of Appeals have similarly rejected agency attempts to impose liability for legal rules "the agency announces . . . for the first time in an enforcement proceeding." *Christopher*, 132 S.Ct. at 2168; *see Dravo*, 613 F.2d at 1232-33 (refusing to punish past conduct based on a newly announced agency interpretation of regulations where those regulations did not "state with ascertainable certainty" that they covered the challenged conduct); *Fabi Construction Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007) (reversing liability of construction company because the agency failed to provide fair notice of what implementing regulations required); *PMD Produce Brokerage Corp. v. Department of Agriculture*, 234 F.3d 48 (D.C. Cir. 2000) (reversing dismissal of administrative appeal because Department of Agriculture failed to provide fair notice of what its internal procedural rules required); *Trinity Broadcasting of Florida Inc. v. FCC*, 211 F.3d 618 (D.C. Cir. 2000) (reversing liability of broadcaster because FCC failed to provide fair notice of what regulations required); *United States v. Chrysler Corp.*, 158 F.3d 1350, 1357 (D.C. Cir. 1998) (reversing agency-ordered car recall because "the NHTSA failed to provide adequate notice" of what the law required); *General Electric*, 53 F.3d at 1333-34 (vacating

finding of liability because the EPA failed to provide a company with "fair notice" of what applicable regulations required).

The FTC's enforcement action in this case should be dismissed because the Commission never provided the "fair notice" that the Constitution and these cases require. The text of Section 5 itself clearly provides no meaningful notice to regulated parties—it generically prohibits "unfair and deceptive" business practices without going into any further detail as to what practices might be deemed "unfair" or "deceptive." 15 U.S.C. § 45. And making matters worse, the FTC has published ***no rules or regulations at all*** explaining what data-security practices a company must adopt to be in compliance with the statute. Thus, although the FTC's complaint faults WHR (among other things) for using "inappropriate[]" software, firewalls, inventory procedures, and incident-response procedures, the FTC has previously provided no "fair notice" telling businesses what software they must use, how they must deploy firewalls, what inventory procedures they must adopt, and what procedures they should follow in the event of a breach. The result is that businesses are left to guess as to what they must do to comply with the law. They must, in the Supreme Court's words, "divine the agency's [position] in advance or else be held liable when the agency announces its [position] for the first time in an enforcement proceeding." *Christopher*, 132 S.Ct. at 2168; *see also E.I. du Pont de Nemours & Co. v. FTC*, 729 F.2d 128, 138-39 (2d Cir. 1984) (holding 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"). That is precisely what due process does not allow.

The President, perhaps recognizing the FTC's "sue now, offer guidance later" approach is bad policy and unconstitutional, eschewed that approach to data-security regulation in his February 12, 2013 Executive Order on Improving Cybersecurity for Critical Infrastructure. *See* Exec. Order

No. 13,636, 78 Fed. Reg. 11739 (Feb. 12, 2013) ("Executive Order") (Hradil Decl., Ex. B); Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013) (attached as Hradil Decl., Ex. C). That Order requires the National Institute of Standards and Technology ("NIST") to lead the creation of a baseline set of standards for reducing cyber risks to critical infrastructure—what the Executive Order calls the "Cybersecurity Framework." The Cybersecurity Framework will establish a "set of standards, methodologies, procedures, and processes" for addressing cybersecurity threats, *id*., and will include "guidance for measuring the performance of an entity in implementing" those standards, *id*. § 7(b). The Framework must also "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach" that includes specific "information security measures and controls" critical-infrastructure operators can implement to "identify, assess, and manage cyber risk." *Id*. In developing the Cybersecurity Framework, the Director of NIST must "engage in an open public review and comment process." *Id*. § 7(d). Compliance with the Cybersecurity Framework is initially "voluntary," *id*. § 8(a), however federal agencies are directed to develop "incentives" to promote compliance and to assess whether "the agency has clear authority to establish requirements based on the Cybersecurity Framework," *id.* § 10(a).

Each of the steps the President's Executive Order recognizes as necessary for effective and lawful data-security regulation is missing from the FTC's approach. The FTC has not issued any "standards, methodologies, procedures, [or] processes" for complying with Section 5, *id*. § 7(a); it has not established "guidance for measuring the performance of an entity in implementing" data-security protections that might comply with the statute, *id*. § 7(b); it has not identified specific "information security measures and controls" that a business might adopt, *id*. § 7(b); and it has not "engage[d] in an open public review and comment process," *id*. § 7(d). Yet there is no reason the

same process the President has determined is necessary to regulate data security for critical infrastructure—a process that develops regulatory rules and standards ***before*** bringing enforcement actions seeking injunctions and millions of dollars—should become unnecessary when the FTC seeks to regulate data security in other sectors of the economy.

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 cannot be stretched so far as to authorize the FTC to regulate the type of data at issue in this case—consumer payment card information. 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 never substantial and always avoidable. 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); *see also Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 174 (3d Cir. 2008) (explaining that § 1643 "creates a ceiling of $50 for cardholder liability for unauthorized charges"). And all major card brands have adopted policies that waive liability for even that small amount.[2] Consumers can thus always "reasonably avoid" any financial injury stemming from the theft of payment card data simply by having their issuer rescind any unauthorized charges. 15 U.S.C. § 1643(a)(1)(B) ("[O]nce a cardholder becomes aware of fraudulent activity on his/her account and notifies the card Issuer,

[2] *See* Visa, 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://www.americanexpress.com/us/content/fraud-protection-center/purchase-protection.html?vgnextchannel=9ee6d6954360c110VgnVCM100000defaad94RCRD&appinstancename=default (same) (all last visited Apr. 26, 2013).

that Issuer is obligated to reverse the charges, or credit the cardholder, for the amount of those fraudulent charges.").

The Third Circuit has recognized that the harm stemming from the theft of financial information often does not cause "substantial injury" to consumers. In *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), hackers successfully accessed systems at a payroll-processing firm that stored sensitive financial information. Individuals who had their financial information potentially compromised then brought suit against the payroll-processing firm, arguing that they had been injured by the theft of their data. *Id*. at 40. In affirming the dismissal of those claims, the Third Circuit held that the plaintiffs had not suffered an "injury-in-fact" from the data breach, and thus lacked constitutional standing to assert their claims. *Id*. at 41. The Court of Appeals explained that the plaintiffs could not show that the hacker was "able to use such [financial] information to the detriment of [plaintiffs] by making unauthorized transactions in [plaintiffs'] names." *Id*. at 42. As the Third Circuit explained it, plaintiffs' "credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked." *Id*. at 45. The court also rejected the plaintiffs' attempts to rely on the "time and money expend[ed] to monitor their financial information" to establish a substantial injury, explaining that such "speculative" expenses were not made "as a result of any *actual* injury." *Id*. at 46 (emphasis in original).

What the Third Circuit said in *Reilly* is equally true here. As in that case, consumers did not suffer any "substantial injury" from the cyberattacks on WHR. In light of federal law and card brand rules concerning the theft of payment-card data, those consumers' "credit card statements are exactly the same today as they would have been had [WHR's] database never been hacked." *Id*. at 45. And because they are not based on any "*actual* injury," any incidental injuries that consumers suffered to

"monitor their financial information," does not amount to the type of "substantial injury to consumers" required under section 45(n).

Indeed, at least one former 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/2012/03/120326 privacyreport.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)." *Id.* at C-5. Adhering to that view, Commissioner Rosch dissented from the FTC's decision to include an "unfairness" claim in its complaint in this case.[3]

The illusory consumer harm in this case also underscores how much the FTC must twist Section 5 to bring an enforcement action against WHR. WHR, unlike the consumers in this case, lost millions of dollars and suffered significant reputational harm when cybercriminals ***attacked its network***. Yet the FTC wants to turn a statute designed to protect consumers from unscrupulous businessmen, *see FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202 (10th Cir. 2005) ("The primary purpose of § 5 is to lessen the harsh effects of caveat emptor."), into a tool to punish businesses victimized by criminals. This is the Internet equivalent of punishing the local furniture store because it was robbed and its files raided. Not only is this result senseless, it cannot be what Congress intended when it enacted Section 5. *See United States v. Bacto-Unidisk*, 394 U.S. 784, 800 (1969) ("In our anxiety to effectuate the congressional purpose of protecting the public, we must

[3] *See* FTC Press Release, *FTC Files Complaint Against Wyndham Hotels* (June 26, 2012), *available at* http://www.ftc.gov/opa/2012/06/.shtm.

take care not to extend the scope of the statute beyond the point where Congress indicated it would stop.").

Even if Section 5 could be construed to mandate certain data-security requirements for payment card data, the standard of liability for failing to protect that data would be demanding and far above what the FTC has alleged in this case. The requirements imposed by Section 5 must be balanced against the risk of consumer injury. *See* 15 U.S.C. § 45(n). And because the risk of consumer injury posed by the theft of payment card data is either non-existent or, at a minimum, exceedingly small, the standard of liability for failing to adequately protect such data would have to be correspondingly high. That is precisely why courts examining data-security issues under state unfair-trade-practices statutes have held that such practices are unfair only when they are egregious or "reckless" in nature. *See, e.g.*, *Worix v. MedAssets, Inc.*, 869 F. Supp. 2d 893, 900 (N.D. Ill. 2012). The FTC does not allege such recklessness or egregiousness here.

D. The Unfairness Count Fails Federal-Pleading Requirements.

Finally, the Amended Complaint should be dismissed because it fails to satisfy basic pleading requirements. *See Iqbal*, 556 U.S. at 678. The Amended Complaint criticizes WHR for failing to employ practices that were "readily available," "adequate," "commonly-used," and "proper." Am. Compl. ¶ 24. But nowhere does the FTC give any factual detail as to what procedures, or combination of procedures, would have met those conclusory standards. For example, the FTC alleges that defendants "failed to ensure the Wyndham-branded hotels implemented adequate information security policies," *id.* ¶ 24(c), but never states what policies would be "adequate." It criticizes defendants' operating systems as "outdated," *id.* ¶ 24(d), but fails to allege what alternative systems would be current. And it states that defendants "failed to employ reasonable measures to detect and prevent unauthorized access," *id.* ¶ 24(h), but does not explain

what measures would be "reasonable"—now or when the alleged breaches occurred. Simply put, the FTC's allegations are nothing more than "legal conclusions couched as factual allegations" and do not state a plausible claim for relief. *Twombly*, 550 U.S. at 555; *see Willey v. J.P. Morgan Chase, N.A.*, 2009 WL 1938987, at *4 (S.D.N.Y. July 7, 2009) (holding that data breach plaintiff failed to satisfy *Twombly* because his allegation of "unreasonable" data security was unsupported by "factual allegations" explaining "how the procedures Chase adopted failed to comply with" the law).

Even looking past the FTC's conclusory allegations of "unreasonable" security, the Commission also has not adequately pleaded causation. *See* 15 U.S.C. § 45(n). The Amended Complaint contains no factual allegations showing *how* the alleged data-security failures caused the intrusions, or *how* the intrusions resulted in any particular consumer harm. Instead, the FTC simply asserts without explanation that the intrusions were the "result" of WHR's data-security program (Am. Compl. ¶¶ 25, 32) and that the intrusions then "resulted" in hackers stealing payment card information and making fraudulent charges (*id.* ¶¶ 36, 39, 40). Such conclusory allegations of wrongdoing are exactly the kind of unadorned assertions that fail federal pleading requirements. *See Iqbal*, 556 U.S. at 678; *see also Katz v. Pershing, LLC*, 672 F.3d 64, 75 (1st Cir. 2012) (data breach plaintiff failed to state claim under *Twombly* and *Iqbal* where he "ha[d] merely given lip service to the elements of causation and harm"). 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 consumer harm.

II. THE COUNT I DECEPTION CLAIM MUST BE DISMISSED

The FTC's Count I deception claim fares no better than its Count II unfairness claim. To impose liability under the "deception" prong of Section 5, the FTC must identify (1) a representation; that (2) is "likely to mislead consumers acting reasonably under the circumstances;"

that (3) is "material." *FTC v. Millennium Telecard, Inc.*, 2011 WL 2745963, at *6 (D.N.J. July 12, 2011). Because such a claim "sounds in fraud," the FTC must meet the heightened pleading requirements of Rule 9(b) when alleging unlawful deception. *FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 853 (C.D. Cal. 2010); *FTC v. Ivy Capital, Inc.*, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011). But even applying general pleading standards, *see, e.g.*, *Iqbal*, 556 U.S. at 678, the FTC's Count I deception claim must be dismissed. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 663.

The FTC alleges that WHR deceived consumers when it stated in its online privacy policy that WHR used "industry standard practices" and "commercially reasonable efforts" to protect the security of payment card data. *See* Am. Compl. ¶ 21; *see also* Hradil Decl., Ex. A (containing the privacy policy in its entirety).[4] In alleging that those statements were deceptive, however, the FTC relies primarily on allegations concerning the state of data-security ***at the Wyndham-branded hotels***. The FTC thus points to a number of alleged "inadequate data-security practices" at the Wyndham-branded hotels, *see id*. Am. Compl. ¶¶ 24(a), 24(b), 24(c), 24(d), 24(f), 24(j), and three instances in which cybercriminals were able to access payment-card data collected and controlled by the Wyndham-branded hotels, *see id.* ¶¶ 25, 30-31, 34-35, 37.

As a matter of law, allegations concerning the state of data-security at the Wyndham-branded hotels cannot support the FTC's deception claim. WHR and the Wyndham-branded hotels are legally separate entities that each maintain their own computer networks and engage in their own

[4] "In evaluating a motion to dismiss, we may consider documents that are attached to or submitted with the complaint, and any 'matters incorporated by reference or integral to the claim, items subject to judicial notice, matters of public record, orders, [and] items appearing in the record of the case.'" *Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006) (quoting 5B Charles A. Wright & Arthur R. Miller, Federal Practice & Procedure § 1357 (3d ed. 2004)).

data-collection practices.[5] And by its plain terms, the WHR privacy policy makes representations ***only*** about the data-security practices at WHR and does not make any representations about data-security practices at the Wyndham-branded hotels. Thus, the privacy policy consistently uses the terms "we," "us," and "our" when making representations about WHR's data-security practices, and specifically defines those terms to ***exclude*** the Wyndham-branded hotels. Hradil Decl., Ex. A at 1. The policy also expressly caveats each representation about data-security by explaining that those representations apply only to "our collection" of data and only "to the extent we control the Information"—caveats that plainly exclude any data collected by the Wyndham-branded hotels. *Id*. And if all of that were not enough, the privacy policy includes a separately-titled section—which the FTC conveniently omitted from its quotation of WHR's privacy policy in the Amended Complaint—that ***expressly disclaims*** making any representations about the security of payment-card data collected by the Wyndham-branded hotels:

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

Id. at 4.

The bottom line is that any reasonable consumer, after reading the privacy policy "as a whole, without emphasizing isolated words or phrases apart from their context," *Millennium*

[5] As a franchisor, WHR collects payment card data through its centralized reservations service—which permits guests to book hotel rooms either online or over the phone—and processes that information through its corporate network. *See* Hradil Decl., Ex. A, at 2. Separate and apart from WHR's practices, each independently owned Wyndham-branded hotel collects payment card data and processes that data on its own local networks. *Id*. at 4.

Telecard, 2011 WL 2745963), at *5 (quotations omitted), would have understood that the policy made statements only about data-security practices at WHR and made no representations about data-security practices at the Wyndham-branded hotels. The FTC's allegations about the state of data security at the Wyndham-branded hotels thus do nothing to support its deception claim against WHR.

WHR's privacy policy—which makes clear WHR accepts responsibility only for its own actions, not those of its franchisees—is consistent with basic principles of franchise law. A franchisee is "a limited independent contractor," *Lodbell v. Sugar & Spice, Inc.*, 658 P.2d 1267, 1274 (Wash. 1983), which operates as an independent business separate and distinct from the franchisor, *Southern States Co-Op, Inc. v. Global AG Assocs., Inc.*, 2008 WL 834389, at *4 n.5 (E.D. Pa. March 27, 2008); *In re Saxby's Coffee Worldwide, LLC.*, 440 B.R. 369 (Bankr. E.D. Pa. 2009). Because a franchisor and its franchisees are independent businesses, a franchisor ordinarily is not responsible "for the acts and omissions of its franchisees." Martin D. Fern, *Establishing and Operating under a Franchise Relationship* § 1.04[C][3] (2000). Courts deviate from this rule only when the franchisor exercises day-to-day control over the activities at the franchisee that caused the alleged harm. *See Capriglione v. Radisson Hotels Int'l, Inc.*, 2011 WL 4736310, at *3 (D.N.J. Oct. 5, 2011) (dismissing tort suit against franchisor for injuries sustained at a franchisee's hotel property because the franchisor "lacked both ownership interest in and control over the day-to-day operations of the Hotel"); *Chen v. Domino's Pizza, Inc.*, 2009 WL 3379946, at *4 (D.N.J. Oct. 16, 2009) (dismissing complaint asserting franchisor was liable to a franchisee's employee for Fair Labor Standards Act because the franchisor did not "ha[ve] any authority or control over the[] employment conditions."); Fern § 1.04[C][3] . By disclaiming responsibility for data-security at the Wyndham-

branded hotels, therefore, WHR's privacy policy was doing nothing more than applying well-established rules of franchise law.

Recognizing that critical shortcoming in its deception case, the FTC makes a half-hearted attempt to allege that WHR made deceptive statements about ***its own*** data-security practices. *See* Am. Compl. ¶¶ 24(g), 24(h), 24(i). But those allegations amount to nothing more than conclusory statements of wrongdoing that fall well short of establishing a "plausible" claim to relief. *Iqbal*, 556 U.S. at 678. Thus, although the Amended Complaint alleges that WHR did not employ certain "adequate[]," "reasonable," or "proper" practices, Am. Compl. ¶¶ 24(g)-(j), those claims fall far short of what federal pleading standards require. Whether a security standard is "adequate" or "reasonable" is a question of law, not of fact, and allegations as to the same are thus properly disregarded on a motion to dismiss. *See Iqbal*, 556 U.S. at 678 (courts are "'not bound to accept as true a legal conclusion couched as a factual allegation'") (quoting *Twombly*, 550 U.S. 544 at 555 (2007)). In any event, the FTC makes no attempt to explain what those terms mean or what it believes would have been "adequate[]," "reasonable," or "proper" in those specific contexts. *See, e.g.*, *Seldon v. Home Loan Servs., Inc.*, 647 F. Supp. 2d 451, 461 (E.D. Pa. 2009) (dismissing complaint because "plaintiffs provide no allegation whatsoever as to how any of these fees qualify as unreasonable").

Furthermore, although the FTC's deception allegations necessarily depend on the Commission proving that WHR's data-security practices were not "industry standard" or "commercially reasonable," the Amended Complaint contains no allegations at all explaining what data-security practices were "standard" in the hospitality industry in 2008 or how WHR's data-security practices fell short of that benchmark. *See Argueta v. U.S. Immigration and Customs Enforcement*, 643 F.3d 60, 75 (3d Cir. 2011) (concluding that "like *Iqbal*, Plaintiffs failed to allege a

plausible [] claim" in part because "Plaintiffs themselves did not really identify in their pleading what exactly [defendants] should have done differently"). That is a fatal omission: Absent allegations explaining what "industry standard" practices would have required in 2008, the Amended Complaint provides no basis for asserting that WHR's privacy policy is deceptive.

Perhaps most telling of all, the FTC does nothing to explain how the alleged deficiencies it identifies placed personal information ***collected by WHR*** at risk. Indeed, the FTC nowhere even alleges that any intruder compromised (or had access to) data collected by WHR. There is thus no basis in law or logic for pointing to the data breaches as evidence of "deceptive" practices by WHR. That fact, coupled with the barebones nature of the FTC's allegations concerning the security of data collected by WHR, conclusively undermines any argument that the WHR privacy policy was somehow "deceptive."

CONCLUSION

For these reasons, WHR respectfully requests that the Court dismiss the FTC's amended complaint as a matter of law.

Dated: April 26, 2013

Respectfully submitted,

By: s/ Jennifer A. Hradil

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

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice to be filed
K. Winn Allen, DC Bar 1000590
Pro Hac Vice to be filed
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 to be filed
ROPES & GRAY, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517
douglas.meal@ropesgray.com

Attorneys for Defendants