IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LABMD, INC.,	)	
	)	
Plaintiff,	)	
	)	Case 1:14-cv-00810-WSD
v.	)	
	)	
FEDERAL TRADE COMMISSION,	)	
	)	
Defendant	)	
_____	)	

MOTION TO DISMISS

Defendant Federal Trade Commission hereby moves this Court to dismiss the above-captioned case pursuant to Fed. R. Civ. P. 12(b)(1) and (6). The FTC has consolidated its memorandum in support of this motion with its opposition to plaintiff's motion for a preliminary injunction. The FTC is contemporaneously filing the consolidated memorandum.

Dated: April 7, 2014

Respectfully submitted,

Of counsel:
JONATHAN E. NUECHTERLEIN
General Counsel
JOHN F. DALY
Deputy General Counsel for
Litigation

JOEL MARCUS-KURN
Attorney

STUART F. DELERY
Assistant Attorney General

MAAME EWUSI-MENSAH
FRIMPONG
Deputy Assistant Attorney General

MICHAEL S. BLUME
Director

Office of General Counsel
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

CERTIFICATE OF COMPLIANCE

I certify that the documents to which this certificate is attached have been prepared with one of the font and point selections approved by the Court in LR 5.1B for documents prepared by computer – namely Century Schoolbook, 13 pt.

Dated: April 7, 2014

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on April 7, 2014, I caused a true and correct copy of the foregoing via CM/ECF on:

Ronald L. Raider
Burleigh L. Singleton
William D. Meyer
KILPATRICK TOWNSEND & STOCKTON LLP
1100 Peachtree Street, NE, Suite 2800
Atlanta, Georgia 30309

Reed D. Rubinstein
DINSMORE & SHOHL, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004

Michael D. Pepson
CAUSE OF ACTION
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006

Attorneys for plaintiff

Dated: April 7, 2014

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LABMD, INC.,	)	
	)	
Plaintiff,	)	
	)	Case 1:14-cv-00810-WSD
v.	)	
	)	
FEDERAL TRADE COMMISSION,	)	
	)	
Defendant	)	
_____	)	

DEFENDANT FTC'S CONSOLIDATED BRIEF IN SUPPORT OF ITS MOTION TO DISMISS AND IN OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

FEDERAL RULES

FEDERAL REGULATIONS

INTRODUCTION

LabMD asks this Court to block an ongoing adjudicatory proceeding before the Federal Trade Commission. The Federal Trade Commission ("FTC") has charged LabMD with violating the Federal Trade Commission Act ("FTC Act") by failing to protect consumers from disclosure of their sensitive personal information. LabMD may present all of its legal and factual defenses before the agency, and when the proceeding is over it may then seek judicial review of any adverse determination.

Nevertheless, LabMD has spent the past four months shopping for a court that will interrupt the administrative process, disrupt Congress's carefully crafted regime for FTC adjudications, and enjoin the pending proceeding. This Court is LabMD's third stop in its attempt to circumvent the statutory administrative and judicial review process – and the third time is not the charm. LabMD has consumed enough time and judicial resources; this Court should reject out of hand its request for a preliminary injunction, dismiss its case, and allow the orderly completion of the pending administrative process as Congress intended.

Congress set forth a comprehensive regime for the conduct and judicial review of FTC adjudicative proceedings. To date, the agency has neither compelled LabMD to do anything nor ordered it to stop any conduct. Should the Commission do so, LabMD will be entitled to judicial review of that decision. In the meantime, the Supreme Court has warned against "turning [the] prosecutor into defendant before adjudication concludes." *FTC v.*

Standard Oil, 449 U.S. 232, 243 (1980). The law is clear that this Court lacks jurisdiction to derail the legislatively established process. That is the case even though the Commission determined, in denying a motion to dismiss at the administrative level, that it has authority over data security practices.

Because the Court lacks jurisdiction, it need not reach the merits of LabMD's challenges. But they are groundless in any event. The FTC Act grants the Commission broad authority that easily encompasses harm to consumers from the release of their sensitive personal information. The Commission may exercise that authority through individual adjudications; there is no requirement that it promulgate rules prior to enforcement. FTC authority can easily co-exist with medical privacy statutes administered by the Department of Health and Human Services ("HHS"), as HHS has explicitly recognized. Indeed, today, the District Court for the District of New Jersey issued an opinion in *FTC v. Wyndham Worldwide Corp.*, No. 13-1887 Slip Op. (April 7, 2014) (attached as Ex. 8), holding that the FTC Act confers on the FTC authority over data security practices and that other statutes that also address data security do not impliedly preempt the FTC Act.

Given the Court's lack of jurisdiction and the strong likelihood that LabMD's meritless challenge will fail, the Court should deny the motion for a preliminary injunction. As LabMD's delay in filing this case shows, there is no urgency. Nor does any harm result from the administrative proceeding beyond "the expense and annoyance of litigation," which the Supreme Court

held does not constitute irreparable harm but is simply "part of the social burden of living under government." *Standard Oil*, 449 U.S. at 244.

BACKGROUND

I. Legal framework

Section 5 of the FTC Act broadly "empower[s] and direct[s]" the Commission "to prevent persons . . . from using . . . unfair . . . acts or practices in or affecting commerce." 15 U.S.C. § 45(a). As a part of an enforcement action or rulemaking proceeding, the Commission has authority to determine that an act or practice is "unfair" if that act or practice "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

Pursuant to this authority, "[t]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace." *See* FTC Report to Congress, Privacy Online, at 2 (June 1998) (attached as FTC Ex. 1). For well over a decade, the Commission has taken the position that the failure to maintain reasonable and appropriate data security measures constitutes an unfair act or practice in violation of Section 5. *See* Order Denying Respondent LabMD's Motion to Dismiss, FTC Dkt. No. 9357, at 8 (Jan. 16, 2014) (hereinafter "Comm'n MTD Denial") (N.D. Ga. Compl. Ex 2). It has brought "administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and resulted in improper disclosures of personal

information collected from consumers online." *Id.* A similar ongoing administrative adjudicatory proceeding against LabMD is the subject of the suit before this Court.

II. The administrative investigation and complaint

LabMD, a Georgia-based medical testing company, conducted clinical laboratory tests on specimen samples from consumers throughout the United States. *See* Complaint, FTC Dkt. No. 9357 (Aug. 28, 2013) (hereinafter "Admin. Compl.") (N.D. Ga Compl. Ex. 4). In 2009, the FTC learned that sensitive personal information in LabMD's possession had been made available to the public on peer-to-peer file sharing networks. N.D. Ga. Compl. Ex. 8 at 2. The FTC staff undertook an investigation into LabMD's data security practices beginning in early 2010. *See* Compl. ("N.D. Ga. Compl.") ¶ 10 (ECF No. 1). The investigation culminated in a Commission determination that there was "reason to believe" that LabMD may have engaged in unfair acts or practices in violation of Section 5 of the FTC Act by failing to maintain reasonable data security practices. *See* Admin. Compl., Preamble (quoting 15 U.S.C. § 45(b)). The Commission determined further that an administrative adjudication of these allegations would be in the public interest. *Id.*

Accordingly, on August 28, 2013, the Commission issued the administrative complaint against LabMD. The complaint alleges that LabMD has accumulated and maintained personal information (such as date of birth, social security numbers, medical information, and bank account or

credit card information) on nearly one million consumers. Admin. Compl. ¶¶ 6-7. In spite of the sensitivity and volume of consumer data that it stores, the company allegedly did not implement or maintain a comprehensive data security program to protect that data; did not use readily available technology to identify commonly known or reasonably foreseeable security risks and vulnerabilities to the security of this data; did not use appropriate measures to prevent employees from accessing consumers' personal information not needed to perform their jobs; did not adequately train employees on basic security practices; and did not use readily available measures to prevent and detect unauthorized access to consumers' personal information. *Id.* ¶ 10. The administrative complaint alleges that, taken together, these practices constitute a failure to provide reasonable and appropriate security for personal information on LabMD's computer networks. *Id.* It further alleges that while LabMD could have corrected its problematic practices "at relatively low cost using readily available security measures," consumers harmed by LabMD's security failures could not have taken steps to protect themselves from such harm because "consumers have no way of independently knowing about" them. *Id.* ¶¶ 11-12.

The administrative complaint discusses one example of LabMD's data security failures: the company allegedly failed to detect that its billing manager had installed Limewire, a peer-to-peer file sharing application, on a LabMD computer. *Id.* ¶¶ 10(g), 18(a). Peer-to-peer software is commonly used to share music, videos, and other materials with other users of

compatible software. The software allows users to choose files to make available to others, but also creates a significant security risk that files with sensitive data will also be shared inadvertently. Once a file has been made available on a peer-to-peer network and downloaded by another user, it can be shared by that user across the network even if the original source of the file is no longer connected. *See* Admin. Compl. ¶¶ 13-16. A third party informed LabMD that a LabMD file containing sensitive information about thousands of consumers was available on a P2P network through Limewire. *Id.* ¶ 17; *see also* Compl. ¶ 3, *LabMD v. FTC,* No. 1:13-cv-1787 (Nov. 14, 2013 D.D.C.) ("D.C. Compl.") (FTC Ex. 2).[1] Hundreds of other files from the billing manager's computer allegedly were also designated for sharing on Limewire. Admin. Compl. ¶ 18.

The administrative complaint recounts an additional security incident, which illustrates the potential for consumer injury resulting from the unauthorized disclosure of consumers' information collected by LabMD. Sacramento police found different LabMD documents containing personal information from hundreds of consumers in the possession of identity thieves. *Id.* ¶ 21. LabMD's alleged failure to maintain reasonable security measures elevates the risk of consumer harm. *See id.* ¶ 10.

[1] That file contained personal information on approximately 9,300 consumers, including their names, dates of birth, social security numbers, information about laboratory tests run, and, in many instances, their health insurance company names, addresses, and policy numbers. Admin. Compl. ¶ 19.

The administrative process is underway. Once the Commission voted out the complaint, it was referred to an administrative law judge ("ALJ"). No remedy may be imposed until the conclusion of the administrative adjudicatory proceeding before the ALJ, *see* 15 U.S.C. § 45(b) (authorizing and governing FTC adjudicatory proceedings); 16 C.F.R. Pt. 3 (rules of practice and procedure governing such cases).

Shortly after the adjudicatory proceeding began, LabMD moved to dismiss the complaint before the Commission. The Commission denied the motion, holding that the complaint concerned matters within the FTC's authority and the agency had not violated LabMD's right to due process. *See* Comm'n MTD Denial at 18-19. The Commission explained further that its "ultimate decision on LabMD's liability will depend on the factual evidence to be adduced in this administrative proceeding." *Id.* at 18. For example, the Commission would need to determine not only "whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures were 'unreasonable' in light of the circumstances." *Id.*

Accordingly, the matter is now before the ALJ, the parties have been conducting discovery, and the evidentiary hearing is set to begin on May 20, 2014. *See* Comm'n MTD Denial at 2. At the hearing, LabMD and the Commission's enforcement staff ("complaint counsel")[2] will present evidence

[2] To ensure separation of the Commission's prosecutorial and adjudicatory roles, complaint counsel remains "walled off" from the Commission for the duration of the proceeding, as required by the Administrative Procedure Act ("APA"). *See* 5 U.S.C. § 554(d); 16 C.F.R. § 4.7(b).

and legal argument to the ALJ. *See* 16 C.F.R. §§ 3.41-3.42. *Cf.* 5 U.S.C. §§ 554(d), 556. LabMD will have the opportunity to refute complaint counsel's evidence and argument, and to present evidence and argument of its own. The ALJ will then issue an "initial decision" containing findings of fact and conclusions of law. 16 C.F.R. § 3.51; *cf.* 5 U.S.C. § 557.

Either LabMD or complaint counsel may appeal the ALJ's initial decision to the full Commission, which would conduct a *de novo* review of both the factual findings and legal conclusions in the ALJ's initial decision. 16 C.F.R. §§ 3.52-3.54; 5 U.S.C. § 557(b). If, after reviewing the record, the Commission determines that LabMD has engaged in "unfair acts or practices" and enters a final order to cease and desist, then LabMD "may obtain a review of such order in the court of appeals," 15 U.S.C. § 45(c), which has "exclusive" jurisdiction "to affirm, enforce, modify, or set aside" the Commission's order, *id* § 45(d).

III. LabMD's multiple federal court challenges to the ongoing administrative proceedings

LabMD has sought to disrupt the enforcement proceeding against it in three different forums. A week after filing its motion to dismiss before the FTC, LabMD filed a complaint against the FTC in the U.S. District Court for the District of Columbia. Four days later, it filed a petition for review in the Eleventh Circuit. While the district court case was pending, the Eleventh Circuit dismissed its case for lack of jurisdiction. N.D. Ga. Compl. Ex. 1. If any court had jurisdiction, the Eleventh Circuit suggested, it would be a

district court, although the court did not "express or imply any opinion about whether a district court has jurisdiction to hear such claims or about the merits of those claims." *Id.* at 2. Yet even though LabMD had a district court case pending in D.C., it dismissed that case. *See* Notice of Voluntary Dismissal, *LabMD v. FTC,* No. 1:13-cv-1787 (Feb. 19, 2014 D.D.C.) (FTC Ex. 3). More than a month later, it filed the instant case – and a motion for emergency relief that it had not asked for in D.C.[3] In each proceeding, the essence of LabMD's claims has remained the same.

ARGUMENT

I. The complaint must be dismissed for lack of jurisdiction

"The burden for establishing federal subject matter jurisdiction rests with the party bringing the claim." *Sweet Pea Marine, Ltd. v. APJ Marine, Inc.*, 411 F.3d 1242, 1247 (11th Cir. 2005). Pursuant to Fed. R. Civ. P. 12(b)(1), the district court is not limited to considering the complaint alone, but may also consider facts in the record. *McElmurray v. Consol. Gov't*

[3] This Court previously heard a related case in 2012, before the administrative complaint was issued. There, the FTC served several civil investigative demands on Michael Daugherty and LabMD. When they refused to comply, the Commission sought an order from this Court to enforce the civil investigative demands. *See* N.D. Ga. Compl. Ex. 8. In response, they argued that the FTC lacked the authority to investigate and bring enforcement actions with respect to data security issues, and that the FTC had been divested of jurisdiction to regulate data security by laws governing health information. Opp'n Brief, *FTC v. LabMD*, No. 1:12-cv-03005-WSD, at 17 (N.D. Ga. Sept. 14, 2012) (FTC Ex. 4). The Court rejected these arguments, explaining that the FTC had made "a plausible argument in support of its assertion of jurisdiction" over data security issues. N.D. Ga. Compl. Ex. 8.

Augusta–Richmond Cnty, 501 F.3d 1244, 1251 (11th Cir. 2007). Absent subject matter jurisdiction, a court may not order injunctive or declaratory relief. 28 U.S.C. § 2201 ("In a case of *actual controversy* within its jurisdiction . . . any court . . . may declare the rights. . . ." (emphasis added)); *Public Serv. Comm'n of Utah v. Wycoff Co.*, 344 U.S. 237, 242 (1952). LabMD cannot show that this – or any other – federal court has jurisdiction to entertain any of LabMD's claims at this time.

A. This Court lacks jurisdiction to consider any of LabMD's claims because doing so would interfere with the ongoing FTC proceeding

Two separate lines of Supreme Court precedent make clear that plaintiff cannot invoke the jurisdiction of this Court to interfere with the ongoing FTC proceeding against it. In *Thunder Basin Coal Co. v. Reich*, 510 U.S. 200, 207-08 (1994), the Supreme Court explained that federal courts lack jurisdiction to consider any *claims* related to an ongoing administrative adjudication when – as is the case here – Congress intended to foreclose interlocutory review. And in the *Ewing v. Mytinger & Casselberry, Inc.*, 339 U.S. 594, 598 (1950) line of cases, the Supreme Court made clear that the type of *relief* plaintiff seeks – enjoining ongoing administrative proceedings – is not available from any federal court.

1. This Court lacks jurisdiction over pre-enforcement challenges to an administrative adjudication

Congress crafted a detailed regime for administrative adjudication of complaints and provided an exclusive means for challenging a final order resulting from an FTC administrative proceeding. The FTC Act specifies that, upon finding "reason to believe" that any person has engaged in "unfair or deceptive act or practice in or affecting commerce," the Commission may undertake an adjudication to determine if such acts were committed. 15 U.S.C. § 45(b). Congress laid out in some detail how that process should proceed, including judicial review. *Id.* Importantly, Congress vested the court of appeals with exclusive jurisdiction to review any final agency cease-and-desist order. *Id.* § 45(c).

LabMD does not challenge a final Commission cease-and-desist order; no such order has been issued. *See* N.D. Ga. Compl. ¶¶ 97, 106. Rather, it challenges a pending administrative complaint and an interlocutory agency order denying a motion to dismiss that complaint. LabMD may raise before the FTC all the claims it raises here. Although the Commission has rejected some of those defenses and arguments, neither the administrative law judge overseeing the proceeding nor the Commission has determined LabMD's liability under the FTC Act. *See* Comm'n MTD Denial.

Where Congress has provided "a detailed structure for reviewing violations" of a statute and granted to the court of appeals exclusive jurisdiction to review administrative decisions resulting from that process,

those legislative requirements "demonstrate[] that Congress intended to preclude challenges" prior to the completion of agency proceedings. *Thunder Basin*, 510 U.S. at 207-208. Thus, a district court is "preclude[d] [from] . . . exercising jurisdiction over [a] pre-enforcement challenge" to agency proceedings. *Id.* at 216. The FTC Act is the same type of statutory regime as that in *Thunder Basin*. The Supreme Court explained that judicial intervention prior to the conclusion of the administrative process was precluded because such premature judicial review would be tantamount to "evad[ing] the statutory-review process." *Id.*[4]

Here, the detailed procedures specified in the FTC Act, *see* 15 U.S.C. § 45(c), (g)-(i), provide a full opportunity for LabMD to obtain judicial review. Where, as here, "Congress has provided an adequate procedure for judicial review of administrative action, that procedure must be followed." *Frito-Lay, Inc. v. FTC*, 380 F.2d 8, 10 (5th Cir. 1967) (per curiam). LabMD is flatly wrong when it contends that under the FTC Act a "district court has jurisdiction until [a final order] has been issued." *See* Pl.'s PI Mem. at 12 (ECF No. 2). The FTC Act provides that *the FTC* and the court of appeals have concurrent jurisdiction until the administrative record is filed with the court. 15 U.S.C. § 45(c), (d). Those provisions say nothing about district court jurisdiction, which would be wholly inconsistent with Congress's grant

[4] The statutory review process laid out in the FTC Act precludes the exercise of jurisdiction over not only an APA claim, but also a constitutional challenge brought in district court pursuant to 28 U.S.C. § 1331. *See Elgin v. Dept. of Treasury*, 132 S. Ct. 2126, 2132-33 (2012).

of "exclusive" jurisdiction to the court of appeals. Congress's chosen regime for review of FTC proceedings makes clear that, until the FTC issues a final order, LabMD must raise its arguments before the agency and may not seek a judicial injunction to sidestep the legislatively mandated administrative process. LabMD will have a full opportunity for review of any adverse result, including review of the Commission's jurisdiction over data security practices. *See* 15 U.S.C. § 45(c)-(d). The Eleventh Circuit's order dismissing LabMD's earlier challenges in that court does not suggest otherwise. Indeed, the court of appeals pointedly did not "express or imply any opinion about whether a district court has jurisdiction to hear such claims or about the merits of those claims." N.D. Ga. Compl. Ex. 1.

The prohibition on invoking the judicial process to nullify the administrative process remains in effect when the FTC has denied a motion to dismiss the administrative complaint. So long as LabMD is entitled to full judicial review at the conclusion of the proceeding – which under the FTC Act it is – it may not "turn[] [the] prosecutor into defendant before adjudication concludes." *Standard Oil*, 449 U.S. at 243.

2. This Court cannot enjoin the ongoing administrative proceedings

LabMD's complaint also must be dismissed in its entirety because district courts lack jurisdiction to enjoin ongoing administrative enforcement

proceedings.[5] The Supreme Court established long ago that having a court separate from the enforcement action enjoin ongoing administrative proceedings would result in unnecessary and premature judicial interference. *See Ewing*, 339 U.S. at 598; *Myers v. Bethlehem Shipbuilding Corp.*, 303 U.S. 41, 48 (1938) ("The District Court is without jurisdiction to enjoin [NLRB's administrative] hearings[.]"). The Court explained that "it has never been held that the hand of government must be stayed until the courts have an opportunity to determine whether the government is justified in instituting suit." *Ewing*, 339 U.S. at 599. Since that time, that principle has been "consistently and strictly observed" by courts throughout the country. *United States v. Alcon Labs.*, 636 F.2d 876, 881-82 (1st Cir. 1981) (the issuance of preemptive injunctive relief "might seriously impair the effectiveness of the Act's enforcement provisions"); *see, e.g.*, *Parke, Davis & Co. v. Califano*, 564 F.2d 1200, 1206 (6th Cir. 1977) ("[I]t was an abuse of discretion to enjoin the [agency] . . . where pending enforcement actions provided an opportunity for a full hearing before a court."). *Cf. N.C. Bd. Dental Examiners v. FTC*, 768 F. Supp. 2d 818, 822 (E.D.N.C. 2011) ("Where the instant lawsuit seeks a

[5] LabMD's request that the Court block FTC enforcement actions against third parties, N.D. Ga. Comp. ¶ 135, runs afoul of "the general prohibition on a litigant's raising another person's legal rights." *United Food & Commercial Workers Union Local 751 v. Brown Grp., Inc.*, 517 U.S. 544, 557 (1996) (quotation omitted). LabMD alleges no "close relation" between it and any third party or any "hindrance to the third party's ability to protect his or her own interests" that would warrant third party standing. *Powers v. Ohio*, 499 U.S. 400, 411 (1991). Accordingly, the request for this type of relief must be dismissed for lack of jurisdiction.

declaration that defendant's litigating position in the administrative proceedings is contrary to law . . . its unmistakable purpose and effect is to short-circuit [*Ewing*]."); *accord S.C. Bd. of Dentistry v. FTC*, 455 F.3d 436 (4th Cir. 2006).

Indeed, courts have found *Ewing* to bar federal courts from exercising jurisdiction over actions to enjoin FTC adjudicative proceedings, even in the face of constitutional and jurisdictional challenges like those plaintiff raises here. *See, e.g.*, *N.C. Bd. Dental Examiners*, 768 F. Supp. 2d 818 (dismissing plaintiff's claims for declaratory and injunctive relief arising from ongoing administrative proceeding initiated by the FTC, despite allegations that the FTC's proceedings exceeded the agency's jurisdiction); *Direct Mktg. Concepts, Inc. v. FTC*, 581 F. Supp. 2d 115, 117 (D. Mass. 2008) ("Any challenges to the propriety of the agency action [including a First Amendment claim] should be addressed in the enforcement action itself."); *POM Wonderful v. FTC*, 894 F. Supp. 2d 40, 44 (D.D.C. 2012) ("[The FTC] is 'perfectly capable' of determining whether [administrative action] exceeds the bounds of the FTC Act [or] violates the First and Fifth Amendments."). Because this Court does not have the power to issue the relief LabMD seeks, the complaint must be dismissed in its entirety.

B. LabMD's claims are all patently unripe

Any unripe claims must be dismissed pursuant to Rule 12(b)(1). *See Digital Properties, Inc. v. City of Plantation*, 121 F.3d 586, 589 (11th Cir. 1997). "A claim is not ripe for adjudication if it rests upon contingent future

events that may not occur as anticipated, or indeed may not occur at all." *Texas v. United States*, 523 U.S. 296, 300 (1998) (quotation omitted).

LabMD's claims are unripe because they depend on the occurrence of far-from-certain contingencies. At this point, it is impossible to know how the FTC will resolve this matter. Depending on the record developed at trial, the administrative proceedings may resolve in LabMD's favor. Before making a final determination, the FTC will "need to determine . . . not only whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures were 'unreasonable' in light of the circumstances. Whether LabMD's security practices were unreasonable is a factual question that can be addressed only on the basis of evidence to be adduced in [the administrative adjudicatory] proceeding." Comm'n MTD Denial at 18-19.

This is *exactly* the kind of case where the ripeness doctrine should "prevent the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements over administrative policies, and also . . . protect the agencies from judicial interference until an administrative decision has been formalized and its effects felt in a concrete way by the challenging parties." *Ohio Forestry Ass'n v. Sierra Club*, 523 U.S. 726, 732-33 (1998) (citation omitted). Indeed, in *Texas v. United States*, the Supreme Court upheld the dismissal of an analogous case on ripeness grounds. There, plaintiff sought a declaratory judgment that would have blocked a proceeding pending before the Department of Justice to determine whether Texas had violated the Voting Rights Act. 523 U.S. at 300. Just as

LabMD claims here, Texas claimed that the statute did not apply to its conduct. The Court held the case was not ripe because:

> The operation of the statute is better grasped when viewed in light of a particular application. Here, as is often true, "[d]etermination of the scope . . . of legislation in advance of its immediate adverse effect in the context of a concrete case involves too remote and abstract an inquiry for the proper exercise of the judicial function."

Id. at 301 (quoting *Longshoremen v. Boyd*, 347 U.S. 222, 224 (1954)).

LabMD suggests that this case is ripe because the FTC has somehow "predetermined" its outcome. N.D. Ga. Compl. ¶¶ 106, 142. However, plaintiff does not allege that the administrative proceedings have resolved all contested issues of fact, let alone whether LabMD violated the FTC Act at all. *See id.* Nor is LabMD correct that the Commission votes in favor of complaint counsel in every instance. *See* N.D. Ga. Compl. ¶ 94. For example, earlier this year, the Commission issued an opinion in an adjudicatory case, reversing the ALJ's rulings holding the respondent liable on certain counts in the complaint, and instead concluded that Complaint Counsel had failed to establish that the respondent's conduct was unlawful. *See In re McWane, Inc., and Star Pipe Products, Ltd.*, FTC Docket No. 9351, Opinion of the Commission (January 30, 2014) (FTC Ex. 5).[6]

[6] LabMD's further suggestion that Commissioner Brill's involvement in the case means the case has been "predetermined" is also entirely without merit. *See* N.D. Ga. Compl. ¶¶ 29-32. Commissioner Brill has recused herself from ongoing proceedings in the underlying administrative matter. *See* Statement of Comm'r Brill, FTC Dkt. No. 9357 (Dec. 24, 2013) (FTC Ex. 6).

C. The Court lacks jurisdiction over plaintiff's APA claim, which does not challenge final agency action

LabMD's first claim for relief seeks redress for alleged APA violations. In addition to the reasons discussed above why the entire complaint must be dismissed for lack of jurisdiction, LabMD's first claim suffers from another fatal flaw: it fails to challenge final agency action because none has occurred.

The APA permits judicial review of "[a]gency action made reviewable by statute and *final agency action* for which there is no other adequate remedy in a court." 5 U.S.C. § 704 (emphasis added). It is well-established that, except as otherwise provided by statute,[7] "[i]f the agency action is not final, the court" lacks "federal subject matter jurisdiction." *Nat'l Parks Conservation Ass'n v. Norton*, 324 F.3d 1229, 1236, 1240 (11th Cir. 2003). None of the actions plaintiff challenges under the APA – the filing of the administrative complaint, the inclusion of a proposed remedy, or the denial of LabMD's motions to dismiss and for a stay, *see* N.D. Ga. Compl. ¶¶ 104-106 – constitutes final agency action.

The Supreme Court has held squarely that the FTC's issuance of an administrative complaint is not final agency action subject to judicial review. *Standard Oil*, 449 U.S. 232. To the contrary, an FTC complaint "represents a threshold determination that further inquiry is warranted and that a

[7] LabMD does not claim it is seeking judicial review of an action "made reviewable by statute" – nor could it because, as discussed *supra* Part I.A.1, the FTC Act grants a right of review only for final FTC cease and desist orders and even then vests exclusive review in the court of appeals.

complaint should initiate proceedings." *Id*. at 241. The Court made clear that a complaint is not a final action even though it is "definitive" on the question regarding whether the Commission had "reason to believe" that the respondent violated the FTC Act. *Id*. The Court warned in particular against judicial "interference with the proper functioning of the agency," which "denies the agency an opportunity to . . . apply its expertise." *Id*. at 242. Because an administrative complaint is not final agency action, a remedy proposed in such a complaint *a fortiori* cannot be final agency action.

Under *Standard Oil*, the FTC's denial of a motion to dismiss also is not final agency action, even when the Commission's denial rejects an argument that the Commission has exceeded its statutory authority. *Standard Oil*, 449 U.S. at 243. As here, Standard Oil had filed a motion to dismiss an FTC administrative adjudication, *id*. at 235 n.5, and a motion for reconsideration, *id*. at 241 n.9. The Commission had denied both of Standard Oil's motions. Even though Standard Oil had no further administrative opportunity to challenge issuance of the complaint, the Supreme Court concluded that judicial review was premature. As the Court explained, to hold otherwise would "mistake[] exhaustion for finality." In filing an administrative motion to dismiss:

> [Plaintiff] may well have exhausted its administrative remedy as to the averment [that the Commission has] reason to believe [an FTC act violation occurred]. But the Commission's refusal to reconsider its issuance of the complaint does not render the complaint a "definitive" action. The Commission's refusal does not augment the complaint's legal force or practical effect upon

> [plaintiff]. Nor does the refusal diminish the concerns for efficiency and enforcement of the Act.

Id.; *see also Reliable Automatic Sprinkler Co., Inc. v. Consumer Prod. Safety Comm'n*, 324 F.3d 726, 733 (D.C. Cir. 2003) ("The policy undergirding the finality requirement is no less applicable to piecemeal appeals on issues of statutory authority than to piecemeal appeals on other points." (quotation omitted)). That rationale applies equally to the Commission's denial of LabMD's motion for a stay.

The Supreme Court recognized in *Standard Oil* that requiring regulated parties to complete the administrative process would impose a burden on them. "[T]he expense and annoyance of litigation is 'part of the social burden of living under government.'" 449 U.S. at 244 (quoting *Petroleum Exploration, Inc. v. Public Service Comm'n*, 304 U.S. 209, 222 (1938)). But "mere litigation expense, even substantial and unrecoupable cost, does not constitute irreparable injury." *Id.*

Despite plaintiff's suggestion, neither the Supreme Court nor the Eleventh Circuit has retreated from *Standard Oil*'s unambiguous holding that the FTC's filing of an administrative complaint or denial of a motion to dismiss does not constitute final agency action. *See* N.D. Ga. Compl. ¶106. The cases relied on by LabMD show no such thing. In *TVA v. Whitman*, 336 F.3d 1236, 1239 (11th Cir. 2003), the Eleventh Circuit found that "legally inconsequential" agency decisions are not final agency action subject to review – which in no way abrogates *Standard Oil*. In *Sackett v. EPA*, the Supreme Court found final agency action where the EPA's order imposed on

the Sacketts the *immediate* "legal obligation to 'restore' their property according to an agency-approved Restoration Work Plan, and [to] give the EPA access to their property." 132 S. Ct. 1367, 1371 (2012). By contrast, the Commission's denial of LabMD's motion to dismiss does not require the company to do *anything*, aside from continue with the administrative process.

Nor do the other, non-binding cases that plaintiff cites call the *Standard Oil* rule into question. *See* N.D. Ga. Compl. ¶106. In *CSI Aviation Servs. v. US Dep't of Transportation*, 637 F.3d 408 (D.C. Cir. 2011), the agency had issued a cease-and-desist letter that effectively required immediate compliance and was not "subject to further agency consideration or possible modification." *Id*. at 412. Moreover, there were no "disputed facts that would bear on" whether the company had violated the law. *Id*. No such factors are present here. *Athlone Indus. Inc. v. Consumer Prod. Safety Comm'n*, 707 F.2d 1485 (D.C. Cir. 1983), addressed exhaustion, not finality – the very distinction recognized in *Standard Oil* as dispositive. *See Ukiah Valley Med. Ctr v. FTC*, 911 F.2d 261, 266 (9th Cir. 1990) (explaining that *Athlone* dealt with exhaustion and not finality). *Trudeau v. FTC*, 456 F.3d 178 (D.C. Cir. 2006), is inapposite because it involved review of an FTC press release that, unlike an administrative complaint, was not reviewable under the ordinary FTC judicial review provisions.

The FTC has argued in other litigation that deference under *Chevron v. NRDC*, 467 U.S. 837 (1984), applies to its construction of Section 5 of the FTC Act in the order denying LabMD's motion to dismiss. *See* N.D. Ga. Compl.

Ex. 6. Contrary to LabMD's contention, that position does not render the LabMD proceeding final. The Commission's ruling represents a definitive interpretation of the application of Section 5 to data security, but as the Supreme Court held in *Standard Oil*, that does not make the proceeding final under the APA.

Even if *Standard Oil* did not definitively resolve the matter, the Court should also consider whether the action affects the legal rights and obligations of the parties; whether the action will have an immediate impact on the daily operations of the regulated party; whether pure questions of law are involved; and whether pre-enforcement review will be efficient. *See TVA*, 336 F.3d at 1248. None of those factors are pertinent here. The FTC's denial of LabMD's motion to dismiss does not affect LabMD's legal rights and obligations and will not have an impact on LabMD's daily operation because it does not resolve whether LabMD's data security practices are unreasonable or require any action or inaction on LabMD's part. Comm'n MTD Denial at 18-19. Nor does this matter involve "pure questions of law." Substantial facts must be resolved before the ALJ and the FTC can assess whether LabMD has violated Section 5. For the same reason, judicial review at this point would be inefficient because it would prevent the FTC from even examining LabMD's conduct. *See Ohio Forestry*, 523 U.S. at 732-33.

II. In the alternative, the complaint should be dismissed for failure to state a claim

Because the Court lacks jurisdiction over the complaint for the foregoing reasons, it need not proceed further. Should it determine that it has jurisdiction, however, the Court should dismiss the complaint because it "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "[A] complaint [does not] suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)). Instead, a valid complaint contains sufficient factual allegations that, if accepted as true, "state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. A claim is plausible on its face only if "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 Court is "not bound to accept as true a legal conclusion couched as a factual allegation," *Papasan v. Allain*, 478 U.S. 265, 286 (1986), or to "accept inferences drawn by plaintiffs if such inferences are unsupported by the facts set out in the complaint," *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1320 (11th Cir. 2006) (citation omitted). In evaluating a Rule 12(b)(6) motion, the Court may consider facts contained in any attachments to, or documents incorporated into, the complaint. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). Even if the Court otherwise

had jurisdiction in this case – which it does not – none of plaintiff's claims for relief survive the 12(b)(6) standard.

A. Plaintiff fails to state a valid claim that the FTC lacks power to regulate data security

LabMD claims that the FTC lacks authority to regulate data security because Section 5 of the FTC Act says nothing about data security. *See* N.D. Ga. Compl. ¶¶ 104, 118. Plaintiff also claims that Congress divested any possible FTC authority over data security in the health field when it passed the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which HHS administers. *Id* ¶¶ 104, 118.[8] Neither of these arguments states a valid claim.

There is no validity to plaintiff's argument that HIPAA and HITECH divest the FTC of otherwise applicable Section 5 authority. To be sure, HIPAA and HITECH address the security of health data. But "[w]hen [multiple] statutes are capable of coexistence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective." *J.E.M. Ag. Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc.*, 534 U.S. 124, 143-44 (2001); *see also* Comm'n MTD Denial at 10-13. The FTC

[8] LabMD further claims that "[n]either the HHS nor the FTC has accused LabMD of violating HIPAA or HITECH." N.D. Ga. Compl. ¶ 17. The FTC, which does not enforce either of those statutes, has never expressed any view on whether LabMD has, or has not, violated those statutes – or whether it is subject to regulation under any statute beyond the FTC Act.

Act, HIPAA, and HITECH clearly are consistent with one another, and Congress wanted sensitive personal health information to be protected under both regimes. *See* Comm'n MTD Denial at 11-14.[9] LabMD contends in effect that HIPAA and HITECH impliedly repealed the FTC's Section 5 authority, but "[a]n implied repeal will only be found where provisions in two statutes are in 'irreconcilable conflict,' or where the [later] Act covers the whole subject of the earlier one and 'is clearly intended as a substitute.'" *Id.* at 11 (citing *Branch v. Smith*, 538 U.S. 254, 273 (2003)).

That is clearly not the case here. Neither HIPAA nor HITECH forecloses the possibility that another agency plays a parallel role in protecting patient data security. Indeed, in adopting regulations implementing HIPAA, HHS stated that "[s]ecurity standards in this final rule establish a *minimum* level of security that covered entities must meet. We note that covered entities may be required by other Federal law to adhere to *additional*[] or more stringent security measures." 68 Fed. Reg. at 8355 (emphasis added).[10] Accordingly, HIPAA and HITECH authority are capable of co-existing with the FTC's authority to police unfair consumer practices in the area of patient-information data-security.

---

[9] Of note, FTC and HHS have worked in tandem in previous enforcement cases, with each agency seeking complementary penalties. *See* Comm'n MTD Denial at 11.

[10] Moreover, HHS regulations provide that state laws "related to the privacy of individually identifiable health information [that are] more stringent than" HHS's requirements are not preempted. 45 C.F.R. § 160.203(b).

In the absence of any reason to believe that HIPAA and HITECH affirmatively displace FTC authority, the Commission's interpretation of Section 5 is entitled to *Chevron* deference. *City of Arlington v. FCC*, 133 S. Ct. 1863, 1868-69 (2013) (whether an agency is acting beyond the scope of its authority is a question of the agency's interpretation of its organic act). The Court explained that the agency's interpretation of its statutory jurisdiction is no different from its interpretation of any other provision of the statute it administers; rather, because the agency's "power to act and how they are to act is authoritatively prescribed by Congress," there is "no principled basis for carving out some arbitrary subset of such claims as 'jurisdictional.'" *Id.* at 1869. Here, the FTC has reasonably interpreted the FTC Act and determined that its broad grant of authority covers potentially harmful data security practices.

It is of no moment that the FTC Act does not address data security. Section 5 of the Act broadly empowers the FTC to take action against *any* "unfair . . . acts or practices in or affecting commerce," as long as the act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(a), (n). Congress crafted this standard broadly to afford the Commission substantial discretion in its application. It therefore does not "delineate all of the specific 'kinds' of practices which will be deemed unfair," but allows the FTC "to define unfair practices on a flexible, incremental basis." *Am. Fin. Servs.*

Ass'n v. FTC, 767 F.2d 957, 967 (D.C. Cir. 1985); *see also Atl. Refining Co. v. FTC*, 381 U.S. 357, 367 (1965) ("[Congress] intentionally left development of the term 'unfair' to the Commission rather than attempting to define 'the many and variable unfair practices which prevail in commerce.'") (quoting S. Rep. No. 592, 63d Cong., 2d Sess., 13 (1914)). Indeed, the Supreme Court has long held that "[n]either the language nor the history of the [FTC] [A]ct suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories." *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 310 (1934). The Commission had ample room to interpret the Act's expansive language as granting authority over data security practices. Comm'n MTD Denial at 3-5; *see also Wyndham,* Slip Op. 10-15.

Thus, federal courts have upheld Commission determinations finding a wide range of acts or practices that satisfy the applicable criteria to be "unfair" within the meaning of Section 5, even though these practices are not explicitly mentioned in Section 5. *See, e.g.*, *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010) (creating unverified checks that enabled fraudsters to take unauthorized withdrawals from consumers' bank accounts); *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1193 (10th Cir. 2009) (covert retrieval and sale of consumers' telephone billing information); *Orkin Exterminating Co. v. FTC,* 849 F.2d 1354, 1364 (11th Cir. 1988) (unilateral breach of standardized service contracts). Accepting plaintiff's contrary approach would significantly hobble the FTC's ability to keep pace with ever-changing methods of consumer harm. But Congress plainly intended the Commission to have the

authority "to determine what practices were unfair" rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (quoting S. Rep. No. 597, 63d Cong., 2d Sess., 13 (1914), and H.R. Conf. Rep. No.1142, 63d Cong., 2d Sess., 19 (1914)). Congress knew that there "is no limit to human inventiveness" in commerce. *Id*. Thus, "[e]ven if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *Id*.

This Court has already found that the Commission's interpretation of Section 5 passes deferential scrutiny, holding that the FTC had made such a showing with respect to its investigation of LabMD:

> The FTC presents a plausible argument for the exercise of its jurisdiction to investigate and enforce in the realm of data security and consumer privacy – which it has done so in at least forty-four instances since 2000 – in light of the threat of substantial consumer harm that occurs when consumers are victims of identity theft – a routine occurrence in the United States.

N.D. Ga. Compl. Ex. 2 at 13. Here too, LabMD has not met its burden to show that the FTC has improperly exercised its statutory authority.

B. Plaintiff's other *ultra vires* claims also fail under 12(b)(6)

The remainder of plaintiff's claims that the FTC has exceeded its authority also fail. *See* N.D. Ga. Compl. ¶¶ 117-119. The first statute that plaintiff contends the FTC has violated, 15 U.S.C. § 45(m)(1)(B), is not at issue here. That provision addresses when "the Commission may commence a civil action to obtain a civil penalty in a district court of the United States."

But the Commission has not sued LabMD in federal court nor is it currently seeking a civil penalty from LabMD. The FTC is also not in violation of 5 U.S.C. § 552(a)(1), which *inter alia* requires agencies to publish the results of formal notice-and-comment rulemaking in the Federal Register. As plaintiff itself vigorously argues, the FTC has not adopted any rule subject to that provision, which makes § 552(a)(1) entirely irrelevant here.

The FTC has also not violated the specific limits 15 U.S.C. § 45(n) places on the agency's Section 5 unfairness authority. Under that provision, an act or practice must "cause[] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition" to be considered unfair. "In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination." *Id.* Poor data security practices surely can harm consumers, including increased vulnerability to identity theft. *See* Admin. Compl. ¶ 12. The administrative complaint alleges that LabMD could have corrected its problematic practices "at relatively low cost using readily available security measures," and that consumers could not take steps to protect themselves against harm from LabMD's security failures because "consumers have no way of independently knowing about" them. Admin. Compl. ¶¶ 11-12. If proven true by the evidence introduced at the administrative hearing, these allegations would

establish that the injury was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits. Plaintiff's claim that the FTC is using public policy as its prime motivation in bringing an enforcement action against LabMD is a "naked assertion devoid of further factual enhancement" that must be dismissed. *Iqbal*, 556 U.S. at 678.

C. Plaintiff fails to make a valid "fair notice due process" claim

1. Plaintiff's claim does not implicate a liberty or property interest

As a threshold matter, a plaintiff attempting to assert a due process claim must demonstrate that a liberty or property interest is implicated. *Bd. of Regents of State Colleges v. Roth*, 408 U.S. 564, 569 (1972). "The mere possibility of remote or speculative future injury or invasion of rights will not suffice" to meet this requirement. *Reichenberger v. Pritchard*, 660 F.2d 280, 282 (7th Cir. 1981); *see Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1147 (2013) ("threatened injury must be *certainly impending* to constitute injury in fact, and that allegations of *possible* future injury are not sufficient.").

In its third claim for relief, plaintiff alleges that its property rights are implicated because a draft order, which the Commission has not in fact entered against LabMD, *could* lead to monetary damages *if* complaint counsel prevails in front of the ALJ, the Commission upholds the determination, and LabMD takes future actions in violation of that (currently

non-existent) order. *See* N.D. Ga. Compl. ¶¶ 156-58. This chain of events is far too attenuated to implicate a cognizable liberty or property interest.

2. Due process does not require the FTC to issue data security regulations before bringing an enforcement action against LabMD

Plaintiff incorrectly contends that due process requires the FTC to issue data security regulations before bringing an enforcement action against LabMD. *See* N.D. Ga. Compl. ¶ 128. But the Supreme Court has rejected such an approach, explaining instead that:

> [Regulatory] problems may arise . . . [that] must be solved despite the absence of a relevant general rule. 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. In those situations, the agency must retain power to deal with the problems on a case-to-case basis if the administrative process is to be effective.

SEC v. Chenery, 332 U.S. 194, 202-03 (1947). Thus, an agency's discretion is "at its peak" when it decides "whether to address an issue by rulemaking or adjudication." *Am. Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990). Proceeding by adjudication rather than rulemaking is especially appropriate "where important factors may vary radically from case to case." *Id.* The Supreme Court has approved of the FTC's case-by-case approach when using its "unfairness" authority under Section 5. *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965) ("The proscriptions [of unfair or deceptive acts and

practices] in Section 5 are flexible, to be defined with particularity by the myriad of cases from the field of business, which necessarily give[] the Commission an influential role in interpreting Section 5 and in *applying it to the facts of particular cases arising out of unprecedented situations*." (emphasis added)); *see also Wyndham,* Slip Op. 18-25.[11]

As the Supreme Court has recognized, "[b]roadly worded constitutional and statutory provisions necessarily have been given concrete meaning and application by a process of case-by-case . . . decision." *NW Airlines v. Transp. Workers Union of Am.*, 451 U.S. 77, 95 (1981). The three-part statutory standard governing whether an act or practice is unfair is sufficient to give fair notice of what conduct is prohibited. *See* 15 U.S.C. § 45(n). Congress envisioned that the FTC would "develop[] and refin[e] its unfair practice criteria on a progressive, incremental basis." *Am. Fin. Servs.*, 767 F.2d at 979. The FTC is acting as Congress envisioned it would, and is in no way

[11] Indeed, in the field of data security, the FTC "has been involved in addressing online privacy issues for almost as long as there has been an online marketplace," and it has "repeatedly and consistently affirmed its authority to challenge unreasonable data security measures as 'unfair … acts or practices.'" Comm'n MTD Denial at 7. Thus, even though the FTC has not promulgated regulations governing data security, all companies holding electronic data have long been on notice that their security practices could be subject to FTC scrutiny. Contrary to LabMD's inaccurate assertion, the FTC has never "t[old] Congress that it lacks statutory authority" over data security. Pl.'s PI Mem. at 16; *see* Comm'n MTD Denial at 7-8.

violating LabMD's due process rights by adjudicating whether certain data security practices are unfair under Section 5 on a case-by-case basis.[12]

3. The FTC is not employing an unconstitutionally vague standard

The FTC's position – that failure to maintain reasonable data security measures can constitute an unfair act or practice within the meaning of Section 5 – does not establish an unconstitutionally vague behavioral standard. *See* N.D. Ga. Compl. ¶ 129-134. LabMD's main complaint is that what constitutes a reasonable data security program varies under the circumstances. The test for whether an economic regulation is unconstitutionally vague is undemanding, especially where, as here, plaintiff has the "ability to clarify" the standard as part of "an administrative process" prior to the imposition of any civil penalties. *Trans Union Corp. v. FTC*, 245 F.3d 809, 817 (D.C. Cir. 2001). Indeed, "[t]he Supreme Court has warned against the mechanical application of vagueness doctrine, emphasizing that an 'economic regulation is subject to a less strict vagueness test' and there should be 'greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe.'" *Harris v. Mexican Specialty Foods, Inc.*, 564 F.3d 1301, 1310-11

[12] Nor is the FTC required to "link its data-security standards" to HIPAA and HITECH. *See* N.D. Ga. Compl ¶ 134. As discussed *supra*, Part II.A, regulated entities commonly are regulated by more than one federal agency or statutory scheme.

(11th Cir. 2009) (quoting *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498–99 (1982)).

Agencies may use broad terms to describe permissible and impermissible conduct without running afoul of the void-for-vagueness doctrine:

> [When an agency establishes a standard that employs] the use of the terms like "adequate," "appropriate," [or] "suitable" . . . it is not impermissibly vague because "a reasonably prudent person, familiar with the conditions the regulations are meant to address and the objectives the regulations are meant to achieve, would have fair warning of what the regulations require." Courts recognize that "specific regulations cannot begin to cover all of the infinite variety of conditions which [regulated parties] must face," and that "by requiring [standards] to be too specific courts would be opening up large loopholes allowing conduct which should be regulated to escape regulation." Indeed, here, the [agency] was tasked with developing [standards] that apply to a diverse industry and the [agency] has explained that using qualifying terms like "adequate" is necessary to address the variety of conditions that exist at different companies.

Alliance for Natural Health U.S. v. Sebelius, 775 F. Supp. 2d 114, 132 (D.D.C. 2011) (quotation omitted). Like the regulation at issue in *Alliance*, specific regulations cannot begin to cover all of the infinite variety of conditions which companies face with respect to data security.

D. Plaintiff does not make a valid "structural due process" claim

Plaintiff's fourth claim for relief seeks to block the FTC's adjudicatory process for what it terms "facial and structural due process violations." N.D.

Ga. Compl. ¶137. This set of untenable arguments must be dismissed for failure to state a claim.

1. The FTC's structure and Rules of Practice do not violate due process

Plaintiff's main "structural due process" claim is that FTC Rules of Practice directing that motions to dismiss administrative complaints be resolved by the Commission itself "transgress constitutional limits on blending of prosecutorial, legislative, and adjudicative functions" in violation of plaintiff's due process rights. *Id.* ¶140. That contention is flatly wrong. *See FTC v. Cement Inst.*, 333 U.S. 683, 702-703 (1948); *Humphrey's Executor v. United States*, 295 U.S. 602, (1935) (finding FTC's exercise of both enforcement authority and quasi-adjudicatory functions constitutional). Due process "is not a technical conception with a fixed content unrelated to time, place and circumstances," *Cafeteria Workers v. McElroy*, 367 U.S. 886, 895 (1961), but "calls for such procedural protections as the particular situation demands." *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972). In the context of administrative adjudications, courts long ago "reject[ed] the idea that the combination [of] judging [and] investigating functions is a denial of due process." *Withrow v. Larkin*, 421 U.S. 35, 52 (1975); *see also Intercontinental Indus., Inc. v. Am. Stock Exch.*, 452 F.2d 935, 943 (5th Cir. 1971) ("The principle is well established . . . that due process is not violated when an administrative agency exercises both investigative and judicial functions."). Rather, in formal agency adjudicatory proceedings, due process is satisfied

when the agency follows the requirements of the APA. *Withrow*, 421 U.S. 35 at 51-52; *see also FTC v. Cinderella Career & Finishing Schs, Inc.*, 404 F.2d 1308, 1315 (D.C. Cir. 1968) (citing numerous cases).

FTC Rule 3.22(a) accords plaintiff due process because it comports fully with the APA. The regulation provides that motions to dismiss administrative complaints "shall be directly referred to and ruled on by the Commission." 16 C.F.R. § 3.22(a).[13] Contrary to plaintiff's contention that only an administrative law judge may lawfully address a threshold motion, the APA contains no requirement that the ALJ play any role at all in adjudications conducted pursuant to 5 U.S.C. §§ 554 and 556, and it certainly does not require that ALJs address dispositive motions in the first instance. Indeed, the APA allows the *entire* adjudication to be presided over *either* by an ALJ, *or* by "the agency" *or* by "one or more members of the body which comprises the agency." 5 U.S.C. § 556(b).[14] The APA thus *a fortiori* permits the Commission to rule on a motion.

---

[13] The FTC amended Rule 3.22(b) in 2009. 16 C.F.R. Parts 3 & 4, Interim Final Rule, 74 Fed. Reg. 1804, 1809-1810 (Jan. 13, 2009). Previously, that Rule allowed the ALJ to resolve motions to dismiss in the first instance, 16 C.F.R. § 3.22 (2008), with subsequent review by the Commission, which could "adopt, modify, or set aside" the ALJ's decision, 16 C.F.R. § 3.44(a) (2008).

[14] Due process concerns regarding separation of prosecutorial and decisionmaking functions are accommodated by the APA's requirements that staff employees "engaged in the performance of investigative or prosecuting functions … may not … participate or advise in the decision … or agency review" and other protective provisions in 5 U.S.C. § 554(d); *see* 16 C.F.R. § 4.7(b). *See also Withrow*, 421 U.S. at 52. Of course, parties are also entitled to judicial review of a final agency decision. 5 U.S.C. § 702.

Moreover, the APA authorizes "[t]he agency . . . in its sound discretion, to issue a declaratory order to . . . remove uncertainty." 5 U.S.C. § 554(e). By using the term "the agency," the statute contemplates issuance of such an order by the agency acting as a whole and says nothing about an ALJ considering such rulings in the first instance. The Commission's order denying LabMD's Motion to Dismiss "removed uncertainty" about the scope of the FTC's authority over LabMD's data security practices. The ruling enabled the ALJ to narrow discovery and avoided wasteful development of irrelevant evidence.

Finally, both the APA and the FTC Act authorize the agency to review an ALJ's factual and legal conclusions de novo. 5 U.S.C. § 557(b); 15 U.S.C. § 45(b) & (c).[15] Because the APA allows the Commission to set aside an ALJ ruling, plaintiff's argument that due process requires giving an ALJ the first crack at dispositive legal issues makes no sense.

Even if plaintiff had stated a due process claim that theoretically could be viable, it would still fail in the present circumstances. "In order to make out a case of denial of procedural due process, there must be a showing of substantial prejudice." *Arthur Murray Studio of Wash., Inc. v. FTC*, 458 F.2d 622, 624 (5th Cir. 1972). Yet the complaint fails to allege any prejudice at all,

---

[15] The "highly deferential" standard on judicial review "is not altered merely because the [agency] disagrees with the ALJ, and [courts] defer to the inferences that the [agency] derives from the evidence, not to those of the ALJ." *Varnadore v. Sec'y of Labor*, 141 F.3d 625, 630 (6th Cir. 1998) (citations omitted); *see also Universal Camera Corp. v. NLRB*, 340 U.S. 474, 494 (1951).

let alone substantial prejudice, from the Commission's consideration of the motion to dismiss. And because the Commission would have reviewed de novo any ALJ decision dismissing or declining to dismiss the complaint, it is difficult to see how plaintiff possibly could have been prejudiced by the Commission's making that decision in the first instance.

2. Plaintiff has no valid ex post facto claim

As discussed above, 15 U.S.C. § 45(n) provides plaintiff with adequate notice of what the law requires. But even if it did not, plaintiff's claim that the FTC is unconstitutionally engaging in ex post facto enforcement of a law must be dismissed. *See* N.D. Ga. Compl. ¶ 141. The Supreme Court long ago established that the Constitution's prohibition on ex post facto law enforcement applies only to laws that are criminal or penal in nature. *See, e.g.*, *Carpenter v. Com. of Penn.*, 58 U.S. 456, 457 (1854). Even if the FTC issues a final cease and desist order, LabMD could incur sanctions only if the company takes further action that violate the order. Such a sanction is patently not criminal or penal in nature. *See, e.g.*, *Houston v. Williams*, 547 F.3d 1357, 1364 (11th Cir. 2008) (city's denial of certain services to sex offenders not penal in nature and, therefore, no subject to prohibition on ex post facto enforcement); *Dufrense v. Baer*, 744 F.2d 1543, 1550 (11th Cir. 1984) (amendments to the Sentencing Guidelines do not implicate ex post facto considerations "because the guidelines. . . are not criminal laws").

E. Plaintiff's First Amendment claims must be dismissed under Rule 12(b)(6)

LabMD has failed to nudge its First Amendment claims, *see* Fifth Claim for Relief, N.D. Ga. Compl. ¶¶144-150, "across the line from conceivable to plausible." *Twombly*, 550 U.S. at 570. The Court cannot plausibly infer a nexus between Mr. Daugherty's First Amendment activity – *i.e.*, his public criticism of the FTC in his published book and in other public statements – and the FTC actions LabMD challenges in this lawsuit.

Even assuming *arguendo* that Mr. Daugherty's expression constitutes protected speech, LabMD fails to satisfy any of the other established prerequisites for proving that the agency's enforcement action violated LabMD's First Amendment rights. LabMD cannot show that the FTC conduct at issue "adversely affected the protected speech," or that "there is a causal connection between the [FTC's purportedly] retaliatory actions and the adverse effect on speech." *Moton v. Cowart*, 631 F.3d 1337, 1341 (11th Cir. 2011) (quotation omitted). First, nothing in the administrative complaint itself challenges anything LabMD or Mr. Daugherty said or expressed, and the remedy proposed as part of that complaint would not restrict their expression in the future. And LabMD's factual contention that the enforcement action had a "chilling" effect on protected speech is utterly implausible, given that LabMD and Mr. Daugherty have not changed their public criticism of the FTC at all.

Moreover, LabMD cannot plausibly show that the FTC's investigation and enforcement action were brought to retaliate for LabMD's or Mr. Daugherty's criticism of the agency. That criticism began *after* the investigation was well underway; indeed, the entire premise of their public critique is that the agency's investigation of LabMD was itself unfair or improper. Just because the target of an agency investigation or enforcement action complains publicly about the agency's conduct cannot render any subsequent pursuit of the action unconstitutional. Otherwise, *any* target of an agency investigation could evade the agency's charges by publicly complaining about them.

LabMD's insinuation that Mr. Daugherty's publication of the book occurred at roughly the same time as the commencement of the enforcement action does not withstand even the minimal scrutiny Rule 12(b)(6) provides. Mr. Daugherty's book was published approximately three years *after* the FTC had begun investigating LabMD. *See* N.D. Ga. Compl. ¶ 26; Admin Compl. at 12. Courts have declined to infer retaliation unless the timing is "unusually suggestive." *Lauren v. DeFlaminis*, 480 F.3d 259, 267 (3d Cir. 2007)); *see also Swanson v. General Services Admin.*, 110 F.3d 1180, 1188 (5th Cir. 1997) (timing must be "close" to support inference of retaliation). A causal connection cannot plausibly be inferred from timing when the allegedly protected speech occurs in the *middle* of an ongoing action. *See Slattery v. Swiss Reinsurance Am. Corp.*, 248 F.3d 87, 95 (2d Cir. 2001) ("[Where] gradual adverse job actions began well before the plaintiff had ever engaged

in any protected [First Amendment] activity, an inference of retaliation does not arise.").

In essence, LabMD asks this Court to determine that the FTC selectively enforced its data security rules against the company because of its president's protected speech. But the "standard [for showing improper selective enforcement] is "demanding," and agency officials are entitled to a presumption "that they have properly discharged their official duties." *United States v. Armstrong*, 517 U.S. 456, 463-64 (1996). LabMD's allegations do not meet this exacting standard.[16] The FTC has brought numerous enforcement actions against firms across the country alleging unfair acts or practices in connection with data security; the action against LabMD – and the relief related to data security sought by the proposed order – was not novel. LabMD has not come close to showing abuse of the FTC's "significant discretion, analogous to that of a criminal prosecutor, in choosing their targets in administrative enforcement proceedings." *Arnold v. CFTC*,

[16] There is nothing constitutionally improper about the subpoena issued to the President and CEO of LabMD regarding statements he made in a book relating to the very subject matter of the administrative proceeding. N.D. Ga. Compl. ¶ 53. Indeed, the ALJ denied enforcement of the subpoena on the ground that the information sought was not relevant, not that it intruded on Mr. Daugherty's speech rights. *See In re LabMD, Inc.*, FTC Docket No. 9357, ALJ Order on Respondent's Motion for a Protective Order at 8 (Nov. 22, 2013) (FTC Ex. 7). Even if the subpoena were somehow constitutionally improper, which it was not, it was issued not by the Commission but by its separated complaint counsel. Complaint counsel's actions and statements as an advocate in an administrative adjudication cannot be attributed to the Commission as a whole.

987 F. Supp. 1463, 1468 (S.D. Fla. 1997) (citing *Butz v. Economou*, 438 U.S. 478, 515 (1978)).

III. LabMD's motion for a preliminary injunction must be denied

"A preliminary injunction is an extraordinary and drastic remedy" *ACLU of Fla., Inc. v. Miami–Dade Cnty. Sch. Bd.*, 557 F.3d 1177, 1198 (11th Cir. 2009), and is "not to be granted unless the movant clearly [satisfies] the burden of persuasion as to all four" of the following factors: (1) a substantial likelihood of success on the merits; (2) irreparable injury in the absence of injunction; (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) that the injunction would not be adverse to the public interest. *Siegel v. LePore*, 234 F.3d 1163, 1176 (11th Cir. 2000) (en banc); *see also All Care Nursing Serv., Inc. v. Bethesda Mem'l Hosp., Inc.*, 887 F.2d 1535, 1537 (11th Cir. 1989) (a showing on all four factors is required). On the first factor, the Supreme Court has made clear that "[i]t is not enough that the chance of success on the merits be 'better than negligible;'" rather, the party seeking a preliminary injunction—or a stay of an administrative agency proceeding—must make a "strong showing that [it] is likely to succeed on the merits," and "more than a mere 'possibility' of relief is required." *Nken v. Holder*, 556 U.S. 418, 434 (2009). The likelihood of success on the merits is generally considered the most important of the four factors. *See Garcia–Mir v. Meese*, 781 F.2d 1450, 1453 (11th Cir. 1986). As shown above, this Court lacks jurisdiction and thus cannot even reach plaintiff's claims. Nor can LabMD succeed on the merits

because its claims are not viable. That is fatal to LabMD's motion and the Court need not proceed further. "If the movant fails to establish one or more of the four prerequisites, the Court is not required to address the others." *Kramer v. Conway*, 962 F. Supp. 2d 1333, 1343 (N.D. Ga. 2013) (Duffey, J.) (citing *Church v. City of Huntsville*, 30 F.3d 1332, 1342 (11th Cir. 1994)).

Nonetheless, it bears noting that LabMD also fails to meet the other three preliminary injunction factors. *See Nken*, 556 U.S. at 434-35 ("simply showing some 'possibility of irreparable injury' fails to satisfy the second factor"). The Supreme Court has made clear that the type of hardship LabMD will experience by awaiting the FTC's decision – "litigation expense, even substantial and unrecoupable cost" – "does not constitute irreparable injury." *Standard Oil* at 244 (quotation omitted). Moreover, LabMD has not explained how the alleged lapse of its insurance policy on May 6 creates an irreparable injury or an exigent circumstance. According to its own exhibits, LabMD knew that insurers were becoming reluctant to renew LabMD's policies no later than mid-January 2014. *See* N.D. Ga. Compl. Ex. 2. Even earlier, on January 6, 2014, LabMD's CEO sent a letter to the staff and other interested parties, announcing that the company would be closed effective January 15, 2014. *See* N.D. Ga. Compl. Ex. 3. In those circumstances, LabMD cannot show any harm stemming from the May 6 lapse in an insurance policy, especially since LabMD had a case pending before the district court in D.C. in January 2014. Yet LabMD did not ask that court for a preliminary injunction or plead exigency; instead, it dismissed its case

voluntarily – and then waited more than a month to file the present case. That is not the action of a company that truly faces the prospect of irreparable harm. To the degree that it will suffer any harm on May 6, LabMD is the sole cause of its purported hardships.

Additionally, LabMD will not suffer any harm to its First Amendment rights. Its president may continue to engage in speech critical of the FTC, as he has for many years. Indeed, the complaint does not allege any way in which his speech (or that of LabMD itself) has been chilled. *See, e.g.*, *Blum v. Bankatlantic Fin. Corp.*, 925 F.2d 1357, 1363 (11th Cir. 1991) (irreparable harm must be "concrete"). Accordingly, the second factor required for preliminary injunctive relief is unmet.

In contrast to the absence of cognizable harm to LabMD, the FTC and the public will suffer harm if the Court were to grant a preliminary injunction. As *Ewing* and related cases make clear, agencies and the public have a strong interest in an orderly administrative process, unencumbered by premature involvement by the federal judiciary. The public interest would be poorly served by hobbling the proper administrative function of a federal agency that is tasked with protecting consumers from unfair and deceptive trade practices. *See* 15 U.S.C. § 45. That is particularly the case here, where thousands of people have allegedly suffered potentially severe harm as a result of unauthorized disclosure of LabMD's data, and many more could be exposed by further unauthorized disclosures.

In short, all of plaintiff's arguments for why an injunction would be equitable and in the public interest depend on its argument that the FTC has exceeded its legal authority. *See* Pl's Mot. Prelim. Injunction at 29. Because it cannot succeed on the merits of this claim, plaintiff also cannot show that an injunction would be equitable or in the public interest.

CONCLUSION

For the foregoing reasons, plaintiff's complaint must be dismissed and its motion for a preliminary injunction must be denied.

Dated: April 7, 2014

Respectfully submitted,

Of counsel:
JONATHAN E. NUECHTERLEIN
General Counsel
JOHN F. DALY
Deputy General Counsel for
Litigation

JOEL MARCUS-KURN
Attorney

Office of General Counsel
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

STUART F. DELERY
Assistant Attorney General

MAAME EWUSI-MENSAH
FRIMPONG
Deputy Assistant Attorney General

MICHAEL S. BLUME
Director

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

CERTIFICATE OF COMPLIANCE

I certify that the documents to which this certificate is attached have been prepared with one of the font and point selections approved by the Court in LR 5.1B for documents prepared by computer – namely Century Schoolbook, 13 pt.

Dated: April 7, 2014

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on April 7, 2014, I caused a true and correct copy of the foregoing via CM/ECF on:

Ronald L. Raider
Burleigh L. Singleton
William D. Meyer
KILPATRICK TOWNSEND & STOCKTON LLP
1100 Peachtree Street, NE, Suite 2800
Atlanta, Georgia 30309

Michael D. Pepson
CAUSE OF ACTION
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006

Furthermore, the following was provided with a copy via overnight delivery:

Reed D. Rubinstein
DINSMORE & SHOHL, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004

Dated: April 7, 2014

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LabMD, INC., Plaintiff, v. FEDERAL TRADE COMMISSION et al. Defendants.	Civil Action No. 1:13-cv-01787 Hon. Colleen Kollar-Kotelly

NOTICE OF VOLUNTARY DISMISSAL WITHOUT PREJUDICE

Pursuant to Fed. R. Civ. P. 41(a)(1)(A)(i), Plaintiff LabMD, Inc. (LabMD), by and through its counsel, hereby gives notice of its voluntary dismissal of this case without prejudice.

1. On November 14, 2014, LabMD filed a Verified Complaint for Declaratory and Injunctive Relief, Dkt. No. 1, in this Court.

2. Defendants have not answered or moved for summary judgment.

3. Fed. R. Civ. P. 41(a)(1)(A)(i) provides that so long as the opposing party has not yet served either an answer or motion for summary judgment in response to the complaint, a plaintiff may voluntarily dismiss his case without a court order by filing a notice of dismissal. *Little v. Trott & Trott, P.C.*, 2009 U.S. Dist. LEXIS 116575, *2 (D.D.C. Dec. 14, 2009) (citing Fed. R. Civ. P. 41(a)(1)(A)(i)); *accord Miniter v. Sun Myung Moon*, 736 F. Supp. 2d 41, 44-45 & n. 7. (D.D.C. 2010).

4. Plaintiff hereby gives such notice of voluntary dismissal.

5. Therefore, this action should be dismissed without prejudice. *See, e.g., Little*, 2009 U.S. Dist. LEXIS 116575 at *3 ("As such, Plaintiff's complaint is automatically DISMISSED WITHOUT PREJUDICE without the need for a court order." (citing Fed. R. Civ. P. 41(a)(1)(A)(i) and emphasis in original)).

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Daniel Z. Epstein
D.C. Bar No. 1009132
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Telephone: (202) 499-4232
daniel.epstein@causeofaction.org.

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.2024
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland. Admitted pro hac vice.
Practice limited to cases in federal court and
administrative proceedings before federal agencies.

Counsel for Plaintiff LabMD

Dated: February 19, 2014

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. The parties' contentions

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. <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 (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. Analysis

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.