FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

FEDERAL TRADE COMMISSION,	:	
Plaintiff,	:	
v.	:	**Civil Action No. 13-1887 (ES)**
WYNDHAM WORLDWIDE CORPORATION, et al.,	:	**OPINION**
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 authority to assert an unfairness claim in the data-security context. Citing recent data-security legislation and the FTC's public statements, Hotels and Resorts likens this action to *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000). It declares that, under *Brown & Williamson*, the FTC does not have the authority to bring an unfairness claim involving data security. As explained below, however, the Court rejects this challenge to the FTC's authority because the circumstances here differ from those in *Brown & Williamson*.

Second, Hotels and Resorts asserts that the FTC must formally promulgate regulations before bringing its unfairness claim. It contends that, without promulgating such regulations, the FTC violates fair notice principles. But precedent instructs that agencies like the FTC need not formally issue regulations. The Court, therefore, rejects Hotels and Resorts' contention that the FTC must issue regulations before bringing its unfairness claim.

Third, Hotels and Resorts argues that the FTC's allegations are pleaded insufficiently to support either an unfairness or deception claim. Hotels and Resorts asserts that the FTC fails to plead certain elements of each of these claims and fails to otherwise satisfy federal pleading requirements. As detailed below for both the unfairness and deception claims, the Court disagrees.

Having resolved each of these issues in favor of the FTC, the Court DENIES Hotels and Resorts' motion to dismiss.

[1] Wyndham Worldwide, Hotel Group and Hotel Management separately move to dismiss the FTC's complaint, (D.E. No. 92), which the Court will address in a separate opinion. On November 7, 2013, the Court heard oral argument on both motions to dismiss. (*See* D.E. No. 139 ("11/7/13 Tr.")).

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 court is not required to accept as true "legal conclusions," and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678.

Finally, "[i]n deciding a Rule 12(b)(6) motion, a court must consider only the complaint, exhibits attached to the complaint, matters of the public record, as well as undisputedly authentic

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 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." (HR's Mov. Br. at 1). Hotels and Resorts asserts that the FTC's action "is the Internet equivalent of punishing the local furniture store because it was robbed and its files raided." (*Id.* at 21).

But Hotels and Resorts' motion to dismiss demands that this Court carve out a data-security exception to the FTC's authority and that the FTC publish regulations before filing an unfairness claim in federal court. These demands are, in fact, what bring us into unchartered territory. And, after having wrestled with arguments in the parties' initial briefing, oral

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 practices" under Section 5 of the FTC Act. (*Id.* ¶¶ 48-49).

1. Whether *Brown & Williamson* preempts the FTC's authority over data security

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

Hotels and Resorts analogizes this action to *Brown & Williamson*, arguing that the FTC's unfairness authority does not cover data security. (HR's Mov. Br. at 7-8, 14). Hotels and

[3] The Court previously granted leave for the following entities to file brief *amici curiae*: the International Franchise Association, (D.E. No. 119); the Chamber of Commerce of the United States of America, Retail Litigation Center, American Hotel & Lodging Association, and National Federation of Independent Business, (D.E. No. 120); TechFreedom, International Center for Law & Economics, and Consumer Protection Scholars Justin Hurwitz, Todd J. Zywicki, and Paul Rubin, (D.E. No. 121); and Public Citizen, Inc. and Chris Jay Hoofnagle, (D.E. No. 122). The Court has considered these submissions and appreciates these entities' assistance in resolving Hotels and Resorts' motion.

Resorts argues that Congress has, in fact, settled on "a less extensive regulatory scheme" and passed narrowly tailored data-security legislation, indicating that these later-enacted laws "shape or focus" the meaning of Section 5. (*Id.* at 10, 14 (quoting *Brown & Williamson*, 529 U.S. at 143, 148)). Hotels and Resorts contends that this "overall statutory landscape" does not authorize the FTC to generally establish data-security standards for the private sector under Section 5. (*Id.* at 7-8).

Specifically, Hotels and Resorts identifies several statutes that purportedly authorize "particular federal agencies to establish minimum data-security standards in narrow sectors of the economy," including: the Fair Credit Reporting Act ("FCRA"); the Gramm-Leach-Bliley Act ("GLBA"); the Children's Online Privacy Protection Act ("COPPA"); and the Health Insurance Portability and Accountability Act of 1996 ("HIPPA"). (*Id.* at 9, 9 n.1 (discussing statutes and citing respective statutory codifications)).[4]

Hotels and Resorts also references pending legislation, namely the Cyber Intelligence Sharing and Protection Act ("CISPA"), arguing that this would "abandon[] any attempt to create comprehensive cybersecurity performance requirements" and is "irreconcilable" with the FTC's data-security regulation since this legislation would exempt liability in certain circumstances. (*Id.* at 12-13).

Hotels and Resorts further argues that, like the FDA's disclaimers over tobacco regulation in *Brown & Williamson*, the FTC has disclaimed authority to regulate data security under Section 5's unfairness prong and, in fact, has asked Congress to give it the very authority it "purports to wield in this case." (*Id.* at 10-11, 14). And Hotels and Resorts contends that, in view of the economic and political considerations associated with data security, "it defies

[4] Hotels and Resorts asserts that Congress's "targeted grants of authority would make no sense if Section 5 already gave the FTC authority to regulate data security in *all* circumstances." (D.E. No. 152-1, Joint Supplemental Letter Brief ("Jnt. Supp. Br.") at 1 (citing the FCRA, GLBA, and COPPA)).

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.* at 142. But, the Court determined that this "would *contradict* Congress'[s] clear intent as expressed in its more recent, tobacco-specific legislation" in which it "foreclosed the removal of tobacco products from the market." *Id.* at 137, 143 (emphasis added). The Supreme Court explained that "Congress, for better or for worse, has created a distinct regulatory scheme for tobacco products, squarely rejected proposals to give the FDA jurisdiction over tobacco, and repeatedly acted to *preclude* any agency from exercising significant policymaking authority in the area." *Id.* at 159-60 (emphasis added).

But no such dilemma exists here. Hotels and Resorts fails to explain how the FTC's unfairness authority over data security would lead to a result that is incompatible with more recent legislation and thus would "plainly *contradict* congressional policy." *See Brown & Williamson*, 529 U.S. at 139 (emphasis added); *see also Massachusetts v. EPA*, 549 U.S. 497,

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 FDCA to regulate tobacco products as customarily marketed." *Id.* at 155-56. In fact, the FDA's assertion to regulate tobacco was "[c]ontrary to its representations to Congress since 1914." *Id.* at 159. Thus, Congress ratified the "FDA's *plain and resolute position* that the FDCA gives the agency *no authority to regulate* tobacco products as customarily marketed." *Id.* (emphasis added).

Here, however, the FTC representations identified by Hotels and Resorts do not amount to an analogous position that would, as a matter of law, support precluding the FTC from bringing any enforcement action in the data-security context. Specifically, Hotels and Resorts seems to rely on the following three representations that purportedly show the FTC disclaiming authority over data security:

[6] Notably, the FTC contends that "Section 45(n) places limitations on the Commission's authority to declare particular actions unfair under Section 5[] either in litigation or rulemaking" and that "[i]t has no application where Congress itself has statutorily defined categories of actions to be unlawful and authorized the FTC to enforce those statutes." (Jnt. Supp. Br. at 7 n.1). Although it had an opportunity do so, Hotels and Resorts revealingly leaves this contention unrebutted. (*See generally* HR's Reply to Jnt. Supp. Br. at 3).

- "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]

But the Court is not convinced that these statements, made within a three-year period, equate to a resolute, unequivocal position under *Brown & Williamson* that the FTC has *no* authority to bring *any* unfairness claim involving data security. *See* 529 U.S. at 156-59. In fact, as Hotels and Resorts must concede, the FTC brought unfairness claims in the data-security context shortly after these representations. (*See* 11/7/13 Tr. at 25:20-24, 74:9-12 (presenting timeline of events showing the FTC bringing unfairness claims in the data-security context in 2005)). And the FTC's subsequent representations confirm its authority in this arena, not deny it. *See, e.g.*, *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing before the*

[7] For the reader's convenience and simplicity's sake, the Court reproduces portions of the FTC's representations and the related citations from Hotels and Resorts' briefing and presentation at oral argument.

Subcomm. on Terrorism, Tech. & Homeland Sec. of the S. Comm. on the Judiciary, 110th Cong. at 5-6 (Mar. 21, 2007).

Although Hotels and Resorts reasonably contends that the "digital age is moving much more quickly [such that] the timeframe here is compressed," the public record here is unlike the lengthy, forceful history of repeated and consistent disavowals in *Brown & Williamson*. Thus, even accepting that the FTC shifted its stance on data security, this cannot limit its authority without more. *See Brown & Williamson*, 529 U.S. at 156-57 ("Certainly, an agency's initial interpretation of a statute that it is charged with administering is not 'carved in stone.'").

Notably, Hotels and Resorts avers that the FTC never indicated that it *did* have unfairness authority over data security in the three-year period that Hotels and Resorts relies upon:

> Where is there any where from 1998 to 2001 where the FTC is telling Congress or even the Executive Branch, that [it has] this authority, so there is no need to do anything? There is nowhere. . . . I would submit the FTC actually doesn't have anything where they go to Congress and in 2000 say we have this authority. There is nothing you need to do.

(11/7/13 Tr. at 26:9-17).

Tellingly, however, Hotels and Resorts fails to explain how this is a relevant consideration under *Brown & Williamson*. Said differently, Hotels and Resorts analogizes this case to *Brown & Williamson*—but fails to explain how *Brown & Williamson* requires a federal agency to *affirm* its authority before asserting it.

Thus, although "subsequent acts can shape or focus" a range of "plausible meanings" that a statute may have, the data-security legislation and the FTC's representations cited by Hotels and Resorts do not call for a data-security exception to the FTC's unfairness authority. *See Brown & Williamson*, 529 U.S. at 143. After all, *Brown & Williamson* was "hardly an ordinary case" because, "[t]o find that the FDA has the authority to regulate tobacco products, one must

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 Resorts' request to carve out a data-security exception to the FTC's authority. *See, e.g.*, *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972) ("When Congress created the Federal Trade Commission in 1914 and charted its power and responsibility under [Section] 5, it explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply." (citing S. Rep. No. 597, at 13 (1914))); *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 967 (D.C. Cir. 1985) ("Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission in 1914 to define unfair practices on a flexible, incremental basis.").[8]

2. Whether the FTC must promulgate rules and regulations to satisfy fair notice principles

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

Hotels and Resorts argues that, even if Section 5 gives the FTC sufficient authority, "it would violate basic principles of fair notice and due process to hold [Hotels and Resorts] liable

[8] The parties vigorously dispute whether a recent FTC administrative adjudication—*LabMD, Inc.*, 2014 WL 253518 (2014) (unanimous commission review)—is entitled to *Chevron* deference. (*See* Jnt. Supp. Br. at 6; HR's Reply to Jnt. Supp. Br. at 1-2). But, even without deferring to the agency's interpretation of Section 5 in *LabMD*, the Court finds that *Brown & Williamson* is distinguishable and thus need not resolve this deference issue.

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" standard does not apply—but that even if it did, reasonableness provides ascertainable certainty to companies. (11/7/13 Tr. at 74:7-19, 153:1-6; Jnt. Supp. Br. at 9 n.2).

Indeed, the FTC analogizes its enforcement action here to other circumstances where agencies bring actions without "particularized prohibitions," such as those involving the National Labor Relations Board ("NLRB") and the Occupational Safety and Health Act ("OSHA"). (FTC's Opp. Br. at 23). In short, the FTC argues that fair notice does *not* necessarily require issuing regulations—and that accepting Hotels and Resorts' argument "would undermine 100

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 impossible of capture within the boundaries of a general rule." *Chenery*, 332 U.S. at 202-03; s*ee also Am. Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990) ("[A]gency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication. The Commission seems on especially

solid ground in choosing an individualized process where important factors may vary radically from case to case.") (citations omitted).[9]

Indeed, "the proscriptions in [Section] 5 are flexible, to be defined with particularity by the myriad of cases from the field of business." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) (internal quotation marks omitted) (explaining that "[t]his statutory scheme necessarily gives the Commission an influential role in interpreting [Section] 5 and in applying it to the facts of particular cases arising out of unprecedented situations"); *see also Sperry & Hutchinson*, 405 U.S. at 239-40.

Accordingly, Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts *without* preexisting rules or regulations specifically addressing the conduct-at-issue. *See, e.g.*, *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1153, 1155-59 (9th Cir. 2010) (affirming summary judgment in favor of the FTC for violation of Section 5's unfairness prong where website "created and delivered unverified checks at the direction of registered users" and "fraudsters and con artists extensively abused the website"); *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1191, 1193-95 (10th Cir. 2009) (affirming summary judgment in favor of the FTC for violation of Section 5's unfairness prong where website sold personal data, explaining that "conduct may constitute an unfair practice under § 5(a) of the FTCA even if it is not otherwise unlawful").

Hotels and Resorts insists that an agency "has the responsibility to state with ascertainable certainty what is meant by the standards [it] has promulgated." *Dravo Corp.*, 613 F.2d at 1232-33 (quoting *Diamond Roofing Co. v. Occupational Safety & Health Review*

[9] *See also FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 520 (2009) ("[T]he agency's decision to consider the patent offensiveness of isolated expletives on a case-by-case basis is not arbitrary or capricious."); *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 294 (1974) ("It is doubtful whether any generalized standard could be framed which would have more than marginal utility. The Board thus has reason to proceed with caution, developing its standards in a case-by-case manner with attention to the specific character of the buyers' authority and duties in each company.").

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 accessible statement' of what the statute requires." (HR's Reply to Jnt. Supp. Br. at 4 (quoting *Beverly Healthcare-Hillview*, 541 F.3d at 202)).

But this does not mean that any ambiguity in a regulation prevents punishment. *Beverly Healthcare-Hillview*, 541 F.3d at 202. Instead, the "ascertainable certainty" standard applies when:

> (1) the agency had given conflicting public interpretations of the regulation, or, (2) the regulation is so vague that the ambiguity can only be resolved by deferring to the agency's own interpretation of the regulation (i.e., a situation in which the ambiguity is resolved by something comparable to a step-two analysis under *Chevron*), and the agency has failed to provide a sufficient, publicly accessible statement of that interpretation before the conduct in question.

Id. (quoting *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004)).

The parties strongly contest whether the ascertainable certainty standard applies. (*See* Jnt. Supp. Br. at 4, 9 n.2; HR's Reply to Jnt. Supp. Br. at 4). Notwithstanding this dispute, however, Hotels and Resorts' arguments boil down to one proposition: the FTC cannot bring an enforcement action under Section 5's unfairness prong without first formally publishing rules and regulations. And Hotels and Resorts does *not* limit this to the data-security context.[10] But

[10] At oral argument, for instance, the FTC argued that Hotels and Resorts demands that, "for every unfairness case that the FTC brings, there must first be a rule" and that the FTC did not "think the argument was just on data-security cases," but "all unfairness cases." (11/7/13 Tr. at 99:3-7). Hotels and Resorts did not contest this argument.

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 affirmed that "it is within the [agency's] discretion whether to proceed between ad hoc litigation or regulation." *Voegele Co. v. Occupational Safety & Health Review Comm'n*, 625 F.2d 1075, 1079 (3d Cir. 1980); *see also PBW Stock Exch.*, 485 F.2d at 732 ("The courts have consistently held that where an agency, as in this case, is given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency.").

Undoubtedly, "laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *Fox Television Stations*, 132 S. Ct. at 2317; *see also Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2168 (2012) ("It is one thing to expect regulated parties to conform their conduct to an agency's interpretations once the agency announces them; it is quite another to require regulated parties to divine the agency's interpretations in advance or else be held liable when the agency announces its interpretations for the first time in an enforcement proceeding and demands deference."); *Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007) ("Even if the Secretary's interpretation were reasonable, announcing it for the first time in the context of this adjudication deprives Petitioners of fair notice. Where, as here, a party first receives actual notice of a proscribed activity through a

---

Indeed, Hotels and Resorts predicts that the Third Circuit will order the FTC to "go back and publish a regulation" since it is "an agency with rule[-]making authority." (*Id.* at 91:23-92:8).

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.*; 11/7/13 Tr. at 87:20-88:1 ("I think it is black letter law that an agency with rule-making authority, which they have, they have rule-making authority, Congress has given it to them, that when they are going to take action, enforcement actions, they have to publish rules in order to give companies fair notice of what is prohibited by their actions.")).

But the contour of an unfairness claim in the data-security context, like any other, is necessarily "flexible" such that the FTC can apply Section 5 "to the facts of particular cases arising out of unprecedented situations." *See Colgate-Palmolive Co.*, 380 U.S. at 384-85. And, Hotels and Resorts invites this Court to dismiss the FTC's complaint on fair notice grounds

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-protecting-personal-information-guide-business_0.pdf. The FTC also cites its various administrative complaints and consent orders—the public accessibility of which are not contested by Hotels and Resorts. (*See* FTC's Opp. Br. at 19; HR's Reply Br. at 6).

[12] Hotels and Resorts asserts that "[s]tatements that do not constrain governmental authority do not provide the fair notice that due process requires." (HR's Reply Br. at 7 (citing *City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999)). The Court finds Hotels and Resorts' reliance on *Morales* unconvincing. *See* 527 U.S. at 63-64 ("That the police have adopted *internal* rules limiting their enforcement to certain designated areas in the city would not provide a defense to a loiterer who might be arrested elsewhere. Nor could a person who knowingly loitered with a well-known gang member anywhere in the city safely assume that they would not be ordered to disperse no matter how innocent and harmless their loitering might be.") (emphasis added).

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. The parties' contentions

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 (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) is "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Hotels and Resorts challenges the FTC's allegations as to the first two elements of this standard, as well as the FTC's purported use of "conclusory standards." (*See* HR's Mov. Br. at 19, 22; 11/7/13 Tr. at 129:7-13). The Court accordingly addresses each of Hotels and Resorts' three contentions.

i. *"Substantial injury" and causation allegations*

First, the FTC adequately pleads "substantial injury to consumers" and that Hotels and Resorts' practices caused this injury. It pleads, in relevant part, that:

> [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 allegations must be "accepted as true." *See Iqbal*, 556 U.S. at 678.

Although the FTC alleges that both consumers *and* businesses suffered financial injury, Hotels and Resorts fails to cite any authority that necessarily preempts an unfairness action where the FTC alleges injury by both groups. Indeed, the FTC here alleges that at least some consumers suffered financial injury that included "unreimbursed financial injury" and, drawing inferences in favor of the FTC, the alleged injury to consumers is substantial. *See Am. Fin. Servs. Ass'n*, 767 F.2d at 972 ("An injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm.") (internal quotation marks and citations omitted).[13]

And the Court is not persuaded by Hotels and Resorts' argument that, since federal law places a $50 limit on the amount of consumer liability for any unauthorized use of a payment card, any alleged injury cannot be substantial. (HR's Mov. Br. at 19 (citing 15 U.S.C. § 1643(a)(1))). The FTC alleges *facts* to the contrary that the Court must accept as true, drawing

[13] Notably, Hotels and Resorts did not dispute the FTC's additional contention at oral argument that the FTC "can protect small businesses," (*see* 11/7/13 Tr. at 125:4-11), at oral argument or in supplemental briefing thereafter.

reasonable inferences in favor of the FTC, not Hotels and Resorts. *See Phillips v. Cnty. Of Allegheny*, 515 F.3d 224, 233-34 (3d Cir. 2008).[14]

Hotels and Resorts argues that the instant action is analogous to *Reilly*, where the Third Circuit affirmed dismissal of claims against a payroll-processing firm that was hacked because the plaintiffs had not suffered an "injury-in-fact." (HR's Mov. Br. at 20 (citing 664 F.3d at 40-41)). In *Reilly*, the Third Circuit set forth that

> Appellants have alleged no misuse, and therefore, no injury.
> . . . .
> In data breach cases where no misuse is alleged, however, there has been no injury—indeed, no change in the status quo. Here, Appellants' credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked. Moreover, there is no quantifiable risk of damage in the future.
> . . . .
> Although Appellants have incurred expenses to monitor their accounts and to protect their personal and financial information from imminent misuse and/or identity theft . . . they have not done so as a result of any *actual* injury (e.g. because their private information was misused or their identities stolen). Rather, they prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent.

Reilly, 664 F.3d at 44, 45-46 (internal quotation marks and citations omitted).[15]

But here, as noted above, the FTC has alleged misuse. (*See, e.g.*, Compl. ¶ 40). Thus, the Court finds that *Reilly* does not compel a finding that the FTC's allegations regarding substantial injury are insufficient as a matter of law. *See* 664 F.3d at 45-46; *see also Anderson v.*

[14] The FTC and Hotels and Resorts dispute whether federal law provides liability protection for debit cards. (FTC's Opp. Br. at 8; HR's Reply Br. at 9). For the reasons discussed above, however, this issue is not material to the Court's resolution of Hotels and Resorts' motion to dismiss.

[15] The parties contest whether non-monetary injuries are cognizable under Section 5 of the FTC Act. (HR's Mov. Br. at 20 (citing *Reilly*, 664 F.3d at 46); FTC's Opp. Br. at 8-9 (citing *Neovi*, 604 F.3d at 1158; *Accusearch*, 570 F.3d at 1194); HR's Reply Br. at 9 (citing *Am. Fin. Servs. Ass'n*, 767 F.2d at 973 n.18; *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007))). Although the Court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue given the analysis of the substantial harm element above.

Hannaford Bros. Co., 659 F.3d 151, 164-65 (1st Cir. 2011) (explaining that courts have reasoned that, "in the absence of unauthorized charges," plaintiffs "lacked a reasonable basis for fearing there would be unauthorized charges to their accounts as a result of the theft" and that this "*very reasoning suggests that these courts would reach a different result if the plaintiffs alleged that they had suffered fraudulent charges to their accounts*") (emphasis added).[16]

The FTC's allegations also permit the Court to reasonably infer that Hotels and Resorts' data-security practices *caused* theft of personal data, which ultimately *caused* substantial injury to consumers. The FTC alleges "a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." (Compl. ¶ 24). And, making reasonable inferences in favor of the FTC, these practices correspond to the allegations involving how intruders perpetrated three data breaches, (*see id.* ¶¶ 25-39)—which ultimately resulted in the alleged substantial injury, (*id.* ¶ 40).

For instance, the FTC alleges that Defendants "failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess" and "did not require the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allowed the use of easily guessed passwords." (*Id.* ¶ 24(f)). Correspondingly, the FTC alleges that "intruders attempted to compromise an administrator account on the Hotels and Resorts' network by guessing multiple user IDs and passwords—known as a brute force attack." (*Id.* ¶ 26).

[16] Hotels and Resorts attempts to discredit *Anderson* because that case "arose solely under Maine law . . . so the court had no opportunity to address whether such minor injury-avoidance costs constitute unavoidable 'substantial injury' under the FTC Act." (HR's Reply Br. at 10). But much of the precedent cited by the parties involves analogous circumstances. In fact, Hotels and Resorts itself relies on a case involving analysis under state law. (HR's Mov. Br. at 22 ("[C]ourts 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." (citing *Worix v. MedAssets, Inc.*, 869 F. Supp. 2d 893, 900 (N.D. Ill. 2012)))).

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.

But the Court cannot make such a far-reaching conclusion regarding an issue that seems fact-dependent. *See FTC v. Inc21.com*, 745 F. Supp. 2d 975, 1004 (N.D. Cal. 2010) (granting summary judgment in favor of the FTC and finding that the "unrebutted evidence supports a finding that the harm suffered by consumers was not reasonably avoidable").

iii. *Other purportedly "conclusory" allegations*

Third, the Court is not persuaded that the FTC's complaint otherwise fails federal pleading standards. Hotels and Resorts criticizes the FTC's use of terms such as "readily available," "adequate," "commonly-used," and "proper." (HR's Mov. Br. at 22 (quoting Compl. ¶ 24)). Hotels and Resorts argues that the "FTC does not give any factual detail as to what procedures, or combination of procedures, would have met those conclusory standards" and that the FTC "does not explain what measures would be 'reasonable.'" (*Id.*).

But the FTC does not merely allege that Hotels and Resorts' practices were unreasonable. *Cf. Willey v. J.P. Morgan Chase, N.A.*, No. 09-1397, 2009 WL 1938987, at *4 (S.D.N.Y. July 7, 2009) (finding that plaintiff did "not support [his] formulaic recitations with factual allegations that describe any insufficiency in [defendant's] security procedures, or with allegations that [defendant] lacked such procedures" or "how the procedures [defendant] adopted failed to comply with the [relevant] [g]uidelines").

Instead, the FTC describes several data-security insufficiencies, including: failing to employ firewalls; permitting "storage of payment card information in clear readable text"; failing to make sure Wyndham-branded hotels "implemented adequate information security policies and procedures prior to connecting their local computer networks to Hotels and Resorts' computer network"; permitting Wyndham-branded hotels "to connect insecure servers to Hotels and Resorts' networks, including servers using outdated operating systems that could not receive

security updates or patches to address known security vulnerabilities"; permitting servers on Hotels and Resorts' networks with commonly-known default user IDs and passwords; failing to "employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess"; failing to "adequately inventory computers connected to Hotels and Resorts' network" to manage devices on its network; failing to "monitor Hotels and Resorts' computer network for malware used in a previous intrusion"; and failing to restrict third-party access "such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary." (Compl. ¶¶ 24(a)-(j)).

The FTC therefore does more than simply assert "that a violation . . . must have occurred simply because the data loss incident occurred." *Cf. Willey*, 2009 WL 1938987, at *4. It alleges insufficiencies that, drawing reasonable inferences in favor of the FTC, led to data-security breaches. (*See* Compl. ¶¶ 24-39).

And, although the FTC does not plead the particularized data-security rules or regulations that Hotels and Resorts' procedures allegedly failed to comply with, this cannot preclude the FTC's enforcement action. *See Sperry & Hutchinson Co.*, 405 U.S. at 239-40; *Colgate-Palmolive Co.*, 380 U.S. at 384-85; *PBW Stock Exch.*, 485 F.2d at 732 (citing *Chenery Corp.*, 332 U.S. at 203). Indeed, Hotels and Resorts' challenge to this effect seems to be a repackaging of its fair notice argument—which this Court has considered and rejected.

B. The FTC's Deception Claim (Count One)

Hotels and Resorts also challenges the FTC's deception claim. (HR's Mov. Br. at 23). In this claim, the FTC cites the Defendants' privacy policy disseminated on Hotels and Resorts' website and alleges that, "in connection with the advertising, marketing, promotion, offering for sale, or sale of hotel services, Defendants have represented, directly or indirectly, expressly or by

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. The parties' contentions

Hotels and Resorts argues that the FTC's deception claim is insufficiently pleaded under either a heightened pleading requirement pursuant to Federal Rule of Civil Procedure 9(b) or the general pleading standard. (HR's Mov. Br. at 23-24). Hotels and Resorts contends that—although its online privacy policy was allegedly deceptive—the FTC "relies primarily on allegations concerning the state of data-security *at the Wyndham-branded hotels*." (*Id.* at 24).

To that extent, Hotels and Resorts asserts that the Wyndham-branded hotels are "legally separate entities that each maintain their own computer networks and engage in their own data-collection practices." (*Id.* at 24-25). Indeed, Hotels and Resorts avers that its privacy policy specifically *excludes* the Wyndham-branded hotels from the policy's data-security representations and that such exclusion of responsibility over franchisees' actions is consistent with franchise law. (*Id.* at 25-27).

Further, Hotels and Resorts argues that the FTC's allegations concerning Hotels and Resorts' own data-security practices "amount to nothing more than conclusory statements of wrongdoing that fall well short of establishing a 'plausible' claim to relief." (*Id.* at 27 (citing *Iqbal*, 556 U.S. at 678)). Hotels and Resorts argues that the FTC fails to allege what data-

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" and, therefore, there is "no basis in law or logic for pointing to the data breaches as evidence of 'deceptive' practices by [Hotels and Resorts]." (*Id.* at 28).

In opposition, the FTC asserts that, although a Section 5 claim of deceptive practices need not meet the Rule 9(b) heightened pleading standard, its complaint does so. (FTC's Opp. Br. at 26-27). The FTC argues that Hotels and Resorts, in fact, concedes certain allegations "are relevant to the data security measures of the Wyndham entities" and, therefore, that it has sufficiently pleaded a claim for deceptive data-security practices. (*Id.* at 28 (citing Compl. ¶¶ 24(g)-(i))).

The FTC also argues that it alleges that Hotels and Resorts was responsible for data-security failures by "permit[ing] computers with unreasonable data security measures on its network." (*Id.* at 27 (citing Compl. ¶ 24)). The FTC avers that, since the alleged data-security failures are "attributable" to Hotels and Resorts, the FTC need not plead "actual control" over the Wyndham-branded hotels' activities. (*Id.* at 28). The FTC adds, however, that the complaint nevertheless pleads such control "over the relevant aspects of the franchisees' data security practices." (*Id.* (citing Compl. ¶¶ 15, 17-19)).

2. <u>Analysis</u>

As an initial matter, the parties dispute whether the FTC must meet a heightened pleading standard under Federal Rule of Civil Rule 9(b) when alleging unlawful deception. District courts

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.'" *FTC v. Millennium Telecard, Inc.*, No. 11-2479, 2011 WL 2745963, at *3 (D.N.J. July 12, 2011) (quoting *FTC v. Tashman*, 318 F.3d 1273, 1277 (11th Cir. 2003)).[18]

This Court is not convinced that the FTC's deception claim requires Rule 9(b) treatment. *See FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1203 n.7 (10th Cir. 2005) ("A § 5 claim simply is not a claim of fraud as that term is commonly understood or as contemplated by Rule 9(b), and the district[] court's inclination to treat it as such unduly hindered the FTC's ability to present its case."). Indeed, Hotels and Resorts summarily asserts that the FTC's claim "'sounds in fraud,'" without any reasoning or analysis. (*See* HR's Mov. Br. at 24 (quoting *Lights of Am.*, 760 F. Supp. 2d at 853; *Ivy Capital*, 2011 WL 2118626, at *3)); *see also Med. Billers Network*,

[17] Some courts have explicitly ruled that Rule 9(b)'s heightened pleading standard does not apply. *See, e.g.*, *FTC v. Sterling Precious Metals, LLC*, No. 12-80597, 2013 WL 595713, at *3 (S.D. Fla. Feb. 15, 2013); *FTC v. Consumer Health Benefits Ass'n*, No. 10-3551, 2012 WL 1890242, at *6-7 (E.D.N.Y. May 23, 2012); *FTC v. Innovative Mktg., Inc.*, 654 F. Supp. 2d 378, 388 (D. Md. 2009); *FTC v. Med. Billers Network*, 543 F. Supp. 2d 283, 314-15 (S.D.N.Y. 2008). Others have found that it does apply. *See, e.g.*, *FTC v. Ivy Capital, Inc.*, No. 11-283, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011); *FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 852-54 (C.D. Cal. 2010).

[18] Hotels and Resorts does not dispute the materiality element of this standard. *See also In re Nat'l Credit Mgmt. Grp., L.L.C.*, 21 F. Supp. 2d 424, 441 (D.N.J. 1998) ("Explicit claims or deliberately-made implicit claims utilized to induce the purchase of a service or product are presumed to be material.").

543 F. Supp. 2d at 314 (explaining that Defendants do not "explain why the pleading requirements of Rule 9(b) should apply to this action").[19]

Nevertheless, the Court finds that, even under a Rule 9(b) heightened standard, the allegations here suffice. *See FTC v. Cantkier*, 767 F. Supp. 2d 147, 154-55 (D.D.C. 2011) ("[A] claim for deceptive acts or practices under Section 5 is not a fraud claim. . . . [T]he Court does not need to rule on the applicability of Rule 9(b) to Section 5 actions here because, even assuming *arguendo* that Rule 9(b) applies, the FTC's allegations have been pled with sufficient particularity.").

Here, the FTC alleges that Defendants "disseminated[] or caused to be disseminated" privacy policies or statements, including statements "regarding the privacy and confidentiality of personal information [] disseminated on the Hotels and Resorts' website." (Compl. ¶ 21 (reproducing a portion of the privacy policy statement disseminated on the Hotels and Resorts' website)). The statement from Hotels and Resorts' website represents, in part, that "[w]e safeguard our Customers' personally identifiable information by using industry standard practices" and make "commercially reasonable efforts" to collect personally identifiable information "consistent with all applicable laws and regulations" and, among other things, that "[w]e take commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy." (*Id.*).

The FTC also alleges that Defendants "failed to adequately inventory computers connected to the Hotels and Resorts' network so that Defendants could appropriately manage the

[19] At most, Hotels and Resorts' contention seems to be premised on a nefarious, intent-like element that is purportedly inherent in a deception claim. (*See* 11/7/13 Tr. at 137:20-138:6, 146:22-147:3). But, "[u]nlike the elements of common law fraud, the FTC need not prove scienter, reliance, or injury to establish a § 5 violation." *Freecom Commc'ns*, 401 F.3d at 1203 n.7.

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

cybercriminals accessing "payment-card data collected and controlled by the Wyndham-branded hotels." (HR's Mov. Br. at 24). The Court is not so convinced for the following two reasons.

First, the Court cannot accept Hotels and Resorts' contention, that, *as a matter of law*, it is necessarily a separate entity from Wyndham-branded hotels such "that each maintain their own computer networks and engage in their own data-collection practices." (*Id.* at 24-25). After all, the FTC alleges that "Defendants 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, by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft," including Defendants' failure "to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their local networks to Hotels and Resorts' computer network." (Compl. ¶¶ 24, 24(c)). And, accepting the FTC's factual allegations as true and drawing reasonable inferences in favor of the FTC, the Court finds that these allegations support the FTC's deception claim against Hotels and Resorts.[20]

Second, the Court is not persuaded by Hotels and Resorts' arguments involving disclaimer. (*See* HR's Mov. Br. at 25). Hotels and Resorts contends that the policy defines "we," "us," and "our" in a certain way that excludes Wyndham-branded hotels, applies to "our

[20] Alternatively, the Court finds that the FTC's complaint sufficiently pleads Hotels and Resorts' control over the Wyndham-branded hotels. (*See* Compl. ¶¶ 15, 17-19); *Cf. Chen v. Domino's Pizza, Inc.*, No. 09-107, 2009 WL 3379946, at *4 (D.N.J. Oct. 16, 2009) ("Plaintiffs' complaint does not contain a single factual allegation indicating that Domino's had any authority or control over their employment conditions.").

Tellingly, Hotels and Resorts' responds that "the allegations in the complaint do not establish that [Hotels and Resorts] exercised the kind of 'day-to-day' control that is necessary to assign vicarious liability to a franchisor"—but cites a case resolved at summary judgment. (HR's Reply Br. at 11 (citing *Capriglione v. Radisson Hotels Int'l, Inc.*, No. 10-2845, 2011 WL 4736310, at *3 (D.N.J. Oct. 5, 2011))); *see also Drexel v. Union Prescription Ctrs., Inc.*, 582 F.2d 781, 786, 789-90 (3d Cir. 1978) (finding that, "on the present record genuine issues of material fact exist regarding the nature of the relationship between appellee and its franchisee which preclude the entry of summary judgment" and explaining that "[w]hether the control retained by the franchisor is also sufficient to establish a master-servant relationship depends in each case upon the nature and extent of such control as defined in the franchise agreement or by the actual practice of the parties").

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 that purportedly "*expressly disclaims* making any representations about the security of payment-card data collected by the Wyndham-branded hotels." (*Id.* at 25 (citing Ex. A to Hradil Decl. at 4)).

Hotels and Resorts thus asserts that "any reasonable consumer, after reading the privacy policy 'as a whole, without emphasizing isolated words or phrases apart from their context' . . . would have understood that the policy made statements only about data-security practices at [Hotels and Resorts] and made no representations about data-security practices at the Wyndham-branded hotels." (*Id.* at 25-26 (citation omitted) (quoting *Millennium Telecard*, 2011 WL 2745963, at *5)).

But the policy also recognizes "the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests" and states that it "applies to residents of the United States, *hotels of our Brands located in the United States*, and Loyalty Program activities in the United States only." (Ex. A to Hradil Decl. at 1 (emphasis added)). And it also states that "[w]e take commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards to ensure that to the extent we *control* the Information, the Information is used only as authorized by us and consistent with this Policy." (Ex. A at 1 (emphasis added)).

Thus, it is reasonable to infer the exact opposite of what Hotels and Resorts posits: that a reasonable customer would have understood that the policy makes statements about data-security practices at Hotels and Resorts *and* Wyndham-branded hotels, to the extent that Hotels and Resorts *controls* personally identifiable information. And, for this reason, the Court finds

unpersuasive Hotels and Resorts' argument that the FTC "does nothing to explain how the alleged deficiencies it identifies placed personal information *collected by [Hotels and Resorts]* at risk." (*See* HR's Mov. Br. at 28).

The Court is not persuaded otherwise by Hotels and Resorts' reliance on case law purportedly involving "similar disclaimers to dismiss deception or fraud-based claims." (HR's Reply Br. at 11 (citing *Pathfinder Mgmt., Inc. v. Mayne Pharma PTY*, No. 06-2204, 2008 WL 3192563, at *16 (D.N.J. Aug. 5, 2008); *Eckler v. Wal-Mart Stores, Inc.*, No. 12-727, 2012 WL 5382218, at *7 (S.D. Cal. Nov. 1, 2012))). As such, *Pathfinder Management* involved a disclaimer that "explicitly states that [p]laintiff is aware that no representations are being made to them outside those contained within the Purchase Agreement and specified schedules and instruments." 2008 WL 3192563, at *16. Notwithstanding this disclaimer, the plaintiff sought to bring certain allegations "based upon representations made outside of the Purchase Agreement," which the Court determined could not "be the basis for alleging fraudulent misrepresentation or fraud in the inducement." *Id.*

Here, however, the allegations regarding the privacy policy do not relate to extrinsic evidence, and Hotels and Resorts does not explain how the FTC's allegations are otherwise analogous to those in *Pathfinder Management.* For similar reasons, the Court is not persuaded by *Eckler*. *See* 2012 WL 5382218, at *7 (dismissing claims where extrinsic evidence in the form of studies allegedly supported plaintiff's claims that a dietary supplement's representations were false or misleading).

Again, at this stage, the Court must draw reasonable inferences in favor of the FTC, not Hotels and Resorts—even if the FTC's deception claim warrants Rule 9(b) treatment. *See Flood v. Makowski*, No. 03-1803, 2004 WL 1908221, at *14 (M.D. Pa. Aug. 24, 2004) ("While Rule

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 that the Court cannot resolve at this juncture. *See FTC v. Nat'l Urological Grp., Inc.*, 645 F. Supp. 2d 1167, 1189 (N.D. Ga. 2008) ("The meaning of an advertisement, the claims or net impressions communicated to reasonable consumers, is fundamentally a question of fact."); *see also Am. Home Prods. Corp. v. FTC*, 695 F.2d 681, 687 (3d Cir. 1982) ("The impression created by the advertising, not its literal truth or falsity, is the desideratum.").

For these reasons, the Court cannot dismiss the FTC's deception claim at this juncture.

V. CONCLUSION

As set forth above, the Court hereby DENIES Hotels and Resorts' motion to dismiss. An appropriate Order accompanies this Opinion.

/s/ Esther Salas
Esther Salas, U.S.D.J.