FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

FEDERAL TRADE COMMISSION,	:	
Plaintiff,	:	**Civil Action No. 13-1887 (ES)**
v.	:	**OPINION**
WYNDHAM WORLDWIDE CORPORATION, et al.,	:	
Defendants.	:	

SALAS, DISTRICT JUDGE

I. INTRODUCTION

The Federal Trade Commission (the "FTC") brought this action under Section 5(a) of the Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. § 45(a), against Wyndham Worldwide Corporation ("Wyndham Worldwide"), Wyndham Hotel Group, LLC ("Hotel Group"), Wyndham Hotels and Resorts, LLC ("Hotels and Resorts"), and Wyndham Hotel Management, Inc. ("Hotel Management") (collectively, "Wyndham" or "Defendants"). The FTC alleges that Wyndham violated Section 5(a)'s prohibition of "acts or practices in or affecting commerce" that are "unfair" or "deceptive."

Specifically, the FTC alleges that Defendants violated both the deception and unfairness prongs of Section 5(a) "in connection with Defendants' failure to maintain reasonable and appropriate data security for consumers' sensitive personal information." (D.E. No. 28, First Amended Complaint for Injunctive and Other Equitable Relief ("Compl.") ¶¶ 1, 44-49). Hotels and Resorts moves to dismiss the FTC's complaint under Federal Rule of Civil Procedure

12(b)(6). (D.E. No. 91-1, Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC ("HR's Mov. Br.") at 6).[1] Its motion to dismiss raises the following three issues.

First, Hotels and Resorts challenges the FTC's au

II. FACTUAL BACKGROUND[2]

Wyndham Worldwide is in the hospitality business. (Compl. ¶ 7). "At all relevant times," Wyndham Worldwide controlled the acts and practices of the following subsidiaries: Hotel Group, Hotels and Resorts, and Hotel Management. (*Id.* ¶¶ 7-10). Through these three subsidiaries, Wyndham Worldwide "franchises and manages hotels and sells timeshares." (*Id.* ¶ 13).

More specifically, "Hotel Group is a wholly-owned subsidiary of Wyndham Worldwide." (*Id.* ¶ 8). Both Hotels and Resorts and Hotel Management, in turn, are wholly-owned subsidiaries of Hotel Group. (*Id.* ¶¶ 9, 10). Hotels and Resorts licensed the "Wyndham" name to approximately seventy-five independently-owned hotels under *franchise* agreements. (*Id.* ¶ 9). Similarly, Hotel Management licensed the "Wyndham" name to approximately fifteen independently-owned hotels under *management* agreements. (*Id.* ¶ 10).

Under these agreements, Hotels and Resorts and Hotel Management require each Wyndham-branded hotel to purchase—and "configure to their specifications"—a designated computer system that, among other things, handles reservations and payment card transactions. (*Id.* ¶ 15). This system, known as a "property management system," stores consumers' personal information, "including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes." (*Id.*).

The property management systems for *all* Wyndham-branded hotels "are part of Hotels and Resorts' computer network" and "are linked to its corporate network." (*Id.* ¶ 16). Indeed, Hotels and Resorts' computer network "includes its central reservation system" that "coordinates reservations across the Wyndham brand" and, using Hotels and Resorts' website, "consumers

[2] The Court must accept the FTC's factual allegations as true for purposes of resolving Hotels and Resorts' motion to dismiss. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *see also Bistrian v. Levi*, 696 F.3d 352, 358 n.1 (3d Cir. 2012) ("As such, we set out facts as they appear in the Complaint and its exhibits.").

can make reservations at any Wyndham-branded hotel." (*Id.* ¶¶ 16, 20). And, although certain Wyndham-branded hotels have their own websites, customers making reservations for these hotels "are directed back to Hotels and Resorts' website to make reservations." (*Id.* ¶ 20).

The FTC alleges that, since at least April 2008, Wyndham "failed to provide reasonable and appropriate security for the personal information collected and maintained by Hotels and Resorts, Hotel Management, and the Wyndham-branded hotels." (*Id.* ¶ 24). The FTC alleges that Wyndham did this "by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." (*Id.*).

As a result of these failures, between April 2008 and January 2010, intruders gained unauthorized access—on three separate occasions—to Hotels and Resorts' computer network, including the Wyndham-branded hotels' property management systems. (*Id.* ¶ 25; *see also id.* ¶¶ 26-39 (detailing the circumstances of the three breaches and impact of each breach)). The intruders "used similar techniques on each occasion to access personal information stored on the Wyndham-branded hotels' property management system servers, including customers' payment card account numbers, expiration dates, and security codes." (*Id.* ¶ 25). And, after discovering the first two breaches, Wyndham "failed to take appropriate steps in a reasonable time frame to prevent the further compromise of Hotels and Resorts' network." (*Id.*).

Wyndham's "failure to implement reasonable and appropriate security measures exposed consumers' personal information to unauthorized access, collection, and use" that "has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses." (*Id.* ¶ 40). Defendants' failure "to implement reasonable and appropriate security measures" caused, for example, the following:

> [T]he three data breaches described above, the compromise of more than 619,000 consumer payment card account numbers, the

> exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.

(*Id.* ¶ 40).

Given these allegations, the FTC brought this action, seeking a permanent injunction to prevent future violations of the FTC Act, as well as certain other relief. (*See id.* at 20-21).

III. LEGAL STANDARD

To withstand a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*

"When reviewing a motion to dismiss, '[a]ll allegations in the complaint must be accepted as true, and the plaintiff must be given the benefit of every favorable inference to be drawn therefrom.'" *Malleus v. George*, 641 F.3d 560, 563 (3d Cir. 2011) (quoting *Kulwicki v. Dawson*, 969 F.2d 1454, 1462 (3d Cir. 1992)). But the

documents if the complainant's claims are based upon these documents." *Mayer v. Belichick*, 605 F.3d 223, 230 (3d Cir. 2010); *see also Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006) ("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.") (internal quotation marks, textual modifications and citations omitted).

IV. DISCUSSION

The Court notes that both the FTC and Hotels and Resorts seem to recognize the importance of data security and the damage caused by data-security breaches. Both also seem to acknowledge that we live in a digital age that is rapidly evolving—and one in which maintaining privacy is, perhaps, an ongoing struggle. And, as evident from the instant action, this climate undoubtedly raises a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future.

Hotels and Resorts characterizes this case as the first instance where "the FTC is asking a federal court to hold that Section 5 of the FT

argument, supplemental briefing, as well as in several *amici* submissions, the Court now endeavors to explain why Hotels and Resorts' demands are inconsistent with governing and persuasive authority.[3]

To be sure, the Court does *not* render a decision on liability today. Instead, it resolves a motion to dismiss a complaint. A liability determination is for another day. And this decision does *not* give the FTC a blank check to sustain a lawsuit against every business that has been hacked. Instead, the Court denies a motion to dismiss given the allegations in *this* complaint—which must be taken as true at this stage—in view of binding and persuasive precedent.

A. The FTC's Unfairness Claim (Count Two)

Hotels and Resorts first challenges the FTC's unfairness claim. (HR's Mov. Br. at 7). Under this claim, the FTC alleges that "Defendants have failed to employ reasonable and appropriate measures to protect personal information against unauthorized access." (Compl. ¶ 47). The FTC alleges that "Defendants' actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition" and, therefore, "Defendants' acts and practices . . . constitute unfair acts or pr

common sense to think that Congress would have delegated [this] responsibility to the FTC." (*Id.* at 12-13 (citing *Brown & Williamson*, 529 U.S. at 133, 160)). In sum, Hotels and Resorts declares that "[t]here 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*." (*Id.* at 14).

In opposition, the FTC argues that *Brown & Williamson* is distinguishable. (D.E. No. 110, Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC ("FTC's Opp. Br.") at 10). The FTC insists that, unlike *Brown & Williamson*, its own assertion of authority here would not result in any statutory inconsistencies. (*Id.*).

The FTC argues that, in actuality, Hotels and Resorts cites statutes that supplement the FTC's Section 5 authority for three reasons: (1) those statutes do not have the "consumer injury" requirement that Section 5 has; (2) they grant the FTC additional powers that it otherwise lacks; and (3) they "affirmatively compel (rather than merely authorize) the FTC to use its consumer-protection authority in specified ways." (Jnt. Supp. Br at 6; *see also* FTC's Opp. Br. at 16 n.4 ("The liability exemption provision [in CISPA] is expressly limited to potential liability from complying with that Act.")).[5] Indeed, the FTC avers that Congress purposely gave it broad power under Section 5 of the FTC Act and that its decision to enforce the FTC Act in the data-security context is entitled to deference. (FTC's Opp. Br. at 11).

Moreover, the FTC argues that, unlike the FDA's repeated denials of authority over tobacco in *Brown & Williamson*, the FTC has never disavowed authority over unfair practices

[5] In its opposition brief, the FTC argued that the subsequent data-security laws "enhance FTC authority with new legal tools" such as "rulemaking and/or civil penalty authority." (FTC's Opp. Br. at 12). At oral argument, however, the FTC seemed to reconcile these data-security laws by arguing that Section 5 requires "substantial injury," whereas these other laws do not. (*See* 11/7/13 Tr. at 44:17-45:22). To provide the parties a full and fair opportunity to present their arguments, as well as provide any updates on recent developments, the Court invited supplemental briefing. (*See* D.E. Nos. 146, 152, 153, 156 and 158). The Court has considered all of these submissions in resolving Hotels and Resorts' motion to dismiss.

related to data security. (*Id.* at 10, 13). Lastly, the FTC proclaims that "any question about the FTC's authority in the data security area is put to rest by the *LabMD* decision"—a recent decision by the FTC in an administrative action that the FTC contends deserves deference under *Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984). (Jnt. Supp. Br. at 6, 8-9).

b. Analysis

The Court rejects Hotels and Resorts' invitation to carve out a data-security exception to the FTC's unfairness authority because this case is different from *Brown & Williamson*. In *Brown & Williamson*, the Supreme Court determined that, "[c]onsidering the [Food, Drug, and Cosmetic Act ("FDCA")] as a whole, it is clear that Congress intended to exclude tobacco products from the FDA's jurisdiction." 529 U.S. at 142. It reasoned that "if tobacco products were within the FDA's jurisdiction, the Act would require the FDA to remove them from the market entirely." *Id.*

531 (2007) (distinguishing *Brown & Williamson*, finding that the "EPA has not identified any congressional action that *conflicts* in any way with the regulation of greenhouse gases from new motor vehicles") (emphasis added). Instead, Hotels and Resorts unequivocally recognizes that "the FCRA, GLBA, and COPPA all contain detailed provisions granting the FTC *substantive* authority over data-security practices." (Jnt. Supp. Br at 2-3).

To be sure, Hotels and Resorts contends that these statutes are "entirely superfluous" if the FTC "already possess[ed] generalized data-security authority under Section 5." (D.E. No. 156, HR's Reply to the Parties' Joint Supplemental Letter Brief ("HR's Reply to Jnt. Supp. Br.") at 2). In fact, Hotels and Resorts posits that "the FTC must prove substantial, unavoidable consumer injury as part of enforcing those statutes" and that "no provision of the FCRA, GLBA, or COPPA purports to relieve the FTC of its duty to prove substantial consumer injury." (Jnt. Supp. Br at 3). In Hotels and Resorts' view, if "both sets of statutes require substantial consumer injury," then "the FTC's understanding of Section 5 cannot be sustained without rendering the terms of the FCRA, GLBA, and COPPA entirely superfluous." (*Id.*).

But this ignores the critical premise of *Brown & Williamson*. *See, e.g.*, 529 U.S. at 133 ("[W]e find that Congress has directly spoken to the issue here and *precluded* the FDA's jurisdiction to regulate tobacco products.") (emphasis added). Here, subsequent data-security legislation seems to complement—*not preclude*—the FTC's authority.

Specifically, the FTC Act defines "unfair acts or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). And Hotels and Resorts identifies statutes, such as the FCRA,

GLBA, and COPPA, that each set forth different standards for injury in certain delineated circumstances, granting the FTC *additional* enforcement tools.[6]

Thus, unlike the FDA's regulation over tobacco, the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme. *See Brown & Williamson*, 529 U.S. at 143 ("[I]f tobacco products were within the FDA's jurisdiction, the Act would require the FDA to remove them from the market entirely. But a ban would contradict Congress'[s] clear intent as expressed in its more recent, tobacco-specific legislation. The inescapable conclusion is that *there is no room for tobacco products within the FDCA's regulatory scheme*.") (emphasis added). No such "inescapable conclusion" exists here. *See id.*

Moreover, in *Brown & Williamson*, Congress's tobacco-specific legislation "creat[ed] a distinct regulatory scheme" that was enacted "against the background of the FDA repeatedly and consistently asserting that it lacks jurisdiction under the FD

> "Currently, the Commission has limited authority to prevent abusive practices in this area. The Federal Trade Commission Act (the 'FTC Act'), 15 U.S.C. §§ 41 *et seq.*, grants the Commission authority to seek relief for violations of the Act's prohibitions on unfair and deceptive practices in and affecting commerce, an authority limited in this context 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) (Chairman Robert Pitofsky proposing that, under new legislation, "[w]eb sites would be required to take reasonable steps to protect the security and integrity" of "personal identifying information from or about consumers" collected "online");
>
> "The Commission's authority over the collection and dissemination of personal data collected online stems from Section 5 of the Federal Trade Commission Act (the 'FTC Act' or 'Act'), and the Children's Online Privacy Protection Act ('COPPA') . . . . As a general matter, however, the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites, or portions of their Web sites, not directed to children." FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, at 33-34 (2000);
>
> "The 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. It has the authority to challenge deceptive practices." Jeffrey Benner, *FTC Powerless to Protect Privacy*, Wired, May 31, 2001 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC).

(11/7/13 Tr. at 19:22-21:5, 24:5-26:4; HR's Mov. Br. at 10-11).[7]

Subcomm. on Terrorism, Tech. & Homeland S

not only adopt an extremely strained understanding of 'safety' as it is used throughout the Act—a concept central to the FDCA's regulatory scheme—but also ignore the plain implication of Congress'[s] subsequent tobacco-specific legislation." 529 U.S. at 159-60.

To be sure, the Court's analysis herein does not simply rest on how "important, conspicuous, and controversial" data security is. *See Brown & Williamson*, 529 U.S. at 161. Undoubtedly, "an administrative agency's power to regulate in the public interest must always be grounded in a valid grant of authority from Congress." *Id.*

And, to that end, the Court is guided by precedent that compels rejecting Hotels and

in this case" without "rules, regulations, or other guidelines explaining what data-security practices the Commission believes Section 5 to forbid or require." (HR's Mov. Br. at 15). Hotels and Resorts contends that the FTC's "failure to publish any interpretive guidance whatsoever" violates fair notice principles and "bedrock principles of administrative law." (Jnt. Supp. Br. at 4 (citing *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) and *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008))).

Hotels and Resorts further asserts that, generally, agencies cannot rely on enforcement actions to make new rules and concurrently hold a party liable for violating the new rule. (HR's Mov. Br. at 15). Indeed, Hotels and Resorts avers that, to do so, the agency must have previously set forth with *ascertainable certainty* the standards it expects private parties to obey—but that the FTC's mere reasonableness standard provides no such guidance "in the highly complex and sophisticated world of data security." (D.E. No. 115, Reply in Support of Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC ("HR's Reply Br.") at 5-6 (citing *Dravo Corp. v. Occupational Safety & Health Review Comm'n*, 613 F.2d 1227, 1233 (3d Cir. 1980))). Hotels and Resorts adds that the FTC's prior consent decrees and its business guidance brochure provide no such guidance. (*Id.* at 6-7; Jnt. Supp. Br. at 5 ("[C]onsent decrees do not constrain FTC discretion and thus cannot provide any meaningful notice to third parties. . . . And the informal brochure on which the FTC so heavily relies . . . is far too vague to provide meaningful guidance, particularly in the complex world of data security.") (citations omitted)).

Hotels and Resorts argues that, moreover, the FTC "can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires"—and that the FTC has not done so here. (HR's Reply to Jnt. Supp. Br. at 3). Hotels and Resorts accordingly argues that, since neither the FTC nor Section 5 itself provides "fair notice," the Court should

dismiss the instant action. (HR's Mov. Br. at 17; *see also* HR's Reply Br. at 4 ("Section 5 also does not permit the FTC to bring data-security enforcement actions without first publishing rules or regulations explaining in advance what parties must do to comply with the law." (citing Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 Geo. Mason L. Rev. 673 (2013)))).

In response, the FTC argues that, in the data-security context, "reasonableness is the touchstone" and that "unreasonable data security practices are unfair." (FTC's Opp. Br. at 17). The FTC contends that the Court can evaluate the reasonableness of Hotels and Resorts' data-security program in view of the following guidance: (1) industry guidance sources that Hotels and Resorts itself seems to measure its own data-security practices against; and (2) the FTC's business guidance brochure and consent orders from previous FTC enforcement actions. (*Id.* at 17-20).

The FTC also asserts that data-security standards can be enforced in an industry-specific, case-by-case manner and, further, that it has the discretion to enforce the FTC Act's prohibition of unfair practices through individual enforcement action rather than rulemaking. (*Id.* at 20, 22). And it argues that the "ascertainable certainty

years of FTC precedent" because "the FTC could never protect consumers from unfair practices without first issuing a regulation governing the specific practice at issue." (Jnt. Supp. Br. at 9).

b. Analysis

"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." *Fox Television Stations, Inc.*, 132 S. Ct. at 2317. At times, Hotels and Resorts seems to improperly characterizes the issue as being whether the FTC must provide any fair notice at all. (*See* HR's Reply to Jnt. Supp. Br. at 3 ("The FTC's primary response is that it is not obligated to provide any fair notice at all . . . .")). But this is not the issue. Instead, the issue is whether fair notice *requires* the FTC to formally issue rules and regulations before it can file an unfairness claim in federal district court. And, to that extent, the Court is not so persuaded.

"[W]here an agency . . . is given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency." *PBW Stock Exch., Inc. v. SEC*, 485 F.2d 718, 732 (3d Cir. 1973) (citing *NLRB v. Wyman-Gordon Co.*, 394 U.S. 759, 772 (1969) (Black, J., concurring); *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947)). After all, "problems may arise in a case which the administrat[ive] agency could not reasonably foresee" or "the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule" or "the problem may be so specialized and varying in nature as to be impossiblu fasquired."

Comm'n, 528 F.2d 645, 649-50 (5th Cir. 1976)). Indeed, "ascertainable certainty" is the "applicable standard for fair notice." *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008).

Correspondingly, Hotels and Resorts asserts that "*Beverly* holds that the 'ascertainable certainty' standard applies," but that "Section 5 contains nothing but generalized, vague language, and the FTC has failed to remedy that vagueness by 'provid[ing] a sufficient, publicly

accepting Hotels and Resorts' proposition would necessarily require the Court to sidestep long-standing precedent, detailed above, that suggests precisely the opposite—i.e., that the FTC does *not* necessarily need to formally publish rules and regulations since the proscriptions in Section 5 are necessarily flexible.

To be sure, the Court finds that neither *Dravo* nor *Beverly* requires the FTC to formally publish a regulation before bringing an enforcement action under Section 5's unfairness prong. Indeed, the Third Circuit has affi

citation, it implicates the Due Process Clause of the Fifth Amendment."); *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995) ("In the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."). Hotels and Resorts uses these precepts to argue that the FTC must issue regulations—or else an FTC unfairness claim must be dismissed.

But the Court is unpersuaded that regulations are the *only* means of providing sufficient fair notice. Indeed, Section 5 codifies a three-part test that proscribes whether an act is "unfair." *See* 15 U.S.C. § 45(n). And, notably, Hotels and Resorts' only response to the FTC's analogy to tort liability—where liability is routinely found for unreasonable conduct *without* the need for particularized prohibitions—is the following: "While the negligence standard has long been a cornerstone of tort law, no Article III court has *ever—not once*—articulated the data-security standards that Section 5 of the FTC Act supposedly imposes on regulated parties." (HR's Reply to Jnt. Supp. Br. at 5). The Court is not persuaded by this argument that essentially amounts to: since no court has, no court can—especially since Hotels and Resorts itself recognizes how "quickly" the digital age and data-security world is moving. (*See* 11/7/13 Tr. at 25:12-14).

Furthermore, agencies in other circumstances can bring enforcement actions without issuing the particularized prohibitions that Hotels and Resorts demands here. *See* 29 U.S.C. § 158(d) (proscribing the NLRB's requirement that "to bargain collectively is the performance of the mutual obligation of the employer and the representative of the employees to meet at reasonable times and confer in *good faith* with respect to wages, hours, and other terms and conditions of employment") (emphasis added); 29 U.S.C. § 654 (requiring, under OSHA, that each employer must "furnish to each of his employees employment and a place of employment

which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees").

Again, given the rapidly-evolving nature of data security, the Court is not persuaded by Hotels and Resorts' attempt to undermine the FTC's analogies involving the National Labor Relations Act and OSHA on the grounds that precedent is lacking. (*See* HR's Reply Br. at 7 ("Unlike data-security regulation under Section 5, the duty to negotiate in good faith has a long-established meaning in contract law. . . . Similarly, there are over 30 years of concrete, specific agency guidelines specifying the obligations imposed by the General Duty Clause.") (citation omitted)).

And, that the Department of Homeland Security and the National Institute of Standards and Technology have purportedly "managed" to "craft generalized data-security rules" is inapposite to the issue here. (*See* Jnt. Supp. Br. at 4). Hotels and Resorts argues that, since these agencies have issued such rules, the FTC "can certainly do the same." (*Id.* at 5). In other words, Hotels and Resorts argues that, because the FTC has the power to issue particularized regulations and that it is plausible to do so, it *must*. (*See id.*

despite the FTC's many public complaints and consent agreements, as well as its public statements and business guidance brochure—and despite Hotels and Resorts' *own* references to "industry standard practices" and "commercially reasonable efforts" in its privacy policy. (*See* Compl. ¶ 21).[11]

The Court declines to do so. *See FTC v. R.F. Keppel & Bro.*, 291 U.S. 304, 310 n.1 (1934) ("It is believed that the term 'unfair competition' has a legal significance which can be enforced by the commission and the courts, and that it is no more difficult to determine what is unfair competition than it is to determine what is a reasonable rate or what is an unjust discrimination."); *Voegele*, 625 F.2d at 1077-78 (affirming that the disputed language in an OSHA regulation implied "an objective standard[,] the reasonably prudent person test," which is not unconstitutionally vague).

Indeed, "the rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment *to which courts and litigants may properly resort for guidance*." *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976) (emphasis added) (internal quotation marks omitted), *superseded by statute on other grounds*, Pregnancy Discrimination Act, 42 U.S.C. § 2000e-(k). Hotels and Resorts' argument that consent orders do not carry the force of law, therefore, misses the mark.[12]

---

[11] *See, e.g.*, Protecting Personal Information: A Guide for Business (2007), http://business ftc.gov/sites/default/files/pdf/bus69-protech

Finally, the Court is not convinced that this outcome affirms Section 5's vagueness such that "FTC data-security actions . . . would be exempted from Rule 12(b)(6) scrutiny," as Hotels and Resorts contends. (*See* HR's Reply Br. at 8). This position ignores that, in addition to various sources of guidance for measuring reasonableness, a statutorily-defined standard exists for asserting an unfairness claim. *See* 15 U.S.C. § 45(n). Moreover, the Court must consider the untenable consequence of accepting Hotels and Resorts' proposal: the FTC would have to cease bringing *all* unfairness actions without first proscribing particularized prohibitions—a result that is in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act.

3. Whether the FTC alleges substantial, unavoidable consumer injury and otherwise satisfies federal pleadings requirements

a. <u>The parties' contentions</u>

Hotels and Resorts proclaims that an unfair practice must, by statute, cause or be likely to cause "*substantial injury to consumers* which is *not reasonably avoidable* by consumers themselves"—but that consumer injury from theft of payment card data is never substantial and always avoidable. (HR's Mov. Br. at 19 (quoting 15 U.S.C. § 45(a))).

More specifically, Hotels and Resorts contends that federal law places a $50 limit on consumer liability for unauthorized use of a payment card and that all major credit card brands waive liability for even this small amount. (*Id.*). And Hotels and Resorts contends that consumers can have their issuer rescind any unauthorized charges. (*Id.*). Hotels and Resorts argues that consumers, therefore, cannot suffer any "substantial injury" from the breaches that were not reasonably avoidable. (*Id.* at 19-20). Hotels and Resorts adds that any "incidental injuries that consumers suffered," such as monitoring financial information, is insufficient. (*Id.* at 20-21 (citing *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011))).

Finally, Hotels and Resorts asserts that the FTC's complaint fails "basic pleading requirements" because the FTC alleges "legal conclusions couched as factual allegations" and fails to adequately plead causation. (*Id.* at 22-23). As to causation specifically, Hotels and Resorts argues that the FTC does not allege "*how* the alleged data-security failures caused the intrusions, or *how* the intrusions resulted in any particular consumer harm." (*Id.* at 23).

In opposition, the FTC argues that its complaint pleads sufficient facts to support an unfairness claim involving data-security practices as follows: (1) that substantial injury resulted from Hotels and Resorts' unreasonable data-security practices; (2) this injury was not reasonably avoidable by consumers; (3) Hotels and Resorts' practices caused this injury; and (4) Hotels and Resorts' practices were unreasonable and there were no countervailing benefits to Hotels and Resorts' failure to address its data-security flaws. (FTC's Opp. Br. at 3-4).

b. Analysis

The Court finds that the FTC's complaint sufficiently pleads an unfairness claim under the FTC Act and satisfies Federal Rule of Civil Procedure 8(a). An act or practice is unfair if it

> [E]xposure of consumers' personal information has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses. For example, Defendants' failure to implement reasonable and appropriate security measures resulted in the three data breaches . . . the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and *more than $10.6 million in fraud loss. Consumers* and businesses suffered *financial injury*, including, but not limited to, *unreimbursed fraudulent charges*, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.

(Compl. ¶ 40 (emphasis added)). For purposes of resolving Hotels and Resorts' motion, these

reasonable inferences in favor of the FTC, not Hotels and Resorts. *See Phillips v. Cnty. Of Allegheny*

Hannaford Bros. Co., 659 F.3d 151, 164-65 (1st Cir. 2011) (expl

Similarly, the FTC alleges that Defendants "failed to adequately inventory computers connected to Hotels and Resorts' network so that Defendants could appropriately manage the devices on its network." (*Id.* ¶ 24(g)). And the FTC correspondingly alleges that, since "Defendants did not have an adequate inventory of the Wyndham-branded hotels' computers connected to its network . . . they were unable to physically locate those computers" and, therefore, "Defendants did not determine that Hotels and Resorts' network had been compromised until almost four months later." (*Id.* ¶ 27).

Likewise, the FTC alleges that Defendants failed to "use readily available security measures to limit access between and among the Wyndham-branded hotels' property management systems," such as firewalls. (*Id.* ¶ 24(a)). And this aligns with the FTC's allegation that intruders "were able to gain unfettered access to the property management systems servers of a number of hotels" because "Defendants did not appropriately limit access between and among the Wyndham-branded hotels' property management systems, Hotels and Resorts' own corporate network, and the Internet—such as through the use of firewalls." (*Id.* ¶ 28).

Finally, the FTC alleges that this "failure to implement reasonable and appropriate security measures exposed consumers' personal information to unauthorized access, collection, and use" and "has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses." (*Id.* ¶ 40). Drawing inferences in favor of the FTC, the identified failures caused the breaches, resulting in the alleged substantial injury. *See Phillips*, 515 F.3d at 231.

At its root, Hotels and Resorts' challenge to the FTC's injury and causation allegations is essentially an appeal for a heightened pleading standard. Hotels and Resorts seems to ask this

Court to read a "recklessness or egregiousness" requirement into the statutorily-defined unfairness standard. (*See* HR's Mov Br. at 22). Similarly, it argues that the FTC should have to plead the precise consumer harm, the "exact alleged deficiencies" that caused the "theft of the information," and how the breaches caused the alleged harm—because, as a government agency, the FTC conducted a pre-suit investigation. (*Id.* at 23; 11/7/13 Tr. at 101:13-102:14, 104:19-23, 108:3-7).

But the Court declines to impose such a heightened standard because Hotels and Resorts cites no authority to this effect. (*See, e.g.*, HR's Mov. Br. at 23 (stating that, "[a]fter a two-year investigation into [Hotels and Resorts'] data-security practices, surely the FTC should be required to say more about how the alleged vulnerabilities 'result[ed]' in consumer harm," but citing no authority)).

ii. *"Reasonably avoidable" allegations*

Second, the FTC adequately pleads that the alleged substantial injury *was not reasonably avoidable*. Hotels and Resorts argues that "[c]onsumers can . . . always 'reasonably avoid' any financial injury stemming from the theft of payment card data simply by having their issuer rescind any unauthorized charges." (HR's Mov. Br. at 19 (citing 15 U.S.C. § 1643(a)(1)); *see also* HR's Reply Br. at 9 ("Even accepting as true the FTC's unsubstantiated allegation that some consumers might not have been reimbursed . . . federal law and card-brand zero-liability policies make clear that any such charges were nonetheless 'reasonably avoidable' by consumers.")). Hotels and Resorts thus effectively asks the Court to hold that, as a matter of law, any financial injury from payment card theft data is reasonably avoidable and that the FTC's allegation to the contrary, (Compl. ¶¶ 40, 43, 48), could not be true under any factual scenario.

implication, that they had implemented reasonable and appropriate measures to protect personal information against unauthorized access"—but that "Defendants did not implement reasonable and appropriate measures to protect personal information against unauthorized access." (Compl. ¶¶ 21, 44-45). Accordingly, the FTC alleges that Defendants' representations "are false or misleading and constitute deceptive acts or practices" under Section 5(a) of the FTC Act. (*Id.* ¶ 46).

1. <u>The parties' contentions</u>

security practices were "standard" in the hospitality industry or how Hotels and Resorts' practices fell short. (*Id.*).

Finally, Hotels and Resorts asserts that the FTC "does nothing to explain how the alleged deficiencies it identifies placed personal information *collected by [Hotels and Resorts]* at risk"

have reached different conclusions as to whether claims under the FTC Act must satisfy Rule 9(b)'s heightened pleading standard.[17] This is an issue of first impression in this District.

Rule 9(b) provides that, "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." To establish liability for the deception prong of Section 5(a), "the FTC must establish: '(1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances, and (3) the representation was material.'"

543 F. Supp. 2d at 314 (explaining that Defendants do not

devices on its network," "failed to employ reasonable measures to detect and prevent unauthorized access to Defendants' computer network or to conduct security investigations," and "failed to follow proper incident response procedures, including failing to monitor Hotels and Resorts' computer network for malware used in a previous intrusion." (*Id.* ¶¶ 24(g)-(i) (identifying various practices that allegedly exposed consumers' personal data)).

Hotels and Resorts dismisses these allegations as "conclusory statements of wrongdoing." (HR's Mov. Br. at 27 (asserting that "the FTC makes a half-hearted attempt to allege that [Hotels and Resorts] made deceptive statements about *its own* data-security practices")). But the Court is not so persuaded. Indeed, Hotels and Resorts' argument again seems to be a repackaging of its fair-notice challenge. (*See* 11/7/13 Tr. at 141:9-16). The Court has, however, already rejected this challenge.

Moreover, accepting Hotels and Resorts' position leads to the following incongruous result: Hotels and Resorts can explicitly represent to the public that it "safeguard[s] . . . personally identifiable information by using industry standard practices" and makes "commercially reasonable efforts" to make collection of data "consistent with all applicable laws and regulations"—but that, as a matter of law, the FTC cannot even file a complaint in federal court challenging such representations without first issuing regulations. *See Voegele*, 625 F.2d at 1078-79; *see also Iqbal*, 556 U.S. at 679 ("Determining whether a complaint states a plausible claim for relief will . . . be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.").

Furthermore, the Court is not convinced that the FTC's other allegations mandate dismissal of its deception claim because, according to Hotels and Resorts, they "concern[] the state of data-security *at the Wyndham-branded hotels*" and that the three breaches involved

collection" of data, and only applies "to the extent we control the Information." (*Id.* at 25 (quoting D.E. No. 91-3, Ex. A to Declaration of Jennifer A. Hradil ("Hradil Decl.") at 1)). Hotels and Resorts also cites language in the policy th

unpersuasive Hotels and Resorts' argument that the FTC "does nothing to explain how the

9(b) requires pleading with specificity, it does not erase the general standard that the Court should draw reasonable inferences in favor of Plaintiffs." (citing *Lum v. Bank of Am.*, 361 F.3d 217 (3d Cir. 2004))).

Moreover, the impression that a reasonable consumer would have had after reading the privacy policy seems to involve fact issues th